Cisco Catalyst SD-WAN Network Monitoring Guide, Release 26.x and Later

Cisco SD-WAN
Updated October 13, 2026

Topics included

1 Cisco Catalyst SD-WAN Manager Monitor Overview....12

Feature history of Cisco SD-WAN Manager monitor overview....13
Monitor overview dashboards....16
Recommendation: customize the monitor overview dashboard....17
Restrictions for customizing the monitor overview dashboard....17
Customize the monitor overview dashboard....17
Add a dashlet....17
Delete a dashlet....18
Rearrange dashlets....18
Restore default settings....18
Filter dashboard data....19
Cisco SD-WAN Manager monitor overview dashlets....20
View Cisco SD-WAN Manager status....20
View controller and device information....21
View certificate status pane....22
View license pane....22
View EoX status....22
Monitor cellular devices....23
View reboot pane....25
View BFD connectivity pane....25
View transport interface distribution pane....26
View WAN edge inventory pane....27
View WAN edge health pane....28
View the transport health pane....29
View the top applications pane....29
View the Application-Aware routing pane....30
View web server certificate expiration date notification....31
View maintenance windows alert notification....31
View application health dashlet....31
View tunnel health dashlet....32
View top alarms dashlet....33
View temperature and energy usage dashlet....33
View underlay alarms dashlet....34
View data plane drops dashlet....35
View WAN edge health dashlet....36
View WAN edge management dashlet....37
View site health dashlet....37
Security....41
View top threats....42

View firewall rule counter....43
View intrusion prevention details....43
View URL filtering categories....44
View advanced malware protection....45
View security events....46
View security Appliance/UTD container....46
View application offload....47
View Secure Internet Gateway/Secure Service Edge tunnels....48
View the SecureX ribbon....48
Multicloud....49
Access job-role resources from explore....51
Energy management....51
Supported platforms for energy management....53
Generate energy management report....53
Converged dashboard for SD-WAN analytics and SD-WAN manager....54
Converged dashboards....54
Applications dashboard....55
Sites dashboard....56
Circuits dashboard....56
Client dashlet....57

2 Monitor Devices and SD-WAN Control Components....60
Feature history: Monitor devices and SD-WAN Control Components....61
Devices and controllers....61
Geographic location of devices....61
Set map filters....61
Viewing device information....62
Configure geographic coordinates for a device....62
View system status....62
View device system resource utilization in Cisco SD-WAN Manager....63
View device system resource utilization using the CLI....63
Open a TAC case....64
Viewing the status of a Cisco Catalyst SD-WAN Validator....64
View the status of a Cisco Catalyst SD-WAN Validator using the Dashboard page....64
View the status of a Cisco Catalyst SD-WAN Validator using the Geography page....65
View the status of a Cisco Catalyst SD-WAN Validator using the Devices page....65
Viewing the status of a Cisco Catalyst SD-WAN Controller....65
View the status of a Cisco Catalyst SD-WAN Controller using the Dashboard page....65
View the status of a Cisco Catalyst SD-WAN Controller using the Geography page....66
View the status of a Cisco Catalyst SD-WAN Controller using the Devices page....66
View control connections....66
View devices connected to Cisco Catalyst SD-WAN Manager....67
View services running on Cisco Catalyst SD-WAN Manager....67
Viewing device status in the overlay network....67

View device status in the overlay network using the Dashboard page....67
View device status in the overlay network using the Geography page....68
View device status in the overlay network using the Devices page....68
Viewing device information....68
View basic device information....68
View detailed device information....69
Viewing device health in a table view....69
Viewing device health in heatmap view....70
View device configuration....70
View the software versions installed on a device....70
View device interfaces....70
Viewing WAN interfaces....71
View WAN interfaces using the Real Time pane....71
View WAN interfaces using the Interface pane....71
View interfaces in the management VPN or VPN 512....72
View DHCP server and interface information....72
View interface MTU information....72
View and monitor cellular interfaces....73
View colocation cluster information....74
View Cisco Colo Manager health....75
View Cisco Catalyst SD-WAN Manager cluster information using the CLI....75
Viewing QoS statistics....75
QoS queue statistics....75
Benefits of QoS queue statistics....75
Restrictions for QoS statistics....76
Monitor the QoS statistics for interfaces....76
Interface QoS statistics....76
Monitor the QoS statistics for tunnels....77
Tunnel QoS statistics....77
Monitor real-time tunnel QoS statistics....78

3 Resource Monitoring....80

Feature History of Resource Monitoring....81
Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices....81
Configure Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI....83
Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI....85

4 Connectivity Fault Management....88

Feature history: Connectivity fault management....89
Ethernet connectivity fault management....89
Restrictions for connectivity fault management....89
How connectivity fault management works in Cisco Catalyst SD-WAN....90
Down maintenance end points....90

Ethernet CFM and Ethernet OAM interaction....91
SNMP traps....91
Configuring Ethernet connectivity fault monitoring using CLI commands....92

5 Data Collection and Telemetry....96
Feature history: Data collection and telemetry....97
Information about data collection and Cisco Catalyst SD-WAN telemetry....97
Enable or disable data collection....98
Enable or disable Cisco Catalyst SD-WAN telemetry....98
Enable or disable cloud services....99
Additional steps to enable data collection on an on-premises Cisco Catalyst SD-WAN Manager instance....99

6 Flow Simulation....102
Feature history: Flow simulation....103
Simulate flows....103

7 Monitoring Hosted Edge Services....106
Feature history: Monitoring hosted edge services....107
Hosted edge services....107
Restrictions for monitoring hosted edge services....107
Start or stop the hosted edge services....107
Monitor the hosted edge services....108

8 Packet trace....112
Feature history: Packet trace....113
Packet trace....113
Guidelines for packet trace....114
Restrictions for packet trace....114
Configure packet trace using CLI commands....115
Monitoring packet trace....116
Monitoring packet trace on Cisco vEdge devices....117
Monitoring packet trace on Cisco IOS XE Catalyst SD-WAN devices....118
Viewing FIA statistics....121
Configuration examples for packet trace....122

9 Viewing QoS Information....124
Feature history: Viewing QoS information....125
Restrictions for QoS monitoring....125
View QoS information in a chart....125
View a real-time QoS information table....127

10 Security Monitoring....128

Feature history: security monitoring....129
View traffic, CPU, and memory usage....129
View the health and reachability of UTD....129

11 Underlay Measurement and Tracing Services....132
Feature history: underlay measurement and tracing services....133
Underlay measurement and tracing services....133
Benefits of underlay measurement and tracing services....134
Prerequisites for underlay measurement and tracing services....135
Restrictions for underlay measurement and tracing services....135
Configuring underlay measurement and tracing services....135
Configure underlay measurement and tracing services using a configuration group....136
Configure underlay measurement and tracing services using CLI commands....137
Trace and view tunnel paths on demand....138
Troubleshooting underlay measurement and tracing services....138
Zero IP address....138
Timeout error....139
Configuration example for underlay measurement and tracing services....139

12 Viewing Network Topology....142
Feature history: Viewing network site topology....143
Information about viewing site topology....143
Supported devices for site topology visualization....144
Prerequisites for site topology visualization....144
View the network site topology....144

13 Monitoring the Network....146
View WLAN output....148
View client details....148
View WiFi configuration....148
View VRRP information....149
View VNF status....149
View Cisco umbrella information....150
View tunnel health in table view....150
View tunnel health in heatmap view....151
View data plane tunnel loss statistics....151
View traffic loss for application-aware routing....152
View the top 100 tunnel connections....152
View tunnel connections for a device....152
View TLOC loss, latency, and jitter information....153
View SFP information....154
View PKI trustpoint information....155
View Cisco Catalyst SD-WAN Validator information....155

View NMS server status....156
View network-wide path insight....156
View multicast information....157
View loss percentage, latency, jitter, and octet information for tunnels....157
View logging information....158
View license information....159
View SAIE flows....159
View Cisco Catalyst SD-WAN Controller policy....161
View ACL information....161
Monitor NAT DIA tracker configuration on IPv4 interfaces....162
View control connections in real time....162
View cloud express information....163
View cflowd information....163
View BGP information....165
BFD protocol....166
BFD operation process....166
BFD session states....166
View BFD session information....168
View ARP table entries....168
View AppQoE information....169
View the system clock....169
Run a traceroute....170
View routing information....170
Rediscover network....172
Feature history of network monitoring....173
Determine the status of network sites....174
View a configuration commit list....175
Run site-to-site speed test....175
Check application-aware routing traffic....176
View internet outages....177

14 Insecure Configuration Management....178
Feature history for insecure configuration management....179
Resilient infrastructure....179
Enable insecure configuration management....180
View insecure configurations....180

15 Secure Cisco Catalyst SD-WAN with Live Protect....182
Feature history for Live Protect....183
Live Protect for Cisco Catalyst SD-WAN....183
Benefits of Live Protect....184
Vulnerability Shield lifecycle....184
Lifecycle policy scope....184
Vulnerability Shield availability....185

Configure Live Protect for Cisco SD-WAN Control Components using Cisco SD-WAN Manager....186
Disable Live Protect using Cisco SD-WAN Manager....187
Monitor Live Protect....187
View shield status for Live Protect....187
View event statistics for Live Protect....188

16 Application Performance and Site Monitoring....190
Feature history of application performance and site monitoring....191
Application performance and site monitoring....191
Restrictions for application performance and site monitoring....192
Configuring application performance and site monitoring....193
Configure application performance and site monitoring using configuration groups....193
Configure application performance and site monitoring using a CLI add-on template....194
Monitor application health....195
Viewing all applications across all sites....195
Viewing all applications for a single site....195
Viewing a single application across all sites....196
Viewing a single application on a single site....196
Viewing application health in table view....196
Viewing application health in heatmap view....196
Troubleshoot application performance and site monitoring....197

17 Managing Alarms....198
Feature history of alarms....199
Alarms....200
Alarm states....201
Alarm fields....202
Viewing alarms....203
Set alarm filters....205
Filter alarm search results....206
Export alarms....207
Alarm notifications....207
Enable email notifications....207
Send alarm notifications....208
Viewing email notifications....210
Edit an email notification....210
Delete an email notification....210
Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands....210
Verify login rate alarms....211
Safety barriers....212
CPU barrier....213
Disk barrier....213
Memory barrier....214

18 Managing events....216
Feature history of events....217
Events....217
Viewing events....218
Viewing events using Cisco SD-WAN Manager....218
Viewing events using CLI Commands....218
Viewing failover events....219
Set event filters....219
Filter event search results....220
Export events....220
Monitor event notifications....221

19 System and Network Logs....222
Feature history of logs....223
Set ACL log filters....224
Audit logging....224
View audit log information....224
Protection against unauthorized login activity....225
Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands....225
Verify a login-rate alarm threshold for Cisco SD-WAN Manager....226
Monitor system login rate alarms....226
Configure lockout policy for Cisco SD-WAN Manager using CLI commands....227
Viewing the logs of configuration template activities....228
Syslog messages....228
Configure system logging....228
View syslog messages using Cisco SD-WAN Manager....228
View syslog messages using CLI commands....229
View system logging settings....229
System log files....229
Syslog message format....230
Cisco SD-WAN Manager log files....231
Configure Cisco SD-WAN Manager logs....232
Viewing logs....232
Viewing the log of certificate activities....233
Traffic logs....233
Traffic logs....233
Benefits of traffic logs....233
Restrictions for traffic logs....234
Generate traffic logs using Cisco SD-WAN Manager....234
Binary Trace for Cisco Catalyst SD-WAN Daemons....236
Configure binary trace level....237
View binary trace level....237
Viewing messages logged by Binary Trace for a Cisco Catalyst SD-WAN process....238

View messages logged by binary trace for all Cisco Catalyst SD-WAN processes....238

20 Reports....240

Feature history of reports....241
Reports....241
Restrictions for reports....242
Run a report....242
Configure email settings....243
View and manage Reports....244
View generated reports....244
Download a report....244
Edit a report....244
Rerun a report....245
Cancel a scheduled report....245
Delete a report....245
Generate CPU, memory, energy report....246
Generate energy management report....246
Generate upgrade pre-check report....247

21 Configuration consistency across Cisco Catalyst SD-WAN Controllers....250

Feature history of configuration consistency across Cisco Catalyst SD-WAN Controllers....251
Configuration consistency across Cisco Catalyst SD-WAN Controllers....251
Multi-stage approach for configuration consistency across Cisco Catalyst SD-WAN Controllers....251
Prerequisites for configuration consistency across Cisco Catalyst SD-WAN Controllers....252
Restrictions for configuration consistency across Cisco Catalyst SD-WAN Controllers....252
Warning messages for offline Cisco SD-WAN Controllers....253
Verify consistent configuration across Cisco Catalyst SD-WAN Controllers....253

22 Packet Capture....256

Feature history of packet capture....257
Bidirectional packet capture....257
Configuring packet capture....258
Configure packet capture using Cisco SD-WAN Manager....258
Configure packet capture using CLI commands....259

1 Cisco Catalyst SD-WAN Manager Monitor Overview

Topics:

- Feature history of Cisco SD-WAN Manager monitor overview
- Monitor overview dashboards
- Customize the monitor overview dashboard
- Cisco SD-WAN Manager monitor overview dashlets
- Security
- Multicloud
- Access job-role resources from explore
- Energy management
- Converged dashboard for SD-WAN analytics and SD-WAN manager

Introduces the Cisco Catalyst SD-WAN Manager monitoring capabilities, outlining key features and how users can leverage monitoring tools to gain insights into network performance and health.

Feature history of Cisco SD-WAN Manager monitor overview

Outlines the evolution of the vManage Monitor Overview dashboard, highlighting feature enhancements for real-time monitoring, customizability, security, global topology, cellular and energy management, integrated analytics, advisories, and improved infrastructure visibility across multiple releases.

Describes the features and functionalities of the Monitor Overview dashboard in Cisco vManage for effective network monitoring.

Table 1: Feature History

Feature Name	Release Information	Description
Enhanced Cisco SD-WAN Manager User Interface for a Consolidated Monitoring View	Cisco vManage Release 20.7.1	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all the monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all the monitoring components have been organized into buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu for you to easily locate these features.
Customizable Monitor Overview Dashboard in Cisco SD-WAN Manager	Cisco vManage Release 20.9.1	This feature adds customizability to the **Monitor Overview** dashboard. It gives you the flexibility to specify which dashlets to view and sort them based on your personal preferences. You can customize the **Monitor Overview** dashboard. You can specify which dashlets to view and sort them based on your personal preferences.
Time Filter in Monitor Overview and Monitor Security Dashboards in Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	The time filter option added to the **Monitor Overview** and **Monitor Security** dashboards in Cisco SD-WAN Manager enables you to filter the dashboard data for a specified time range.
View Sites in Global Topology View	Cisco vManage Release 20.11.1	You can view all sites or a single site in the global topology view for geographical regions worldwide by clicking the inverted-drop-shaped icon on the **Monitor Overview** dashboard.
View Top Alarms	Cisco vManage Release 20.11.1	You can view alarm details for a single site on the **Monitor Overview** dashboard. Click **View Details** to open the **Monitor** > **Logs** > **Alarms** window and view the alarm details.
View WAN Edge Management	Cisco vManage Release 20.11.1	You can view the WAN Edge Management dashlet on the **Monitor Overview** dashboard.

Feature Name	Release Information	Description
Security Dashboard Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enhances the security dashboard in Cisco SD-WAN Manager. The security dashboard introduces a **Actions** drop-down list that enables you to edit the security dashboard, reset the security dashboard, and view the **SecureX** ribbon in the security dashboard. Also, you can access the Cisco Talos portal from Cisco SD-WAN Manager. A hyperlink of the Cisco Talos portal is added to the security dashboard.
Global Network View with Network-Wide Path Insight Integration	Cisco Catalyst SD-WAN Manager Release 20.12.1	Network-Wide Path Insight is now integrated with the global network view. This feature also introduces enhancements to the geomap view by providing real-time monitoring of the health of each site. **Global Topology View** is now called as **Global Network View** in Cisco Catalyst SD-WAN Manager.
Security Dashboard Enhancements	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enhances the security dashboard to provide greater flexibility while troubleshooting security threats down to a device level in Cisco Catalyst SD-WAN.
Explore Menu Option	Cisco Catalyst SD-WAN Manager Release 20.13.1	An Explore page provides quick access to various Cisco resources relevant to specific job roles–**NetOps**, **SecOps**, **AIOps**, and **DevOps**. The resources include developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more, in a single pane of glass.
Security Dashboard Enhancements	Cisco Catalyst SD-WAN Manager Release 20.14.1	The Security dashboard in Cisco SD-WAN Manager has the following enhancements: • A **Security Appliance/UTD Container** dashlet is added to monitor the health status of the Firewall and UTD components, such as the Cisco Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), and Cisco URL filtering. • A new **Application Offload** dashlet is introduced that displays the breakdown of application traffic across SIG or Secure Service Edge (SSE) tunnels and Direct Internet Access (DIA), and provides more details about the application traffic. • Enhancements to existing dashlets to provide additional information about events. • A redirect is added from the Intrusion Prevention dashlet to the Talos website to view Snort rules.

Feature Name	Release Information	Description
Improved Monitoring of Cellular-Enabled Devices	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1 Cisco IOS CG Release 17.14.1	Cisco SD-WAN Manager provides detailed information about the connectivity of cellular-enabled devices, and the health of the connections, to provide a holistic view of cellular connectivity health. In addition, you can filter the device list to specifically display cellular-enabled devices, among other filter options.
Converged Cisco SD-WAN Manager and Cisco SD-WAN Analytics Dashboard	Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature introduces a converged dashboard in Cisco SD-WAN Manager that merges the monitoring and analytics capabilities from both Cisco SD-WAN Manager and Cisco SD-WAN Analytics. This converged dashboard displays management data from the Cisco SD-WAN Manager alongside analytical insights from Cisco SD-WAN Analytics. To view a converged dashboard in Cisco SD-WAN Manager, Cisco SD-WAN Analytics must be onboarded into Cisco SD-WAN Manager.
Energy Management	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature introduces a new dashboard that displays the Cisco SD-WAN Manager power utilization, energy usage, device capability, and consumption data.
Improved Monitoring of Cellular-Enabled Devices	Cisco Catalyst SD-WAN Manager Release 20.16.1	The following cellular monitoring dashlets in Cisco SD-WAN Manager have been enhanced to provide additional insights for building and maintaining a competitive cellular WAN solution: • Cellular Device Count • Cellular Health • Cellular Data Usage
Advisories	Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature provides centralized visibility into security vulnerabilities and critical field notices for your Cisco SD-WAN network. It offers EoX Status section that provides detailed End-of-Support and End-of-Sale information for effective replacement and upgrade planning.
Underlay Health Visibility	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature provides enhanced monitoring and troubleshooting capabilities for the underlying network infrastructure that supports your Cisco Catalyst SD-WAN overlay.

Feature Name	Release Information	Description
Energy Management Dashboard	Cisco Catalyst SD-WAN Manager Release 26.1.1.1	The Energy Management dashboard in Cisco SD-WAN Manager has the following enhancements: • Energy management reporting • Offline-mode support • Carbon intensity metrics • Time period comparison • Site-to-Site comparisons
Energy Management Enhancements	Cisco Catalyst SD-WAN Manager Release 26.1.1.1	This feature enhances the support on IR platforms. For details on supported platforms, see Supported Platforms for Energy Management.

Monitor overview dashboards

Explains the customizable Monitor Overview dashboard, which displays dashlets for components and services and allows adding, deleting, rearranging, and restoring dashlets. Describes how customized settings persist in a database and are retrieved across sessions and upgrades.

A monitor overview dashboard is a user interface dashboard that

- displays all the available dashlets that help monitor the different components and services of a Cisco Catalyst SD-WAN overlay network, and
- lets users add, delete, or rearrange dashlets and restore default settings.

Monitor overview dashboard options

The customized dashboard settings are saved in a database. These settings are retrieved in these scenarios:

- When you log in to Cisco SD-WAN Manager again.
- When you navigate from another window to the **Monitor Overview** dashboard.
- When you upgrade Cisco SD-WAN Manager from an earlier release to a new release.

This feature is available in both single-tenant and multitenant deployments. In multitenant deployments, this feature is available only for the tenant dashboard.

Note

Use Google Chrome to access Cisco SD-WAN Manager. Firefox is also supported.

Users belonging to all the standard and custom user groups, regardless of the read or write permissions, can customize the **Monitor Overview** dashboard.

Recommendation: customize the monitor overview dashboard

Outlines why customizing the Monitor Overview Dashboard improves visibility and speed. Consider prioritizing relevant dashlets, removing clutter, and arranging content to see key metrics at a glance and evaluate them more efficiently.

Cisco recommends customizing the dashboard to prioritize relevant dashlets, reduce clutter, and organize content to evaluate key metrics more efficiently.

- Flexibility: Customizing the dashboard enables you to view the most relevant dashlets, and to reduce clutter by removing the dashlets that are less relevant for your purposes.
- Efficiency: You can view all the key metrics at a glance, and evaluate and analyze them more quickly.
- Easy Organization: You can drag and drop the dashlets and organize the dashboard according to your requirements. For example, you can easily drag a dashlet that is particularly relevant to you, to the top.

Restrictions for customizing the monitor overview dashboard

Outlines restrictions for customizing the Monitor Overview dashboard, including scope in multitenant environments, non-customizable UI elements, and limitations during edit mode, with the minimum supported release referenced for deployment eligibility.

Customize only the Monitor Overview dashboard and note that some interface elements are fixed and certain actions are disabled while you edit.

- In multitenant deployments, this feature is available only for the tenant dashboard.
- This feature is available only for the **Monitor Overview** dashboard.
- The menu bar, which runs across the top of the **Monitor Overview** dashboard, is not customizable.
- When the dashboard is in edit mode, other actions, such as selecting a time period for which to display data, viewing real-time data, and so on, are disabled.

Customize the monitor overview dashboard

Provides a reference for customizing the Monitor Overview dashboard, including the minimum release requirement, and consolidates related screen information through a referenced table.

Add a dashlet

Configure the dashboard by adding available dashlets in vManage Overview. Use Edit Dashboard to add and save selected dashlets. This task helps customize monitoring views based on your operational needs.

Before you begin

Follow these steps to add a dashlet:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Edit Dashboard**.
3. Click **Add Dashlet**.

   The **Add Dashlet** option is available only if additional dashlets are available to be added. It is not available on the default dashboard.
4. Choose the dashlets that you want to add.
5. Click **Add**.
6. Click **Save**.

Delete a dashlet

Configure the dashboard layout by removing an unwanted dashlet from the Monitor > Overview page in vManage: enter Edit Dashboard, delete the dashlet, confirm deletion, and save your changes to update the view.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.
2. From the **Actions** drop-down list, choose **Edit Dashboard**.
3. Click the **Delete** icon adjacent to the corresponding dashlet name.
4. To confirm the deletion of the dashlet, click **Yes**.
5. Click **Save**.

Rearrange dashlets

Configures the Monitor Overview dashboard by moving dashlets and saving the customized layout. The Actions menu provides access to the dashboard editing controls.

Rearrange dashlets on the Monitor Overview dashboard by using Edit Dashboard to drag and drop tiles, then save the customized layout.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** .
2. From the **Actions** drop-down list, choose **Edit Dashboard** .
3. Drag and drop the dashlets according to your requirements.
4. Click **Save** .

The customized layout is saved on the Monitor Overview dashboard.

Restore default settings

Restores the Monitor Overview page to its default view by selecting Reset to Default View from the Actions list and applying the change.

Restore the Monitor Overview page to its default view using the Actions list and apply the change.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** .
2. From the **Actions** drop-down list, choose **Reset to Default View** .
3. Click **Apply** .

Filter dashboard data

Configure time-based filters on the Monitor Overview and Monitor Security dashboards to refine displayed data within a specified range. Use dashboard-level or dashlet-level filters to view recent health and application metrics. Default retention and availability vary by dashlet.

Filter data on the Monitor Overview and Monitor Security dashboards by a specific time range to focus on recent site, tunnel, WAN Edge, application, transport, and alarm metrics.

You can view the data on the **Monitor Overview** and **Monitor Security** dashboards based on a specified time range. A time filter option is available on these dashboards. On the **Monitor Overview** dashboard, the time filter option is applicable to these dashlets:

- **Site Health**
- **Tunnel Health**
- **WAN Edge Health**
- **Application Health**
- **Transport Health**
- **Top Alarms**
- **Top Applications**

This feature is available in both single-tenant and multitenant deployments. In multitenant deployments, this feature is available only in the tenant dashboard.

Time filter values: 1 hour, 3 hours, 6 hours, 12 hours, 24 hours, 7 days, 30 days.

Only in the **Transport Health** dashlet, the data is available up to 7 days. In the **Site Health**, **Tunnel Health**, **WAN Edge Health**, **Application Health**, and **Top Applications** dashlets, the data is available up to 24 hours.

Default: 24 hours

Before you begin

Minimum release: Cisco vManage Release 20.10.1

Follow these steps to filter dashboard data:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview** or **Monitor** > **Security**.
2. From the time filter drop-down list, choose a value.

   You also can apply the time filter at the dashlet level. To do this, click **View Details** in the corresponding dashlet, and choose a time filter value in the right navigation pane. The time filter value applied at the dashboard level, and not at the dashlet level, is preserved after closing the navigation pane.

The dashlets display the data based on the chosen time.

Cisco SD-WAN Manager monitor overview dashlets

Introduces the monitor overview dashlets in Cisco SD-WAN Manager, highlighting their features and functionality for network monitoring and visibility.

View Cisco SD-WAN Manager status

Verify device and controller health and resource usage in the management UI by navigating to Monitor > Devices, checking the Health column, and opening System Status to view CPU and memory details in Device 360.

Use this task to view the health of a device or controller and review CPU and memory usage in the management interface.

You can view details about the health of a device or controller, and the CPU and memory usage on Cisco SD-WAN Manager.

Note

When you enter any keyword in the search table filter, results that partially match your search will display. For more accurate results, use the column search feature. This allows you to search within a specific column, ensuring that the results are more relevant to your query. This applies to all pages within the SD-WAN Manager where the search table filter and column search filters are visible.

Follow these steps to view device and controller health and resource usage:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   In the table, the **Health** column shows the device or controller health. Place the cursor over the icon in the column to display **Good**, **Fair**, or **Poor**.

   Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, these are the health status indicators for edge devices:

   - **Good**: Edge device is using less than 88% of available memory, and less than 80% of CPU resources.
   - **Fair**: Edge device is using greater than or equal to 88% of available memory, or 80% of CPU resources.
   - **Poor**: Edge device is using greater than or equal to 93% of available memory, or 90% of CPU resources.

> **Note**
>
> Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, Cisco SD-WAN Manager uses the same threshold values as those used by edge devices to measure the health of all edge devices. This ensures that health status is shown consistently on the device and on the Cisco SD-WAN Manager.

2. Click a Cisco SD-WAN Manager controller in the table.
3. Under **SECURITY MONITORING**, click **System Status**.

> **Note**
>
> If a Cisco SD-WAN Manager controller is using more than 90% of total memory or CPU, its performance may be degraded. If you cannot log in to Cisco SD-WAN Manager, contact Cisco TAC for assistance.

The **Device 360** page shows the CPU and memory usage.

View controller and device information

Provides an overview of Control Components and WAN Edges indicators in the Monitor overview, how to drill down to device details and tools, and how vManage displays autonomous routers and legacy behavior differences across releases.

> **Note**
>
> From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is called **Control Components**.

The **Control Components** and **WAN Edges** areas of the menu bar, which runs across the top of the **Monitor** > **Overview** page, display the total number of Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN Manager instances in the overlay network. They also display the status of the devices in the network.

When you click a device number, the **Monitor** > **Devices** page displays detailed information about each device. Click **...** adjacent to the corresponding device to access the device dashboard or the Real Time view or to access the **Tools** > **SSH Terminal**.

In addition to routers in controller mode, from Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco SD-WAN Manager can monitor routers that are in autonomous mode and not part of the Cisco Catalyst SD-WAN overlay network. You can use the **show version | include mode** command to check the mode of a router. On various pages such as the **Devices** page (**Monitor** > **Devices**), these routers appear with the label **SD-Routing** in the **Device Model** column to distinguish them from routers that are part of the overlay network.

In Cisco vManage Release 20.6.x and earlier releases, Cisco SD-WAN Manager behaves in these ways:

- The **Control Components** and **WAN Edges** areas are grouped together in the **Summary** area. (The **Summary** area is part of the **Dashboard** > **Main Dashboard** page.)
- When you click a device number, a pop-up window that displays detailed information of each device, opens.

- The device dashboard or the Real Time view is part of the **Monitor** > **Network** page.

View certificate status pane

Provides an overview of the **Certificate Status** pane that displays certificate states across all controllers and counts expired or invalid certificates, and opens the **Monitor** > **Devices** > **Certificate** page with hostname, system IP, serial number, expiration, and status details.

The **Certificate Status** pane displays the state of all certificates on all controller devices, and it shows a count of all expired or invalidated certificates. Click the **Certificate Status** pane to open the **Monitor** > **Devices** > **Certificate** page, which displays the hostname and system IP of the device on which the certificate is installed, the serial number of the certificate, and its expiration date and status.

In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has this behavior:

- The **Certificate Status** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of the **Monitor** > **Devices** > **Certificate** page when you click the **Certificate Status** pane.

View license pane

Provides an overview of the Licensing pane that shows totals for configured and licensed devices, and explains how to open the Monitor > Devices > Licensing page to view device identifiers, license status and type, account details, and related subscription information.

Use the **Licensing** pane to view totals for configured and licensed devices and to access detailed device licensing information on the related Monitor > Devices > Licensing page.

This device information is displayed:

- Hostname
- Chassis number and device model
- IP address
- Template name
- Smart account and virtual account of the device
- Master software license agreement (MSLA)
- License status of the device
- License type and license name
- Subscription ID

In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has this behavior:

- The **Licensing** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of the **Monitor** > **Devices** > **Licensing** page when you click the **Licensing** pane. The pop-up window displays the name of the device, number of licensed devices, number of total licenses, and last assigned on status.

View EoX status

Verify end-of-life and end-of-support status for Cisco products in vManage to plan replacements or upgrades effectively. Verify EoX announcements from Monitor > Devices under EoX Status to access detailed information that supports device lifecycle planning and decision-making.

From Cisco Catalyst SD-WAN Manager Release 20.18.1 you can access detailed information about End-of-Support and End-of-Sale to plan replacements or upgrades effectively.

Before you begin

Follow these steps to view EoX status:

Procedure

1. From Cisco SD-WAN Manager, click **Monitor** > **Devices**.
2. Under **EoX Status**, you can view end-of-life and end-of-support announcements for Cisco products.

Monitor cellular devices

Provides a brief overview that describes how to monitor cellular devices and clarifies the purpose at a high level for administrators who need to observe device status and related information.

View cellular device count

Provides an overview of the Cellular Device Count dashlet, including its renaming, minimum supported release, and filters that display counts by product, carrier, and radio access technology with active and standby statuses.

The **Cellular Device Count** dashlet has been enhanced to provide additional information about cellular devices managed by Cisco SD-WAN Manager. The **Cellular Device Count** dashlet displays the total number of cellular devices in a donut chart, showing active devices and standby devices. The data on the dashlet changes based on the selected filter.

> **Note**
>
> Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the **Cellular Carriers Details** dashlet has been renamed to **Cellular Device Count** dashlet.

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

Filter options

The dashlet offers different filtering options:

Count by Product: This filter shows the top 5 products and their count by status. It also provides details on the types of cellular devices, such as PIM modules, integrated devices, NIM modules, and dongles. Click **View Details** for more information about the types of products.

Count by Carrier: This allows you to filter the devices by different cellular carriers. This also displays the number of devices associated with each carrier.

Count by Radio Access Technology: This filter shows the number of devices using different radio technologies such as 3G, 4G, and 5G. For 5G, it shows the split between NSA and SA. If 5G NR-NSA is configured, both radio access technologies are counted but considered a single cellular device. In a Dual PIM scenario, if both PIMs are active, they are counted as two cellular devices.

Click **View Details** to see more granular information about the **Cellular Device Count** dashlet.

View cellular health dashlet

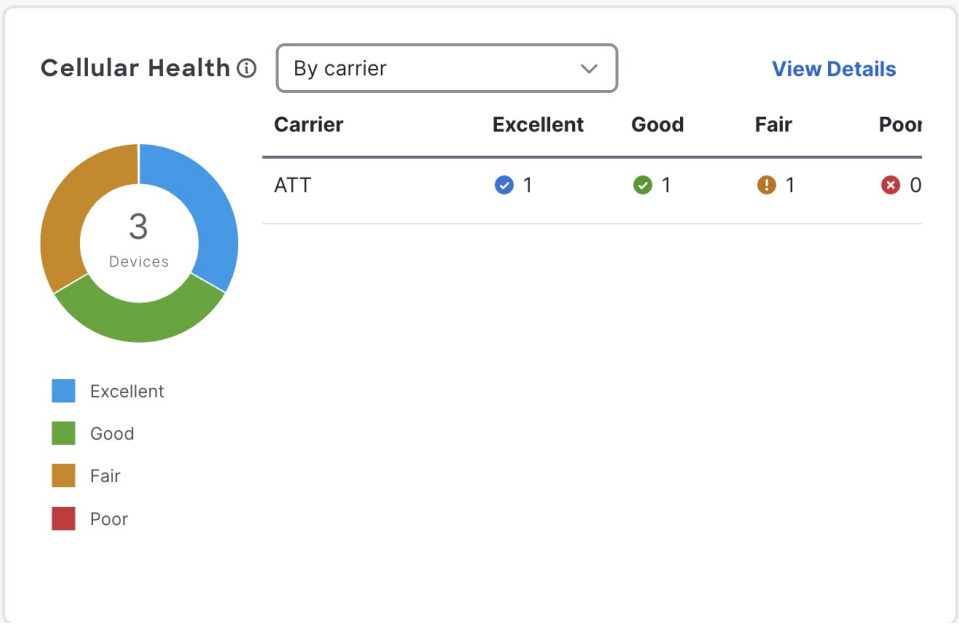
Provides an overview of the Cellular Health dashlet in the Monitor > Overview page, notes the minimum supported release, and describes color-coded health metrics, filters by carrier and radio technology, the donut chart of device health, and real-time link uptime reporting.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1.

View detailed information about the connectivity of cellular-enabled devices, and the health of the connections using the **Cellular Health** dashlet in the **Monitor > Overview** page.

This is the Cellular Health dashlet:

Figure 1: Cellular health



Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the **Cellular Health** dashlet has been enhanced to provide additional information about the health status of cellular connections managed by Cisco SD-WAN Manager. It displays the health metrics of cellular devices categorized based on different filters such as carriers and radio technology. The donut chart displays the total number of cellular devices, with health details represented by color codes: Excellent, Good, Fair, and Poor.

Color coding

The health status is color-coded to indicate the quality of the connection:

- Excellent: Blue
- Good: Green
- Fair: Orange
- Poor: Red

Filter options

The dashlet offers different filtering options:

By Carrier: This filter shows the health status of cellular devices based on their carriers. It displays the number of devices under each health category for each carrier.

By Radio Technology: This filter categorizes the health of devices based on the technology used, such as 4G, 5G, and others. It provides a breakdown of health status within each technology type.

Health Metrics: Metrics such as Received Signal Strength Indicator (RSSI), Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), Signal-to-Interference-plus-Noise Ratio (SINR), and Energy per Chip per Interference (EC/IO) are used to determine the health status.

Click **View Details** to see more granular information about the **Cellular Health** dashlet.

Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, the cellular link uptime is reported in real-time instead of minutes.

View cellular devices

Provides steps to view cellular-enabled devices by opening the Monitor and Devices pages and filtering Type to Cellular, enabling administrators to list only cellular-capable devices in their inventory for verification and monitoring purposes.

Use the Monitor and Devices pages to view cellular-enabled devices by setting Type to Cellular, and ensure the environment meets the minimum supported release.

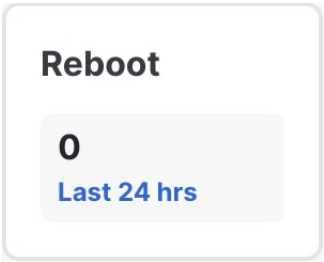
Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click the **Summary** pane to expand. Under **Type** choose **Cellular**.

   View all the cellular-enabled devices on your Cisco SD-WAN Manager.

View reboot pane

Provides an overview of the Reboot pane, which reports device reboot counts for the last 24 hours and opens a sidebar listing each reboot's device, time, and reason, with a Crashes view that lists crash indices, core times, and filenames.



The **Reboot** pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. When you click **Reboot**, the **Reboot** sidebar appears, which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than once, each reboot option is reported separately.

In the **Reboot** sidebar, click **Crashes** to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has this behavior:

- The **Reboot** pane is part of the **Dashboard** > **Main Dashboard** page.
- A pop-up window opens instead of a sidebar when you click **Reboot**.

View BFD connectivity pane

Provides an overview of the Site BFD Connectivity pane in Cisco Catalyst SD-WAN, describes Full, Partial, and Unavailable states for site BFD sessions, and explains interactions to view details and open device dashboards.

A site is a specific physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each device at a site is identified by the same site ID.

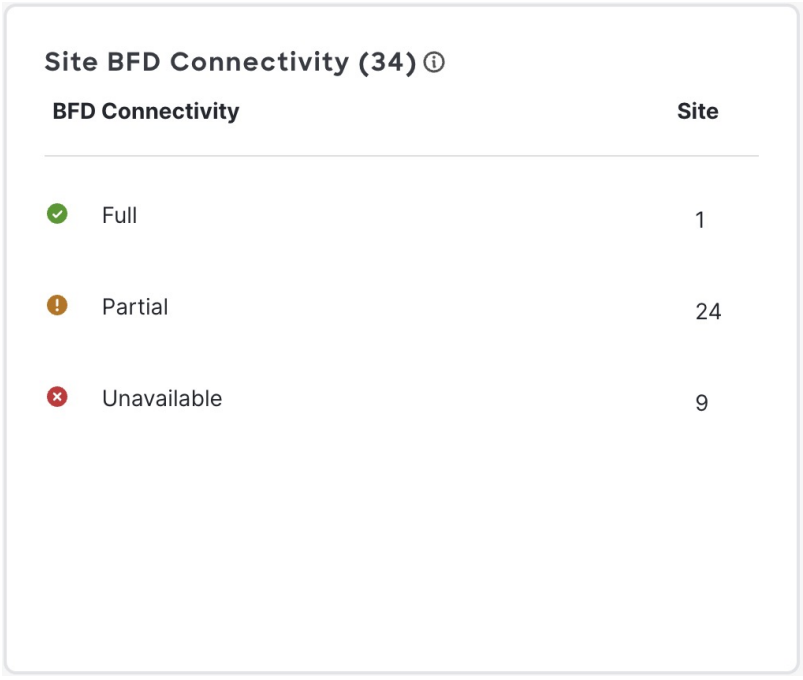
The **Site BFD Connectivity** pane displays the state of a site's data connections. When a site has multiple WAN Edge routers, this pane displays the state for the entire site, not for individual devices. The **Site BFD Connectivity** pane displays three states:

- **Full**: Total number of sites where all BFD sessions on all WAN Edge routers are in the up state.
- **Partial**: Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- **Unavailable**: Total number of sites where all BFD sessions on all WAN Edge routers are in the down state. These sites have no data plane connectivity.

Note

The Site Count includes only sites with the installed devices that are up and running. Some sites are excluded from the Site Count if one of the installed devices in the site is down or if TLOC or tunnels are down (relevant for sites with two devices).

When you click **Full**, **Partial**, or the **Unavailable** status, a sidebar appears displaying detailed information of each site, node, or tunnel. For the desired device, click **...** to access the Device Dashboard or Real Time view in the **Monitor** > **Devices** page or to access **Tools** > **SSH Terminal**.



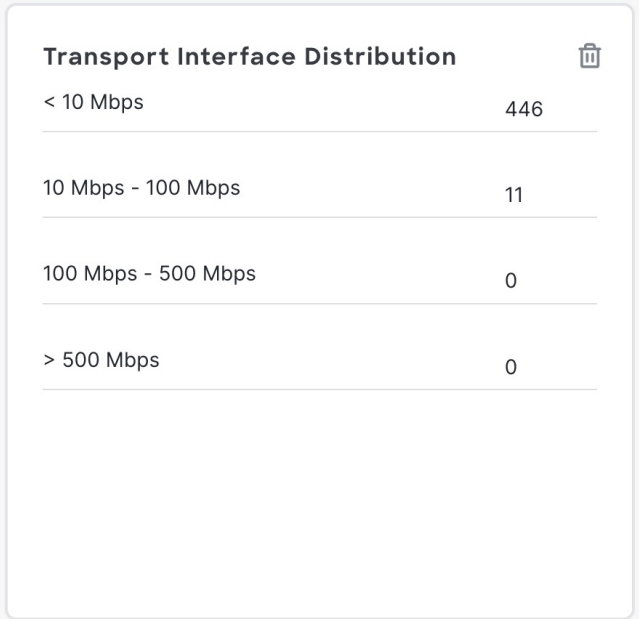
View transport interface distribution pane

Provides an overview of the Transport Interface Distribution pane that reports 24-hour interface usage for WAN Edge interfaces in VPN 0, including TLOCs, and describes the sidebar and percent utilization views with graph and table details.

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0, including all TLOC interfaces. It provides sidebar and percent utilization views with graphical and tabular details.

This is the Transport Interface Distribution dashlet:

Figure 2: Transport interface distribution



When you click the usage statistics, a sidebar appears, displaying the System IP, Interface, and Average details of interface usage.

Click **View Percent Utilization** to view the interface usage in the last 24 hours for all WAN Edge interfaces in graphical format. The graph is depicted for TLOC Distribution Utilization (%) Vs Interface Count. The tabular statistics displays the Hostname, Interface, Average/Low/High Upstream (%), Average/Low/High Downstream (%), and Bandwidth Utilization information.

View WAN edge inventory pane

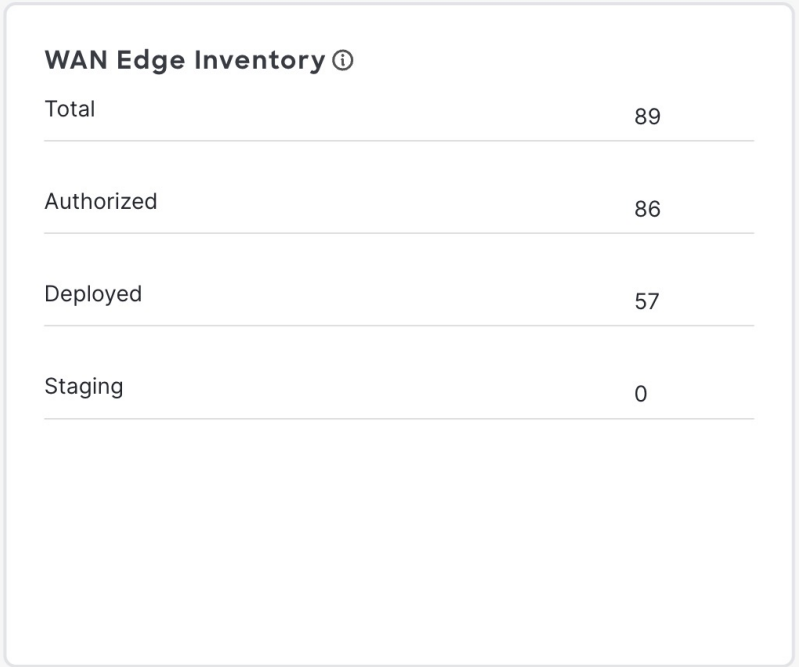
Provides an overview of the WAN Edge Inventory pane counts–Total, Authorized, Deployed, and Staging–and describes how statistics display router details and legacy behavior differences in specific releases.

Counts in the WAN edge inventory pane

The **WAN Edge Inventory** pane provides four counts:

- Total: Total number of WAN Edge routers whose authorized serial number has been uploaded on theCisco SD-WAN Manager server. The serial number is uploaded in the **Configuration** > **Devices** page.
- Authorized: Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid in the **Configuration** > **Certificates** > **WAN Edge List** page.
- Deployed: Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.
- Staging: Total number of WAN Edge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These routers do not take part in any routing decisions nor do they affect network monitoring through the Cisco SD-WAN Manager.

When you click any statistics, a sidebar appears displaying a table with the hostname, system IP, site ID, and other details of each router.



View WAN edge health pane

Provides an overview of the WAN Edge Health pane and the thresholds that define Good, Fair, and Poor states across reachability, control plane, data plane, resources, and attributes, and explains drilldown options to device views and SSH in vManage.

The **WAN Edge Health** pane displays an aggregated view for each router state and a count of how many WAN Edge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- **Good**: Number of routers with memory, hardware, and CPU in good state. Using less than 88% of total memory and 80% of total CPU is classified as good.
- **Fair**: Number of routers with memory, hardware, or CPU in fair state. Using equal to or greater than 88% of total memory and equal to or greater 88% of total memory is classified as in a fair state.
- **Poor**: Number of routers with memory, hardware, or CPU in poor state. Using more than 93% of total memory and more than 93% of total CPU is classified as in a poor state.

The **WAN Edge Health** dashlet displays details about the thresholds of good, fair, and poor devices.

Table 2: Device state conditions and thresholds

Conditions	Good Devices	Fair Devices	Poor Devices
Reachability	Reachable	Reachable	Not Reachable
Control Plane	All control Connections up	One control connection up	No control connections up
Data Plane	All BFD tunnels up and all TLOCs up	One BFD tunnels up and one TLOCs up	No BFD tunnels up and no TLOCs up
Resources	CPU Usage < 80% Memory Usage < 88%	CPU Usage >=80% Memory Usage >=88%	CPU Usage >= 90% Memory Usage >= 93%
Attributes	All attributes met	Any attributes met	Any attribute met

When you click the statistics, a sidebar appears displaying a table with the last one hour of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. For the desired hostname, click **...** to access the Device Dashboard or Device Details view in the **Monitor** > **Devices** page or to access the **Tools** > **SSH Terminal** page.

View the transport health pane

Describes how to assess link quality by viewing aggregated loss, latency, and jitter metrics, selecting a metric and time period, and opening detailed information in a tabular sidebar.

Use the Transport Health pane to assess link quality by viewing aggregated average loss, latency, and jitter across link color combinations.

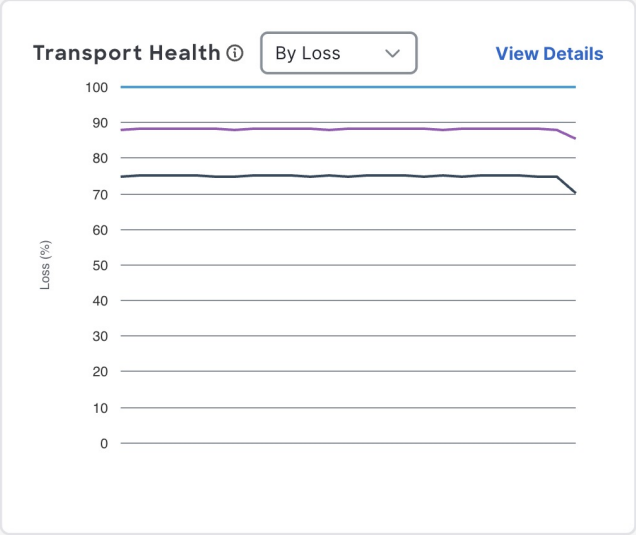
Transport Health pane

The **Transport Health** pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

View transport health metrics

Follow these steps to view the Transport Health pane:

1. From the **Type** drop-down list, select loss, latency, or jitter.



2. Click the **Time** drop-down list to select a time period for which to display data.
3. Click **View Details** .

   You can change the displayed type and time period using the same controls.

   The sidebar displays the information in tabular format.

The Transport Health pane displays aggregated metrics for the selected type and time period, and the details sidebar shows the information in a tabular view.

View the top applications pane

Verify Top Applications pane data in vManage Monitor > Overview to review SAIE flow statistics by VPN and time range, open the sidebar for charts or details, and inspect SSL Proxy policy action views for selected durations.

Use the Top Applications pane to review SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting WAN Edge routers in the overlay network.

The **Top Applications** pane in the Cisco SD-WAN Manager**Monitor** > **Overview** page displays the SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting WAN Edge routers in the overlay network.

> **Note**
>
> Flow DPI data is collected by Cisco SD-WAN Manager on schedule but processed on user requests. Flow DPI based reports are available after data is processed.

Follow these steps to view and analyze the Top Applications data:

Procedure

1. To list top applications by VPN, select a VPN from the drop-down list. To select a time period for which to display data, click the **Time** drop-down list.
2. Click **View Details** to open the **Top Applications** sidebar. It displays a more detailed view of the same information.
3. In **SAIE Application**, from the **VPN** drop-down list, select the desired VPN, and then click **Search**.

   > **Note**
   >
   > In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Application** is called **DPI Application**.

   - Click **Chart** to list the applications.
   - Click **Details** to display more information about the applications.

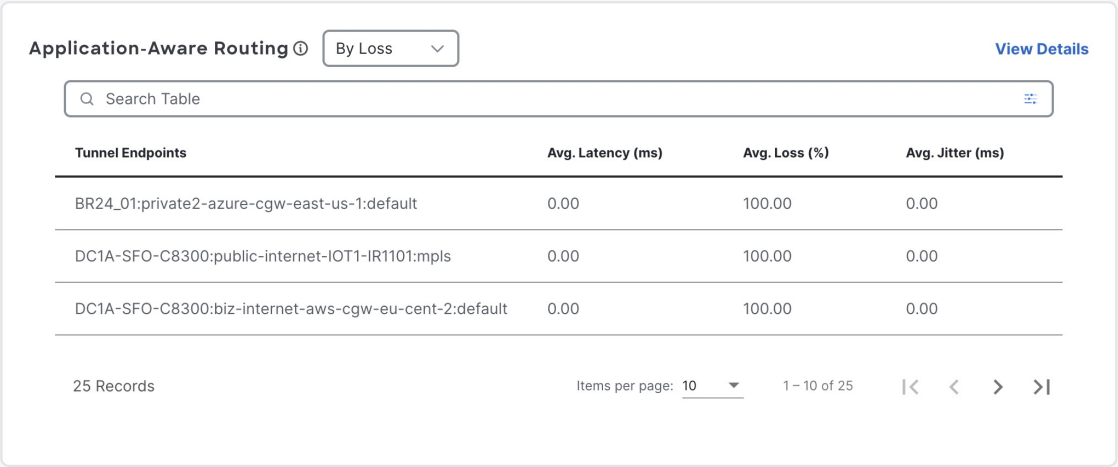
4. Click **SSL Proxy**, from the **View by Policy Actions** drop-down list, select the policy action. All Policy Action, Encrypted, Un-Encrypted, Decrypted view are supported. From the **VPN** drop-down list, select the desired VPN, and then click **Search**. The **Hour** option displays statistics for the selected hour duration.
   - Click **Chart** to list the SSL applications.
   - Click **Details** to display more information about the SSL applications.
5. Click **X** to close the window and return to the **Monitor** > **Overview** page.

View the Application-Aware routing pane

Describes how the pane identifies the 10 worst tunnels by loss, latency, or jitter and opens charts for selected rows. Users can review the 25 worst tunnels for a chosen time period in View Details.

Users can view tunnel charts and detailed tunnel data from the Application-Aware Routing pane.

The **Application-Aware Routing** pane displays the 10 worst tunnels based on criteria you specify from the **Type** drop-down list, which includes loss, latency, and jitter. So, if you choose loss, this pane shows the 10 tunnels with the greatest average loss over the last 24 hours.



1. Click any row to display a graphical representation of the data.
2. Select a time period for which to display data or click **Custom** to display a drop-down for specifying a custom time period.
3. Click **View Details** to open the **Application-Aware Routing** sidebar.

   It displays the 25 worst tunnels based on criteria you specify from the **Type** drop-down list, which includes loss, latency, and jitter.

View web server certificate expiration date notification

Provides details about web server certificate expiration notifications, including where to configure validity, where to view alerts, and the schedule for advance warnings in current and earlier releases.

When you establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you configure the time period for which the certification is valid, in the **Administration** > **Settings** screen. At the end of this time period, the certificate expires. The Web Server Certificate shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco SD-WAN Manager **Monitor** > **Overview** page displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

View maintenance windows alert notification

Provides details about when and where SD-WAN Manager displays a maintenance window alert notification. The Monitor > Overview page shows the alert two days before the start when a maintenance window is configured, with earlier releases showing it on the Dashboard > Main Dashboard page.

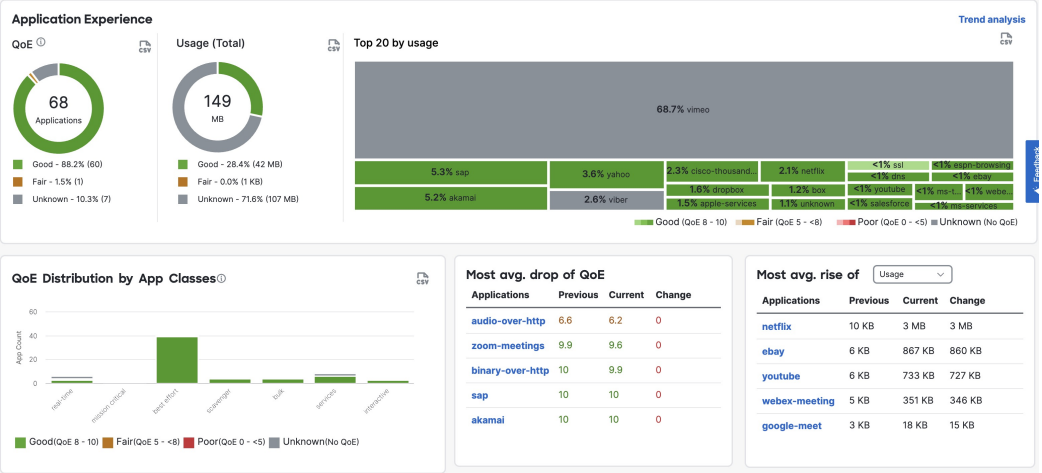
If an upcoming maintenance window is configured on the Cisco SD-WAN Manager server, in the **Administration** > **Settings**, the Cisco SD-WAN Manager **Monitor** > **Overview** page displays a maintenance window alert notification two days before the start of the window.

View application health dashlet

Provides an overview of the Application Health dashlet in Monitor Overview, including QoE-based Good, Fair, and Poor status visualization, bandwidth usage and change graph, filtering by health status, and link to Monitor > Applications.

Minimum supported release: Cisco vManage Release 20.10.1

The Application Health dashlet on Monitor Overview summarizes application health across sites. It displays application QoE as **Good**, **Fair**, or **Poor**, provides a bar graph for bandwidth usage and change, supports filtering by health status, and links to **Monitor > Applications**.



You can view a summary of the health of all applications on the **Application Health** dashlet on **Monitor Overview** dashboard.

You can view the usage of applications across all sites in a graphical format. The graph indicates whether the application performance is **Good**, **Fair**, or **Poor** based on the application Quality of Experience (QoE).

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays the application bandwidth usage information and changes in bandwidth from the last time period for each application. You can filter the applications based on the health status using the drop-down list for **Good Performing Applications**, **Fair Performing Applications**, and **Poor Performing Applications**.

Click **View Details** to open the **Monitor > Applications** window.

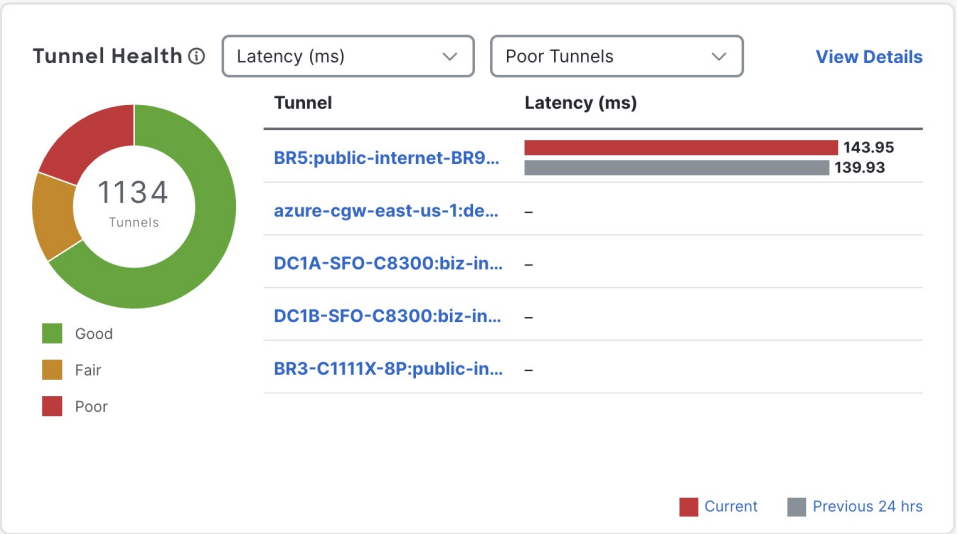
View tunnel health dashlet

Provides an overview of the **Tunnel Health** dashlet in **Monitor Overview**, with health metrics, filters for health and performance, a bar graph of status change, and a link to **Monitor > Tunnels**.

Minimum supported release: Cisco vManage Release 20.10.1

You can view details about the tunnel health on **Monitor Overview** dashboard. This is the Tunnel Health dashlet:

Figure 3: Tunnel health



The **Tunnel Health** dashlet lists this information about all tunnel end points:

- Health
- Average latency, loss, and jitter data

You can view the tunnel health across all sites in a graphical format. You can also filter the tunnel information based on the health status using the drop-down list for **Good Tunnels**, **Fair Tunnels**, and **Poor Tunnels**, and **Latency**, **Loss**, and **Jitter**.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays current status of the tunnel and the change in status from the last time period.

Click **View Details** to open the **Monitor > Tunnels** window to view the tunnel health in table view.

View top alarms dashlet

Provides an overview of the Top Alarms dashlet on the Monitor Overview dashboard and explains how it lists critical and major site alarms by type, with a link to detailed information on the Alarms page.

Minimum supported release: Cisco vManage Release 20.11.1

You can view all critical and major alarms for a site in the **Top Alarms** dashlet on the **Monitor Overview** dashboard.

All the critical and major alarms appear based on the alarm type such as CPU usage, SLA violations, and so on. Click **View Details** to open the **Monitor** > **Logs** > **Alarms** page to view more details about the alarms for a site.

View temperature and energy usage dashlet

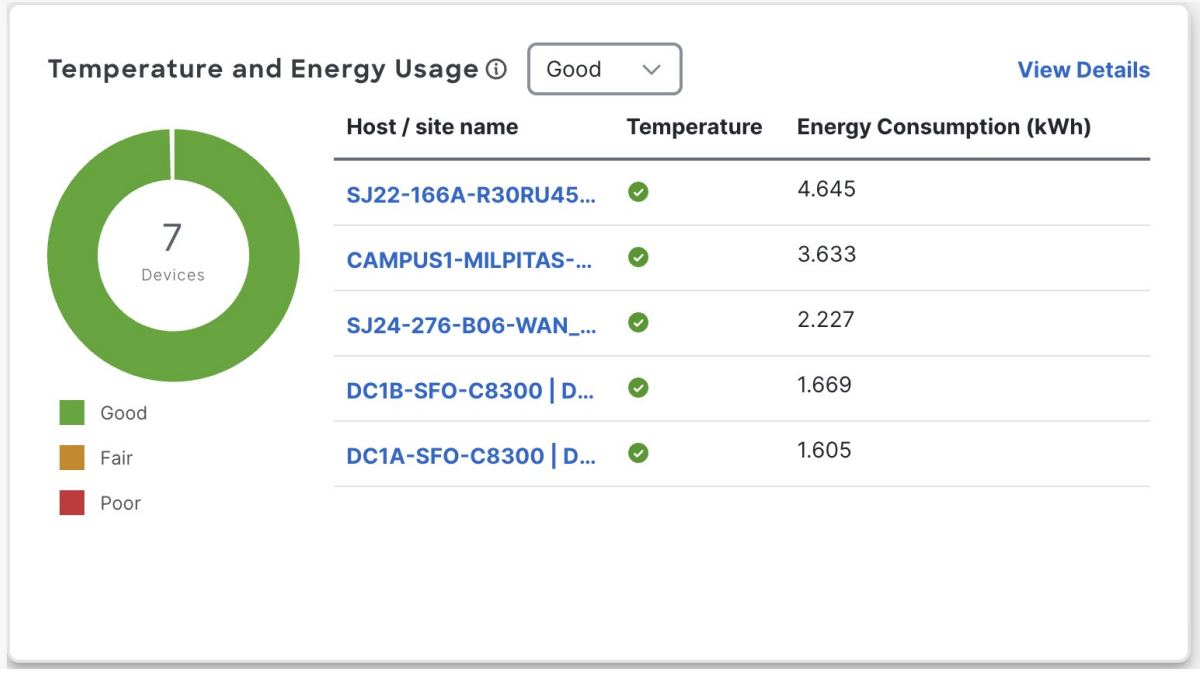
Provides a summary of the Temperature and Energy Usage dashlet that reports temperature sensor and power consumption status for devices, including health categories and navigation to detailed device charts.

The Temperature and Energy Usage dashlet is a new dashlet that allows you to view:

- The status of the temperature sensor, and
- The status of the power consumption

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

You can view the status of the temperature sensor and power consumption of the Cisco IOS XE Catalyst SD-WAN devices in the **Temperature and Energy Usage** dashlet on **Monitor Overview** dashboard.



The health status is categorized as Good, Fair, or Poor based on predefined temperature thresholds:

- Good: The current temperature reading is below the minor threshold.
- Fair: The current temperature reading is at or above the minor threshold but below the critical threshold.
- Poor: The current temperature reading is at or above the critical threshold. You can filter the view based on the health status using the drop-down list.

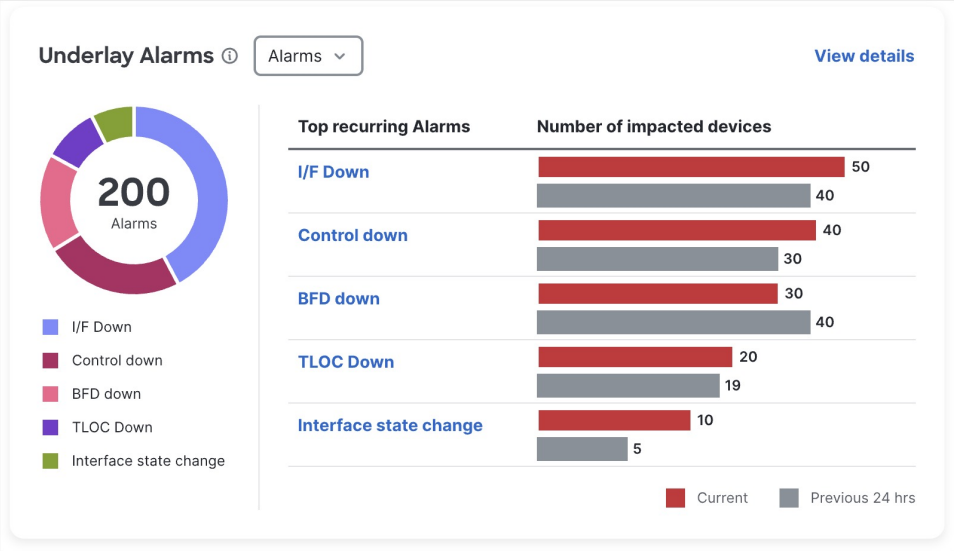
  Click **View Details** to go to the **Monitor** > **Devices** page. Click the host name to navigate to the Device page and view the temperature and energy usage history chart in the **System Status** tab.

View underlay alarms dashlet

Provides an overview of the Underlay Alarms dashlet, which summarizes critical and major alarms for VPN-0 interfaces and offers a link to the Alarms page for deeper analysis and troubleshooting.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

The Underlay Alarms dashlet provides an overview of critical and major underlay alarms affecting your network. This dashlet displays only VPN-0 interface alarms. When you navigate to **View Details** from this dashlet, you may also see alarms for non-VPN-0 interfaces.



- **Critical Alarms** include: Interface State-Change, Interface Admin State Change, Control All Vsmarts DOWN, Control Site DOWN, Control Vsmart DOWN, Control Node DOWN, Control Vmanage DOWN, BFD Site DOWN, and BFD Node DOWN.
- **Major Alarms** include: Control TLOC DOWN and BFD TLOC DOWN.

  Click **View Details** to query these alarms and redirect to the Alarms page for a comprehensive view.

View data plane drops dashlet

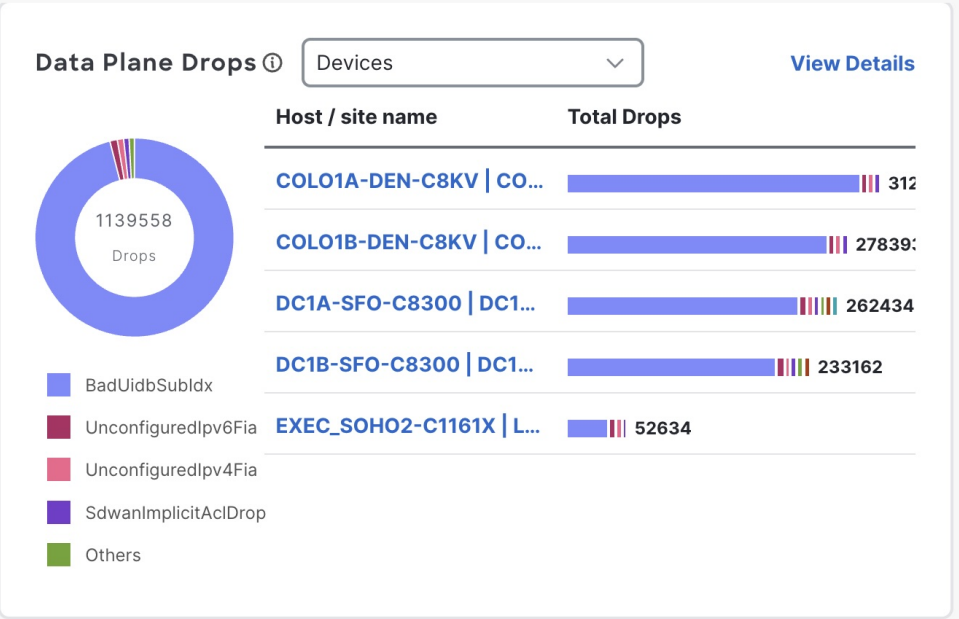
Provides an overview of the Data Plane Drops dashlet that shows various data plane drops on cEdge routers, displays historical device statistics with only non-zero values, and offers a View Details option for accessing more detailed information.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

You can view the various drops seen on the data plane on the Cisco IOS XE Catalyst SD-WAN devices.

This is the Data Plane Drops dashlet:

Figure 4: Data plane drops



The dashlet displays historical data from device statistics. Only non-zero drop statistics are displayed. Click **View Details** to access more detailed data plane drop information.

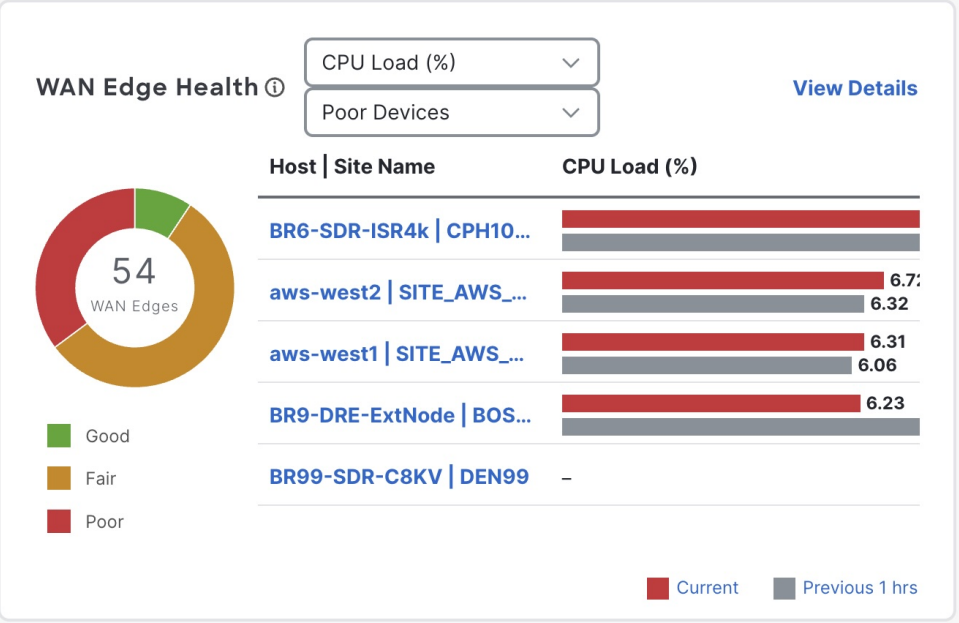
View WAN edge health dashlet

Provides an overview of the WAN Edge Health dashlet on the Monitor Overview dashboard, including device state visibility, CPU utilization trends, filtering by health and load metrics, and access to detailed device health.

Minimum supported release: Cisco vManage Release 20.10.1

You can view the state for each WAN edge device and the number of WAN edge devices in that state in the **WAN Edge Health** dashlet on **Monitor Overview** dashboard:

Figure 5: WAN edge health



Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar chart displays the CPU utilization of WAN edge devices at a site, and the changes in CPU utilization from the last time period.

You can filter the **WAN Edge Health** dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load** and **Memory Load**.

Click **View Details** to open the **Monitor > Devices** window to view the device health in table view.

View WAN edge management dashlet

Provides a summary of the **WAN Edge Management** dashlet on the **Monitor Overview** dashboard, including device state visibility, filtering by configuration type for **Locked Devices** and **Unlocked Devices**, and access to **Monitor > Devices** for detailed table views.

Minimum supported release: Cisco vManage Release 20.11.1

You can view the state for each WAN edge device and the number of WAN edge devices in that state in the **WAN Edge Management** dashlet on **Monitor Overview** dashboard.

You can filter the **WAN Edge Management** dashlet view based on the configuration type using the drop-down list for **Locked Devices** and **Unlocked Devices**.

Click **View Details** to open the **Monitor > Devices** window to view the configured device details in table view.

View site health dashlet

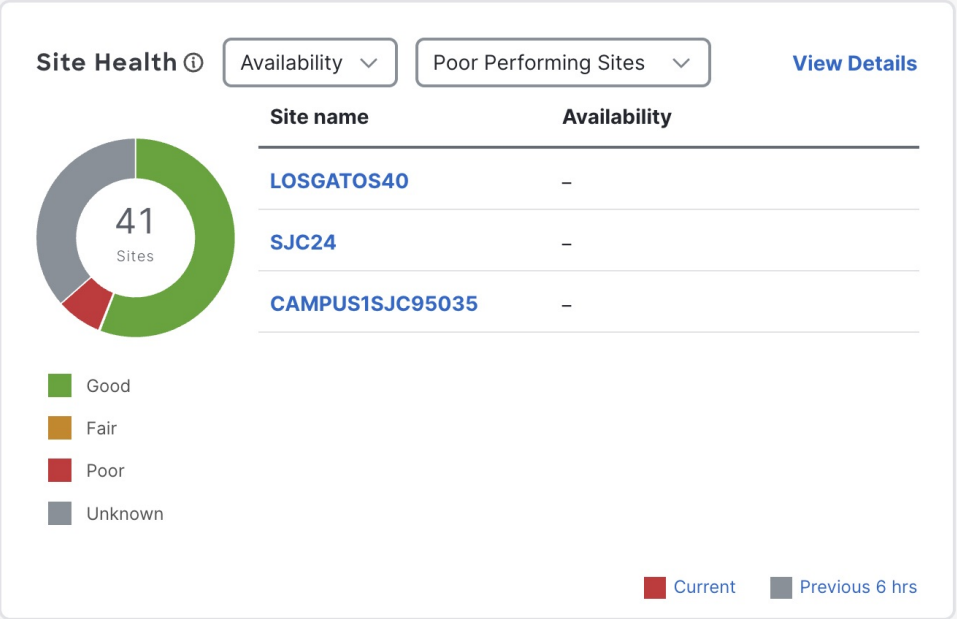
Provides an overview of the Site Health dashlet on the Monitor Overview dashboard and describes how it calculates site health, displays bandwidth trends, and supports filtering and detail view options across sites.

Minimum supported release: Cisco vManage Release 20.10.1

You can view the overall health across all sites in the **Site Health** dashlet on the **Monitor Overview** dashboard.

The **Site Health** dashlet displays the health, which is calculated by the average Quality of Experience (QoE) across all sites. The site health depends on the health metrics of devices, tunnels, and applications at that site.

Figure 6: Site health dashlet



Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a bar graph displays the bandwidth usage information for each site, and changes in bandwidth from the last time period. You can filter the view based on health status using the drop-down list for **Good Performing Sites**, **Fair Performing Sites**, and **Poor Performing Sites**.

Click **View Details** to open the site table view window.

View site health in table view

Provides an overview of the sites table view that shows site, device, tunnel, and application health scores, and recent application usage for the last hour, and explains how overall health states map to Good, Fair, and Poor conditions.

Minimum supported release: Cisco vManage Release 20.10.1

In the sites table view you can view the site health, tunnel health, device health, application health, and application usage.

The sites table view displays all the sites by default and the overall health scores for sites, devices, tunnels, and applications. The table also displays the application usage data for the last one hour.

Site health metrics

The average health metric of sites is calculated using these conditions:

Health	Condition
Good	All applications, WAN edge devices, and tunnels are in good state.
Fair	Any one application, WAN edge device, or tunnel in fair state.
Poor	Any one application, WAN edge device, or tunnel in poor state.

View site health in heatmap view

Provides an overview of the heatmap view that displays site health as Good, Fair, or Poor, shows aggregated data for the last three hours, and lets users adjust the time interval to filter site details.

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, the grid of colored squares displays the site health as **Good**, **Fair**, or **Poor**. You can hover over a square or click to display additional details of a site at a specific time. The data shown here in the aggregated dats for the last three hours. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

View sites in global network view

Verify sites, device status, and tunnel health in Global Network View. Use time ranges, filters, search, and region topology, and open site topology, dashboards, and tunnel views to navigate details for monitoring and troubleshooting.

Use Global Network View to visualize sites and tunnels on a global topology, inspect site details, and access topology, dashboards, tunnels, and troubleshooting pages for monitoring and issue resolution.

- Refine visibility with time ranges, health filters, and search, and view multi-region connectivity when available.

Minimum supported release: Cisco vManage Release 20.11.1

> **Note**
>
> From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is called **Control Components**.

You can view sites in the global topology view by clicking the drop pin icon on the **Monitor Overview** dashboard.

You can view all the WAN edge devices and sites for geographical regions worldwide. Aggregated sites show the number of sites. The color of the aggregated site shows the site health.

Note

For a new deployment, Cisco Catalyst SD-WAN Manager may take up to 30 minutes to populate the Global Network View based on when Cisco Catalyst SD-WAN Manager collects and processes the site health information from all the WAN edge devices in the overlay.

In the **Global Network View** page, the alarms heatmap does not appear for the last 30 minutes, which is the default selection. To view the alarms heatmap, select any of the other time range values from the drop-down list.

Before you begin

You must configure the latitude and longitude on the routers to view the sites in the corresponding geographical location on the map.

Follow these steps to view sites and site health in Global Network View:

Procedure

1. Click the drop pin icon on the **Monitor Overview** dashboard to open the global topology view.

   You can view all the WAN edge devices and sites for geographical regions worldwide.

2. Click an individual site to view site details in the side pane.

   Site details such as **Hostname**, **Site ID**, **Device Model**, **System IP**, **Health**, **Reachability**, and more are displayed.

   Aggregated sites show the number of sites, and the aggregated site color shows the site health.

   When you click the troubleshooting options available in the side pane, Cisco Catalyst SD-WAN Manager displays the relevant troubleshooting pages.

3. Click **Site Topology** to view the site topology of a specific site.
4. Click **Site Dashboard** to view a specific site dashboard.
5. Click **View Tunnels** in the side pane to see the tunnels associated to a specific site.

   Click a tunnel line to view detailed tunnel information. Click the back button to return to Global Network View.

6. Filter the global topology view by site health using the **Good**, **Fair**, and **Poor** options.
7. Select a time range of 30 minutes, 1, 3, 6, 12, or 24 hours.

   If you select any option other than 30 minutes, you can view the heatmap view of the site health.

8. Use the search option to filter sites based on configuration groups, policy groups, tags, and similar criteria with the **Contains** and **Match** options.
9. Click the summary icon to display the topology view of site and tunnel health across geographical locations.

   Click the non-zero number in the topology view to view the site and tunnel health details. If you click the eye icon, you can view the tunnel connection with aggregated tunnel health between the sites.

10. Click the arrow on the left to open the network hierarchy menu, then click a site to view details in the side pane.

    You can view these details for control components or WAN edge device details for the selected site:

    - **Device Health**

- **Reachability**
- **BFD**
- **Controller Control**
- **CPU Load**
- **Memory Utilization**
- **Device Model**
- **System IP**
- **Configuration Group**
- **Policy Group**

If a device from the site is attached to a configuration group or policy group, click the configuration group or policy group to view or modify the configurations.

11. Click **Create a trace** to start a new Network-Wide Path Insight trace.

    The Network-Wide Path Insight feature is integrated with the global network view and it is supported only on WAN edge devices. With the Network-Wide Path Insight feature, Cisco Catalyst SD-WAN Manager lets you initiate application tracing and displays the trace results collected from multiple devices in a consolidated view. For more information, see Start a New Trace.

    To view more information about the trace, click **Insight Summary**. The **Insight Summary** window displays information about the trace from this site from the last 24 hours, including the number of traces, trace start time, and trace stop time. The traffic flow for applications and events is displayed in a pie chart. The application distribution, the event distribution, and event impacts to application are also displayed on this window. There are four events that are displayed in this page: Local Drop, WAN Loss, SLA Violation and Qos Congestion.

    To start another trace, click **Start a New Trace** from the **Insight Summary** page. To view Network-Wide Path Insight details, click **NWPI Details**.

12. If Multi-Region Fabric is enabled, click **Region** to display the regional topology.

    The topology diagram shows the access regions and the core region, indicating the number of border sites and edge sites in each access region. For access regions that have a border router providing connectivity to the core region, the diagram shows a link between the access region and the core region.

    Click a region in the diagram to show which other regions it has connectivity to through the core region—links to those regions are highlighted.

    Click a link between an access region and the core region to display BFD session information related to connections between the two regions, similar to the information provided by the **show sdwan BFD sessions** command.

13. Click a troubleshooting option in the side pane to open the relevant troubleshooting pages.

    When you click the troubleshooting options available in the side pane, Cisco Catalyst SD-WAN Manager displays the relevant troubleshooting pages.

The Global Network View displays sites and tunnel health, and you can open site details, topology, dashboards, and tunnels. Time ranges, filters, and search refine visibility, and regional topology shows inter-region connectivity and related BFD session information when available.

Security

Provides an overview of the Security dashboard, including available dashlets by release and Actions menu options, with notes about dashboard location changes and minimum supported software versions.

List dashlets and options on the **Monitor** > **Security** page in Cisco SD-WAN Manager. Identify availability by release, minimum supported versions, and capabilities of the **Actions** menu.

Dashlets

Table 3: Dashlets

Dashlet Name	Version
Actions	Cisco vManage Release 20.11.1 and later releases
Top Threats	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
Firewall Rule Counter	Cisco vManage Release 20.6.1 and earlier releases **Note** Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases, **Firewall Enforcement** is renamed to **Firewall Rule Counter**.
URL Filtering	Cisco vManage Release 20.6.1 and earlier releases
Advanced Malware Protection	Cisco vManage Release 20.6.1 and earlier releases
Intrusion Prevention	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
SIG/SEE Tunnels	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
Security Events	Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases
Security Appliance/UTD Container	Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases
Application Offload	Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases

Actions

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1.

The **Actions** drop-down list in the security dashboard includes these options:

Table 4: Actions

Option	Description
Edit Security Dashboard	Choose this option to edit the security dashboard. You can perform these actions: • Rearrange: Drag and move the dashlets within the security dashboard. • Delete: Click **Delete** to delete a dashlet.
Show SecureX Ribbon	Click **Show SecureX Ribbon** to view the **SecureX** ribbon in the security dashboard. You can use the **SecureX** ribbon to access the **SecureX** portal from the security dashboard. For more information, SEE View SecureX Ribbon.
Reset to Default View	This option is displayed if you have edited the security dashboard page. Click this option to revert to the default view of the security dashboard.

View top threats

Verify top threats in the Top Threats dashlet and drill down for details. Use View Details, Devices Impacted, and Last Occurrences to see file, signature, device-level, and recent event information.

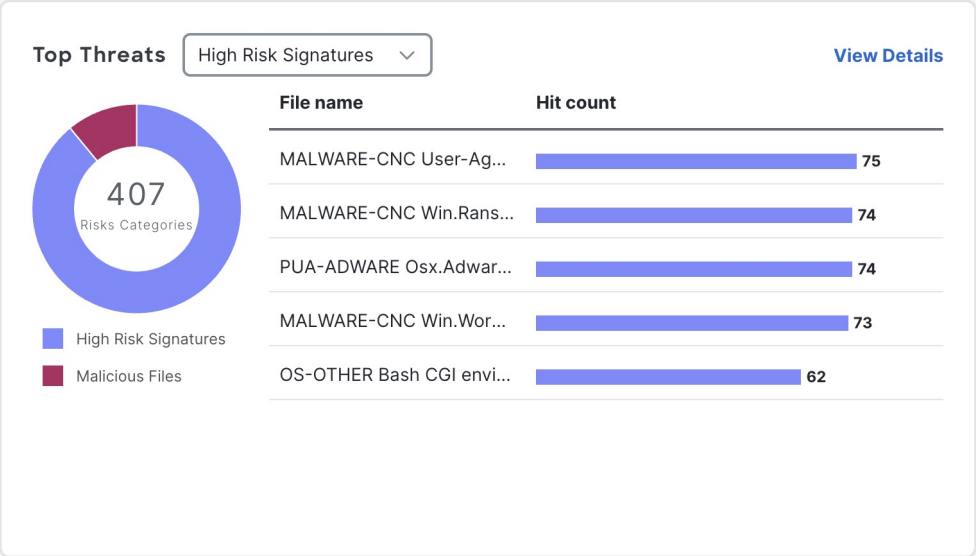
The **Top Threats** dashlet provides a high level view of top five threats found in the network-based on Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) data. You can view the threat information for malicious files or high risk signatures by choosing from the options in the **Top Threats** drop-down list.

Before you begin

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

Procedure

1. Click **View Details**.



View more information about the threats such as file name, type of event, device name, and more.

2. Click a device number in the **Devices Impacted** column.

   View the threat details at a device level.

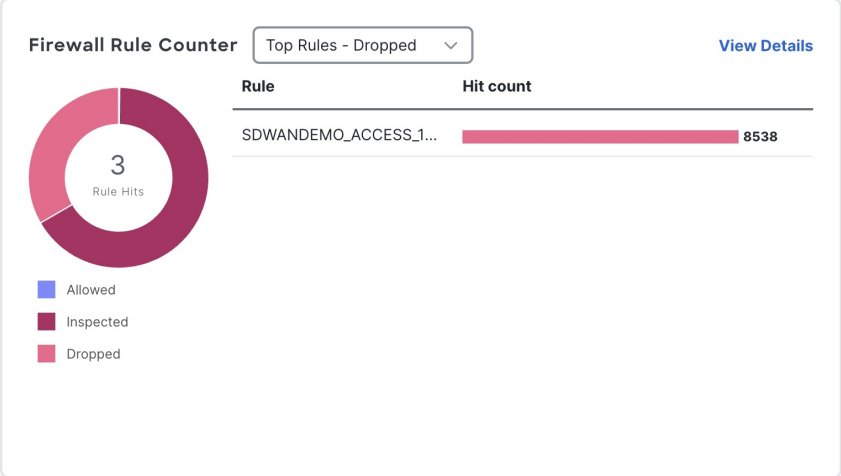
3. Click an entry in the **Last Occurrences** column.

   View additional information about the most recent event.

View firewall rule counter

Provides reference information for the Firewall Rule Counter dashlet in Cisco vManage. It displays per-rule hit counters, supports viewing top allowed, inspected, or dropped rules, and enables access to rule details and device-level hit data.

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.



The **Firewall Rule Counter** dashlet counts the hits on each rule and displays the counters for each rule. Choose the options in the **Top Rules** drop-down list to view the top five rules according to traffic that was allowed, inspected, or dropped.

Click **View Details** to view additional details for a rule. Click a device number in the **Device Hits** column to view the rules at a device level.

Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for data traffic inspection. Zone-based firewalls allow inspection of TCP, UDP, and ICMP data traffic. A zone can contain a group of one or more VPNs. Grouping VPNs into zones allows users to establish security boundaries in the overlay network so that users can control all data traffic that passes between zones.

A firewall policy defines the conditions that the data traffic flow from the source zone must match to allow the flow to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged.

View intrusion prevention details

Verify intrusion prevention information in the dashboard and access details for threats, signature IDs, impacted devices, and last occurrences to investigate events and link to Talos Snort rule references.

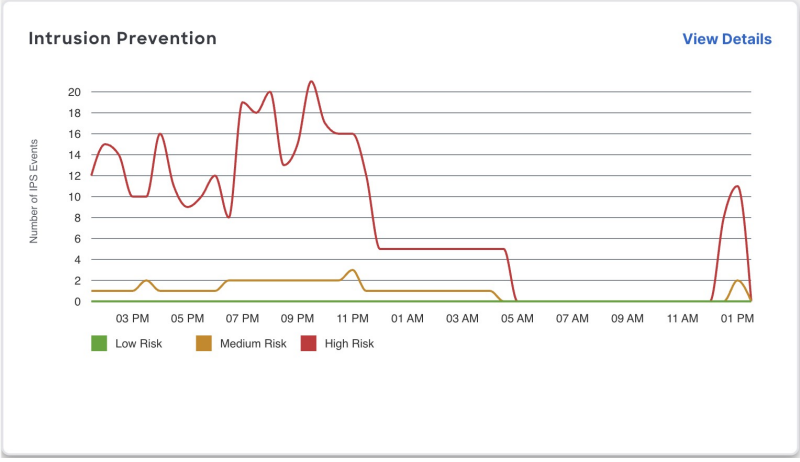
The **Intrusion Prevention** dashlet displays threats that are categorized as low risk, medium risk, and high risk threats.

Before you begin

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

Procedure

1. Click **View Details** to view more details about a threat.



2. Click an entry in the **Signature ID** column to be directed to the Talos website, which will display the Snort rules that are used to report vulnerabilities.
3. Click a device number in the **Device Impacted** column to view more details about the threats at a device level.
4. Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

View URL filtering categories

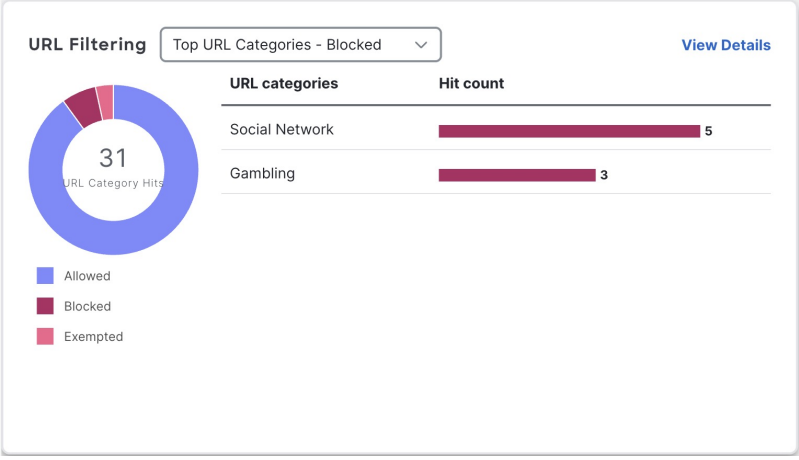
Verify URL filtering insights in the Dashboard by selecting Top URL Categories, viewing details, and drilling down to device-level access. This helps assess allowed, blocked, and exempted categories, including the Exempted category in supported releases.

The URL Filtering dashlet summarizes permitted, blocked, and exempted URL categories and supports filtering and drill-down for additional detail.

Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new URL filtering category, **Exempted**, has been added to the **URL Filtering** dashlet.

Procedure

1. Choose an option in the **Top URL Categories** drop-down list to filter the URL categories and view information about a particular URL category.



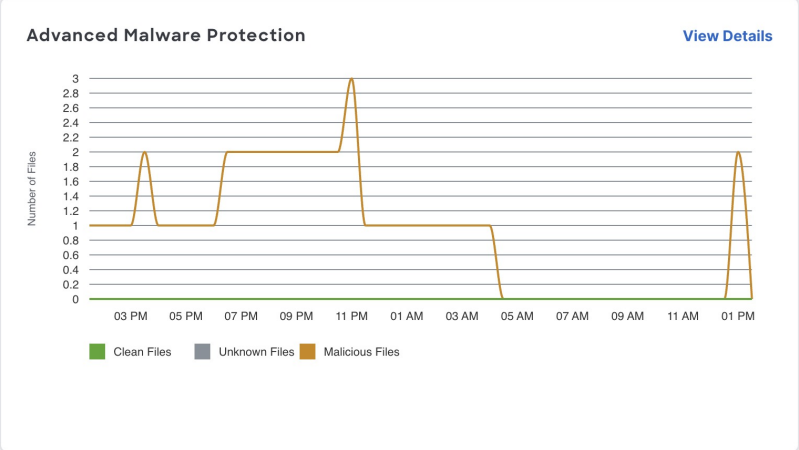
2. Click **View Details** to view more information about the URL categories.
3. Click a device number in the **Device Accessed** column to view additional details for a URL category at a device level.

View advanced malware protection

Provides an overview of the Advanced Malware Protection dashlet that reports counts of malicious, unknown, and clean files over a selected period, and offers links to detailed file, device, and recent event information.

The **Advanced Malware Protection** dashlet displays the number of malicious files, unknown files, and clean files that AMP has identified over a specific time period.

Cisco Advanced Malware Protection (AMP) blocks malware based on file reputation and uploads unknown files to Cisco AMP Threat Grid for further analysis. This pane shows the number of file reputation and file analysis events over the specified time period.



> **Note**
>
> Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new category **Clean Files** hase been added to the **Advanced Malware Protection** dashlet.

Click **View Details** to view an analysis of the files. Click a device number in the **Device Impacted** column to view additional details about the files at a device level.

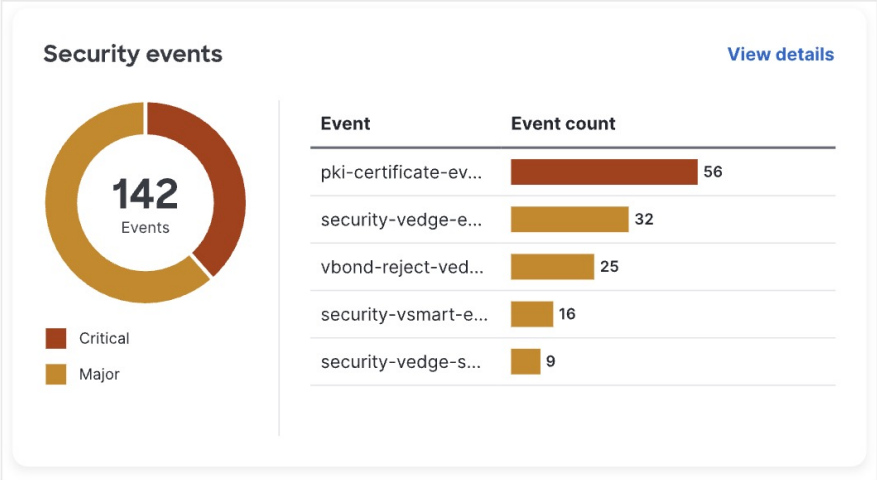
Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

View security events

Provides an overview of the Security Events dashlet, which counts security events in the overlay and classifies them as major or crucial, and identifies the minimum supported release. It also explains how to open detailed information for individual events.

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Security Events** dashlet displays a count of all security events that have occurred within the Cisco Catalyst SD-WAN overlay, and classifies them either major or crucial. Click **View Details** to view additional details about the security events.



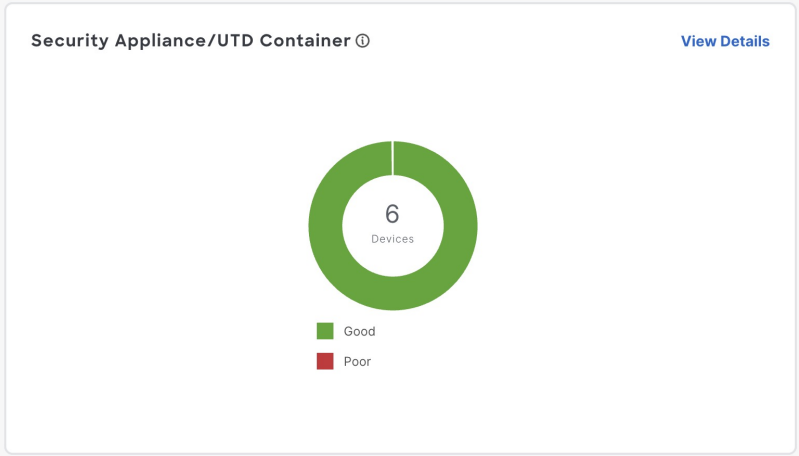
View security Appliance/UTD container

Provides an overview of the Security Appliance/UTD Container dashlet that reports NGFW and security process health, container state, IPS signature updates, and cloud connectivity status, with color-coded health indicators and a link to detailed views.

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1.

The **Security Appliance/UTD Container** dashlet displays the health status of the Next-Generation Firewall (NGFW) and the security processes running on the Cisco IOS XE Catalyst SD-WAN devices.

If everything is functioning properly, the health status is displayed in green. When issues arise with two or more components, the status is displayed in red.



The dashlet provides an overview of various security components and monitors these items:

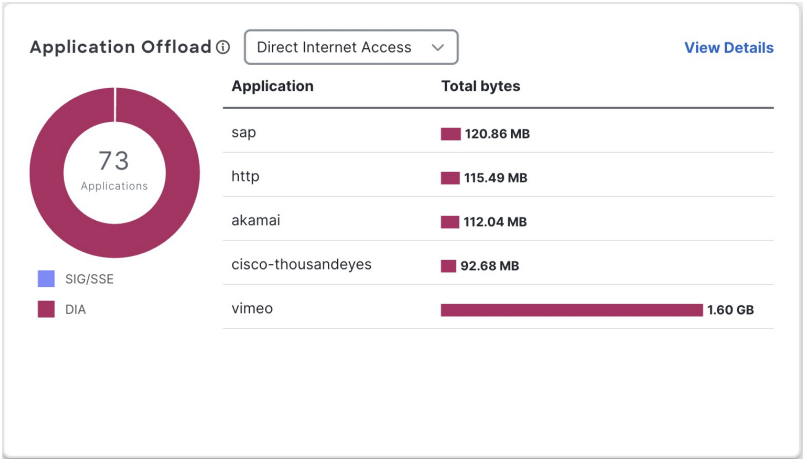
- Device security health
- Operational state of the UTD container
- IPS signature update status
- Cloud connectivity for:
  - URL filtering
  - Advanced Malware Protection

To view more information about the health status of **Security Appliance/UTD Container**, click **View Details**.

View application offload

Provides an overview of the Application Offload dashlet, which displays application traffic by SIG/SSE tunnels or DIA. It visualizes data with doughnut and bar charts and offers a View Details option for deeper insights.

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1.



The **Application Offload** dashlet provides a high-level overview of the application traffic. You can view the application traffic information by choosing SIG/SSE tunnels or DIA options from the drop-down list.

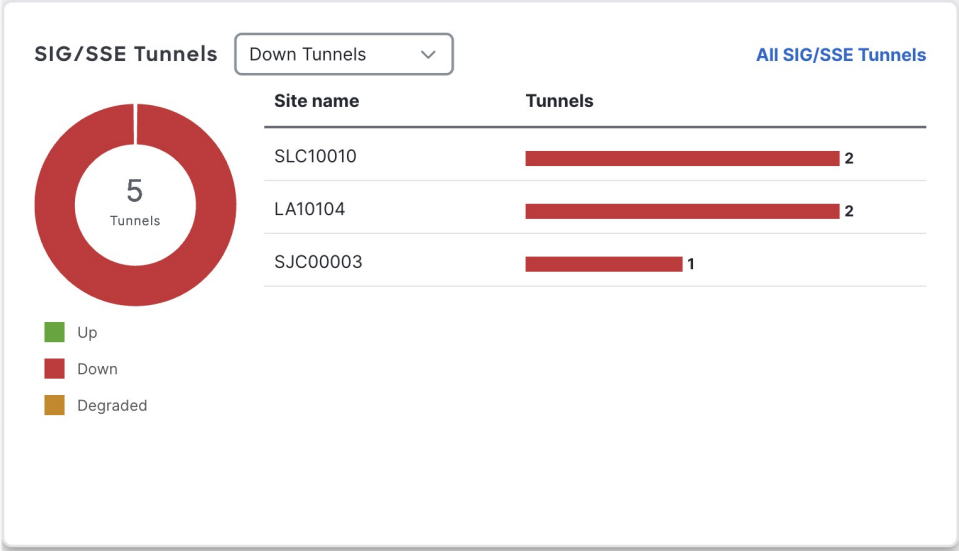
The **Application Offload** dashlet represents the application traffic information using a doughnut chart and a bar chart. While the doughnut chart displays a breakup of the applications by SIG or Secure Service Edge (SSE) tunnels or DIA, the bar chart displays the top five applications in descending order of usage based on the option chosen from the drop-down

list. Hover the mouse pointer over the chart elements to view the names and values that are associated with each application.

To view more information about the applications, click **View Details**.

View Secure Internet Gateway/Secure Service Edge tunnels

Provides an overview of Secure Internet Gateway tunnels in the dashlet, including counts, status (up, down, degraded), and site names, and directs users to All SIG Tunnels for additional configuration details.



Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1.

The **Secure Internet Gateway Tunnels** dashlet provides information about the number of Secure Internet Gateway (SIG) tunnels, their status, whether they are up, down, or degraded, as well as the site names of the tunnels that are being reported.

Click **All SIG Tunnels** to view additional details of the configured SIG tunnels.

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

You can view information about Secure Service Edge tunnels, their status, whether they are up, down, or degraded, as well as the site names of the tunnels that are being reported.

Click **All SIG/SSE Tunnels** to view additional details of the configured Secure Service Edge tunnels.

Note

When you delete a tunnel group on Cisco SD-WAN Manager and Cisco SD-WAN Manager fails to send the delete request to Cisco Secure Access, then the tunnel group on Cisco Secure Access is not active again. The work around for this is to delete the tunnel groups manually on Cisco Secure Access.

View the SecureX ribbon

Verify access to the SecureX ribbon from the security dashboard and complete initial SecureX setup to enable portal integration today. This ensures that configured applications are available and the ribbon is visible after authentication.

Starting with Cisco Catalyst SD-WAN Manager Release 20.12.6, the SecureX ribbon is no longer available in the Cisco SD-WAN Manager.

When you click **Show SecureX Ribbon** for the first time, the **SecureX Setup** dialog box is displayed.

Before you begin

To access the SecureX portal, log in with your registered user credentials.

Procedure

1. From the **Current Region** drop-down list, choose a region for access to the SecureX portal.
2. Click **Enable SecureX** to enable your access to the SecureX portal.

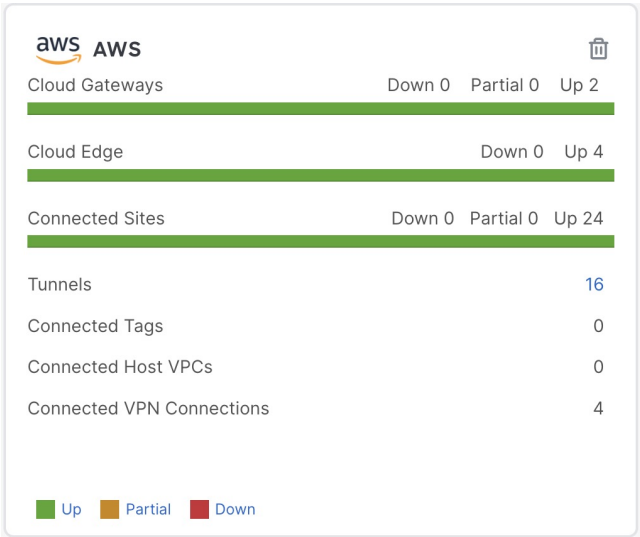
   A validation code appears.
3. Click the **here** hyperlink to proceed with the authentication steps for SecureX.

Multicloud

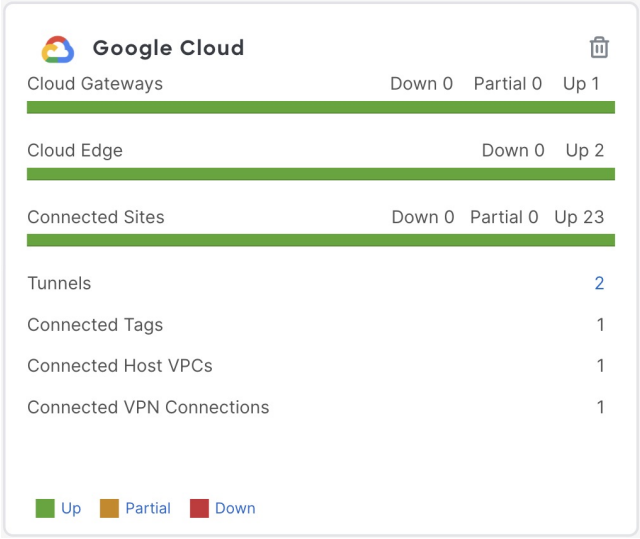
Lists the panes available on the Monitor Multicloud page, including Amazon Web Service, Google Cloud Platform, Microsoft Azure, Megaport, and Equinix. Provides a note that earlier releases place these panes under Dashboard Multicloud.

These panes are available on the **Monitor** > **Multicloud** page in Cisco SD-WAN Manager.

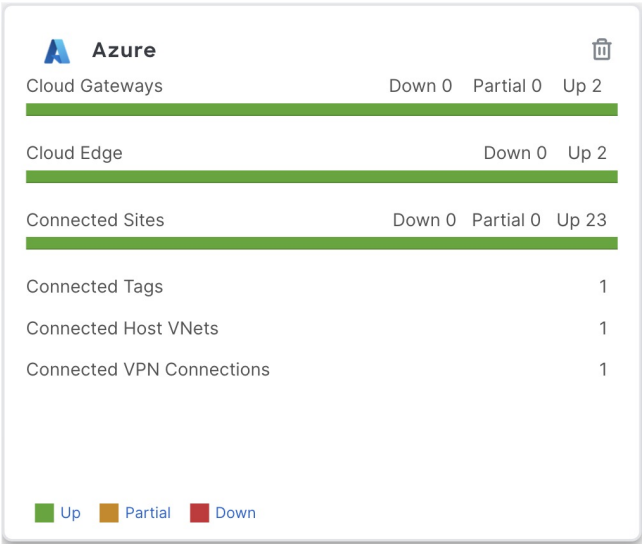
- **Amazon Web Service**



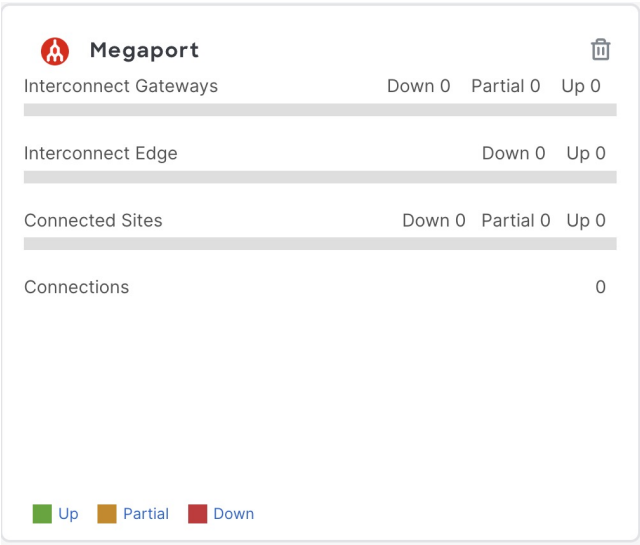
- **Google Cloud Platform**



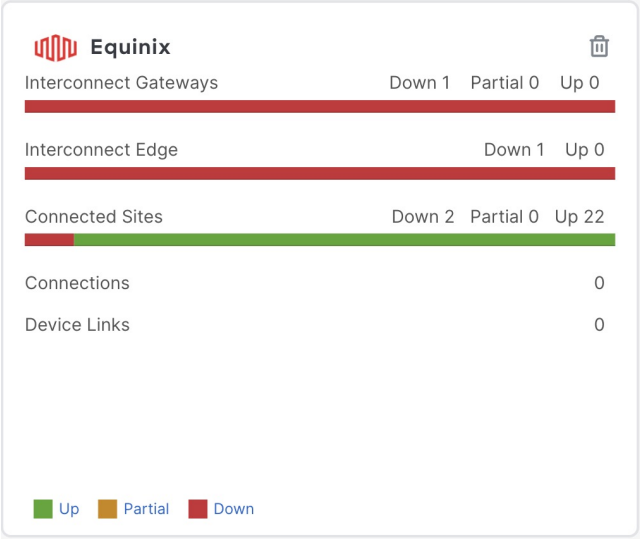
- **Microsoft Azure**



- **Megaport**



- **Equinix**



For more information about these panes, see *Cisco SD-WAN Cloud OnRamp Configuration Guide*.

Access job-role resources from explore

Verify access to Explore in Cisco Catalyst SD-WAN Manager to view resources grouped by job role. Select NetOps, SecOps, AIOps, or DevOps to open relevant features and Cisco resources such as developer guides, APIs, Cisco DNA Center, and Cisco ThousandEyes.

The **Explore** menu option opens a page presenting four job roles–**NetOps**, **SecOps**, **AIOps**, and **DevOps**. Based on the job role that you choose, the Explore page displays relevant Cisco Catalyst SD-WAN features, along with other Cisco resources such as developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more.

The resources appearing in each job role present relevant functionality pertaining to that job role.

Before you begin

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

Procedure

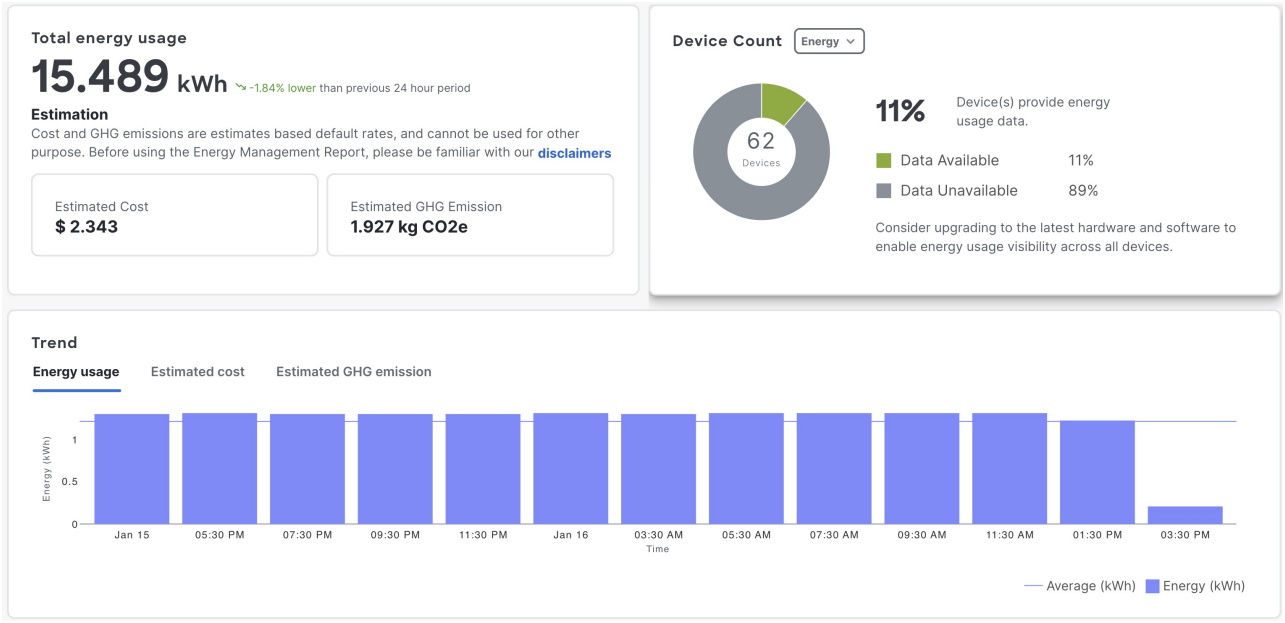
1. From the Cisco SD-WAN Manager menu, choose **Explore**.
2. Click any job role to view and access various resources specific to your choice.
   - **NetOps**
   - **SecOps**
   - **AIOps**
   - **DevOps**

Energy management

Provides an overview of the Energy Management page, listing dashboard panes and descriptions and summarizing enhancements for reporting, offline support, carbon intensity metrics, time period comparisons, and site-to-site analysis.

The **Monitor** > **Energy Management** page is available in Cisco SD-WAN Manager starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a. The table lists the available panes and their descriptions for energy management.

Pane	Description
Total energy usage	Displays total energy (in kWh) used by all devices in the last specified hours.
Device Capability	Displays the number of devices supporting power tracking, with Energy or Cost and Emission filters.
Energy usage trend	Displays power usage trend for the last specified hours, aggregated at intervals.
Consumption by sites	Displays site-based power consumption with a pie chart and detailed table.
Comparison	Displays energy usage comparison between two time periods.



Note

Enable Cloud Services to see **Total energy usage**, **Device Capability**, **Energy usage trend**, **Consumption by sites**, and **Comparison** data.

Energy management dashboard enhancements

The energy management dashboard includes enhancements to help users monitor, analyze, and optimize energy consumption within Cisco SD-WAN Manager starting from Cisco Catalyst SD-WAN Manager Release 26.1.1.1.

- Energy management reporting – improved reporting capabilities allow you to generate energy management reports using a new template in PDF or CSV format.
- Offline-mode support displays static data for key metrics when there is no cloud connectivity.
- Carbon intensity metrics introduce carbon intensity insights for better sustainability tracking. Carbon intensity is calculated in the backend and shown on the UI for the dashlets.

- Time period comparison enhances the comparison of energy metrics across different time periods.
- Site-to-Site comparisons include all key energy metrics for comparative analysis between sites. In the dashboard multi-site view, you can create a donut chart for data usage, cost, emissions, and carbon intensity.

Supported platforms for energy management

Lists platforms that support energy management for the specified Cisco SD-WAN releases. Content references specify the cEdge and Cisco SD-WAN Manager versions and the supported Catalyst Edge and Industrial Router platforms.

Identify the platforms that support energy management based on the referenced Cisco SD-WAN software versions, and present the supported Catalyst Edge and Industrial Router models.

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a these platforms are supported:

- Cisco Catalyst 8100 Series Edge
- Cisco Catalyst 8200 Series Edge
- Cisco Catalyst 8300 Series Edge
- Cisco Catalyst 8500 Series Edge

From Cisco Catalyst SD-WAN Manager Release 26.1.1.1 these platforms are supported:

- IR1101
- IR1821
- IR1831
- IR1833
- IR1835
- IR8140H
- IR8140H-P
- IR8340
- ESR6300
- vedge-ESR-6300-LIC
- vedge-ESR-6300-NCP

Generate energy management report

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports** > **Reports**.
2. Click **Report Templates**.
3. In the **Report Templates** page, choose a **Energy management report** card and click **Generate**.

   The Energy management report window appears.
4. In the Energy management window, enter the name of the report in the **Report name** field.
5. Choose sites from the **Sites** drop-down list.
6. Choose the **File type**.

- **CSV**
- **PDF**

7. Choose the **Time range**.
8. Choose the **Schedule**.
   - **Run now**
   - **Run later (one-time)**
   - **Run recurring**
9. (Optional) Choose the **Delivery method**.

   You can enter up to 5 email addresses in the **Email** field.

A new energy management report is created in the specified format and are available in the **My reports** tab. Reports are also delivered to the email addresses mentioned. For more details on the Reports, see Reports.

Converged dashboard for SD-WAN analytics and SD-WAN manager

Provides a concise overview of the converged dashboard that unifies SD-WAN Analytics and SD-WAN Manager, outlining its purpose and scope for centralized visibility and control in a single interface.

Converged dashboards

Explains the converged dashboard that integrates analytics with manager views, renders Analytics pages within the interface, and presents reports and dashlets, with access dependent on onboarding and administrative settings within the system.

A converged dashboard is a SD-WAN dashboard that

- integrates analytics and manager data within a single interface
- renders Analytics pages inside the manager.

Access, pages, and reports in converged dashboard

Access the converged dashboard in Cisco SD-WAN Manager.

From Cisco Catalyst SD-WAN Manager Release 20.15.1, a converged dashboard is available that integrates data from both Cisco SD-WAN Analytics and Cisco SD-WAN Manager within a single interface. To access this converged dashboard, Cisco SD-WAN Analytics must be onboarded into Cisco SD-WAN Manager.

The converged dashboard renders Analytics pages within Cisco SD-WAN Manager in these menus:

- Under the **Overview** menu: the pages for **Applications**, **Sites**, and **Circuits** are rendered.
- Under the **Analytics** menu: all menus are rendered except for **Internet Outages**.
- Under the **Logs** menu: the **Traffic Logs** page is rendered.

For more information about onboarding Cisco SD-WAN Analytics into Cisco SD-WAN Manager, see Onboard Cisco SD-WAN Analytics.

If Cisco SD-WAN Analytics is onboarded to Cisco SD-WAN Manager, the **Cloud Services** option in the **Administration** > **Settings** is enabled automatically. This means that a converged dashboard is available in Cisco SD-WAN Manager.

To disable Cisco SD-WAN Analytics, change its status to Disabled (or toggle the switch off).

View Cisco SD-WAN Analytics data in Cisco SD-WAN Manager.

When Cisco SD-WAN Analytics is enabled, the dashboard in Cisco SD-WAN Manager displays data from Cisco SD-WAN Analytics, including details on Applications, Circuits, Sites, and Clients through specific dashlets. You can click these dashlets for more detailed information instead of being redirected to Cisco SD-WAN Analytics.

View reports in converged dashboard.

All Applications Reports, which is a Cisco SD-WAN Analytics report, displays a view of how different applications are performing across an overlay for all sites. The **Executive Summary** report in the converged dashboard displays the same Executive Summary report as seen in the standalone Cisco SD-WAN Analytics when it is not part of the convergence. For more reports in Cisco SD-WAN Manager, see Information About Reports.

Applications dashboard

Provides an overview of application performance across the overlay and individual sites in the Applications dashboard, with widgets for Application Experience, trend analysis, QoE distribution by application classes, and trending applications, plus a visual and link to related documentation.

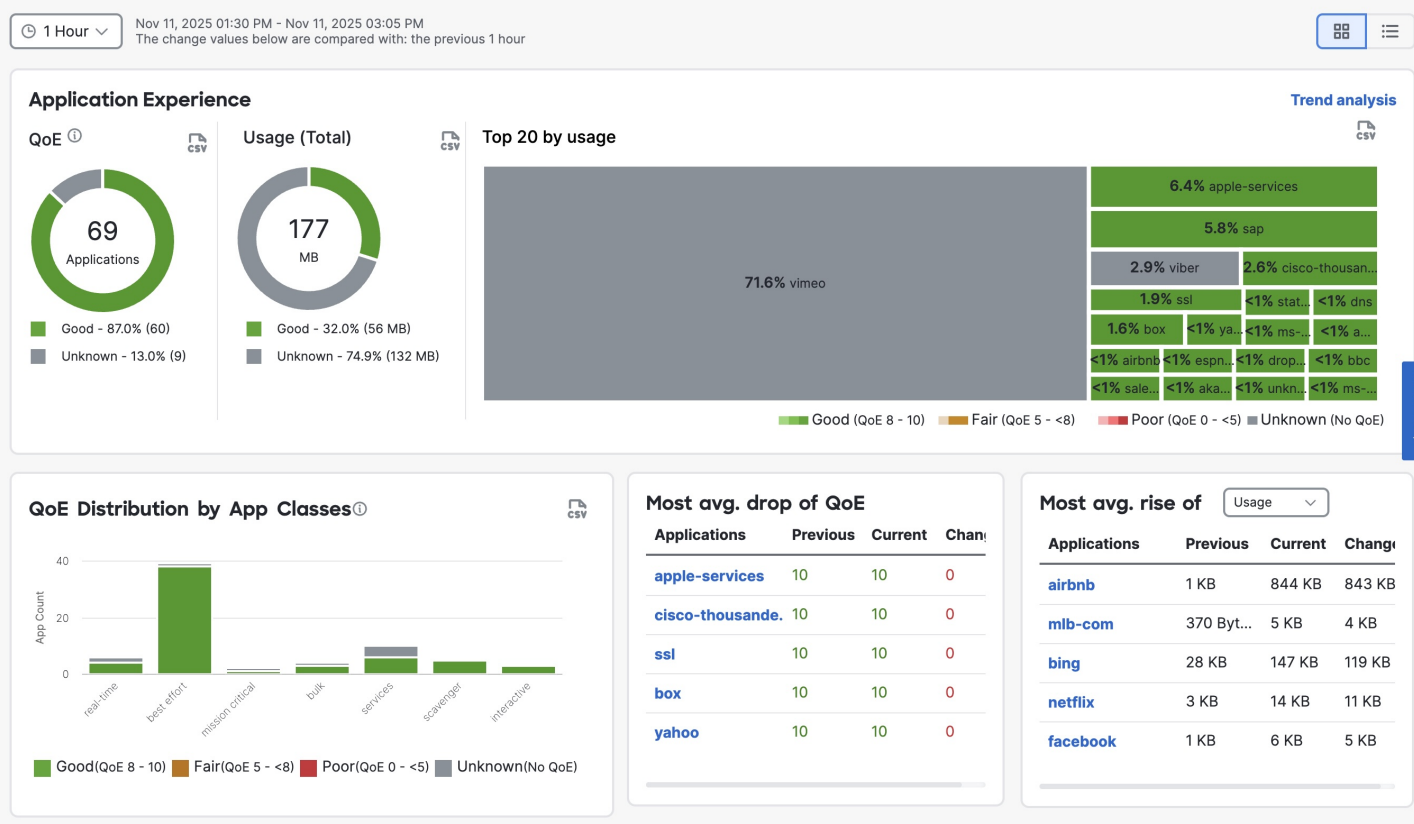
The **Applications** dashboard displays information on how different applications are performing across an overlay for all sites, and for a single site. The **Applications** dashboard gives an overview of Application performance for all applications across an overlay and across all sites, and compares it to other metrics such as overall bandwidth and bandwidth increase.

The **Applications** dashboard presents the performance metrics in these widgets:

- Application Experience
- Application Trend Analysis
- QoE Distribution by Application Classes, and
- Trending Applications

This is the Applications dashboard:

Figure 7: Application experience



For more information about the **Applications** dashboard, see Application Dashboard in Cisco SD-WAN Analytics.

> **Note**
>
> The **Applications** dashboard displays Cisco SD-WAN Analytics data only when viewed on a converged dashboard.

Sites dashboard

Provides visibility into site availability, utilization, and latency across the network for a selected time period. Provides comparative insights by contrasting current site performance with metrics from the previous period and links to Sites analytics details.

The **Sites** dashboard provides visibility into site availability and usage across the entire network for the selected time period. The **Sites** page helps you to view the performance of applications on the overlay from a site perspective. It provides the ability to view overlay performance in terms of sites and provides insights into site performance in terms of availability, utilization and latency, and compares these parameters with the corresponding metrics from the previous time period.

For more information about Sites analytics, see Site Dashboard in Cisco SD-WAN Analytics.

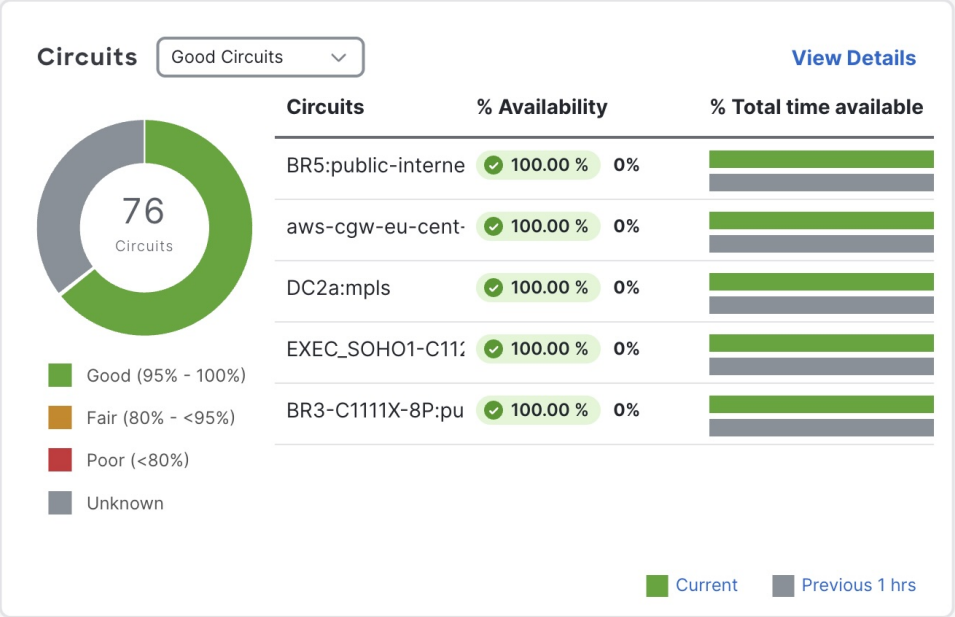
Circuits dashboard

Provides insights into circuit availability, utilization, and network performance across the fabric and at individual sites. Summarizes overall and per-site metrics through the Circuits dashboard to help assess health and identify issues quickly.

The **Circuits** dashboard provides valuable insights into circuit availability, utilization, and network performance. It offers a comprehensive overview of circuit performance across the entire fabric as well as for individual sites.

This is the Circuits dashlet:

Figure 8: Circuits

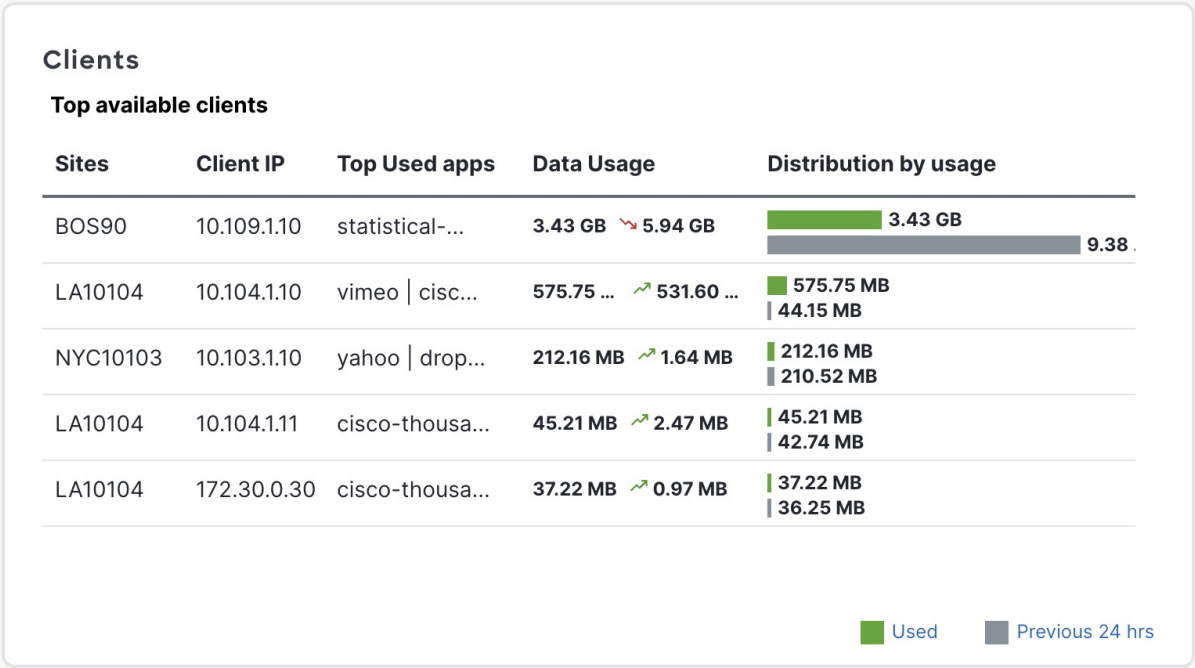


For more information about Circuits analytics, see Circuits Dashboard in Cisco SD-WAN Analytics.

Client dashlet

Provides an overview of the Clients dashlet, which displays top clients in the overlay, current data usage, changes since the last period, and the top five applications ranked by bandwidth.

The **Clients** dashlet displays the top clients of data in the overlay, the current usage of data and the changes in the usage of data from the last time period. The top clients are tracked by using respective client IP addresses in the overlay network. The dashlet also displays the top five applications that are used by the clients, and the data is ranked by bandwidth.



Note

The **Clients** dashlet is not available by default. To view the **Clients** dashlet, you must add the dashlet. For more information about adding dashlets, see Add a dashlet on page 17.

2 Monitor Devices and SD-WAN Control Components

Topics:

- Feature history: Monitor devices and SD-WAN Control Components
- Devices and controllers
- Geographic location of devices
- Set map filters
- Viewing device information
- Configure geographic coordinates for a device
- View system status
- View device system resource utilization in Cisco SD-WAN Manager
- View device system resource utilization using the CLI
- Open a TAC case
- Viewing the status of a Cisco Catalyst SD-WAN Validator
- Viewing the status of a Cisco Catalyst SD-WAN Controller
- View control connections
- View devices connected to Cisco Catalyst SD-WAN Manager
- View services running on Cisco Catalyst SD-WAN Manager
- Viewing device status in the overlay network
- Viewing device information
- View device configuration
- View the software versions installed on a device
- View device interfaces
- Viewing WAN interfaces
- View interfaces in the management VPN or VPN 512
- View DHCP server and interface information
- View interface MTU information
- View and monitor cellular interfaces
- View colocation cluster information
- View Cisco Colo Manager health
- View Cisco Catalyst SD-WAN Manager cluster information using the CLI
- Viewing QoS statistics

Monitor Devices and SD-WAN Control Components.

Feature history: Monitor devices and SD-WAN Control Components

Feature history for monitoring devices and SD-WAN Control Components.

Developments in monitoring devices and SD-WAN Control Components, by release.

Table 5: Feature history

Feature name	Release information	Description
Data Plane CPU and Memory Utilization	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a; Cisco Catalyst SD-WAN Manager Release 20.16.1	Monitor data plane CPU and memory utilization on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
QoS statistics for interfaces and tunnels	Cisco Catalyst SD-WAN Manager Release 20.18.1	Monitor traffic across network interfaces and tunnels with real-time and historical statistics, including class-level traffic insights and per-tunnel QoS statistics.
One Minute Granularity for Interface Statistics	Cisco IOS XE Catalyst SD-WAN Release 26.1.1; Cisco Catalyst SD-WAN Manager Release 26.1.1.1	Collect granular interface statistics for devices every minute for real-time troubleshooting and performance analysis.

Devices and controllers

Information about Cisco Catalyst SD-WAN devices and control components.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

Geographic location of devices

Information about the geographic location of Cisco Catalyst SD-WAN devices and links in the overlay network.

Information about the geographic location of Cisco Catalyst SD-WAN devices and links in the overlay network.

The Geography page displays a map of the geographic location of Cisco Catalyst SD-WAN devices and links in the overlay network.

The browser running SD-WAN Manager must have internet access. If it does not, ensure that the browser can access openstreetmap.org.

To view device locations, from the **VPN Group** list select a VPN group, from the **VPN Segment** list select a VPN segment, and set filters.

Set map filters

Set filters to control the devices and connection states displayed on the Geography page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Select **Filter**.
3. Select the device group. **All** displays all devices and **No Groups** displays devices that are not in a group.
4. Select the device types to display.
5. Select the control and data-link states to display.
6. Move the pointer outside the Filter box to close it. The map updates dynamically.

Viewing device information

Information about viewing device details and connection states on the Geography page.

Information about viewing device details and connection states on the Geography page.

Hover over a device icon to display its system IP address, hostname, site ID, device type, and status. Select the device icon twice to open the **View More Details** page, then select **Device Dashboard**, **Device Details**, **SSH Terminal**, **Site Topology**, or **Links**. Thin, bold, dotted, and gray lines identify active, multiple, down, and consolidated control or data connections. Hover over a line to view its state.

Configure geographic coordinates for a device

Configure the latitude and longitude used to display a device on the Geography page.

Procedure

1. Use the System Feature template under **Configuration** > **Templates** to configure coordinates. If the device is not attached to a configuration template, use **Tools** > **SSH Terminal** and select the device.
2. Use **show system status** to check **vManaged** and **Configuration template**.
3. For an unmanaged device, enter configuration mode with **config** on a Cisco vEdge device or **configure-transaction** on a Cisco IOS XE Catalyst SD-WAN device.
4. Configure the latitude and longitude with **system gps-location latitude degrees.minutes.seconds** and **gps-location longitude degrees.minutes.seconds**, then save the configuration with **commit**.

Device-location priority is GPS, geo-fencing, manual configuration, then system default. Site-location priority is network hierarchy, the first device in the site, then the geographical view.

View system status

View status information for a selected device or controller.

The **System Status** page displays reboot and crash counts, hardware component status for modules, temperature sensors, USB, power supplies, and fans, and CPU and memory usage for selected time periods. A green check mark indicates an operational component, a red circle with an X indicates a down component, an orange triangle indicates an error, and N/A indicates that the component does not apply to the selected device.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco SD-WAN Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select a device. A Cisco vEdge device displays **System Status** by default. For a Cisco IOS XE Catalyst SD-WAN device or controller, select **System Status** in the left pane.

View device system resource utilization in Cisco SD-WAN Manager

View CPU, memory, and power-usage details for a device or controller.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a Cisco IOS XE Catalyst SD-WAN device or controller.
3. Select **System Status** in the left pane.
4. On the **System Status** page, view control-plane CPU and memory, data-plane CPU and memory, and power usage in the **CPU & Memory** pane.
5. Select **Real Time**, a predefined period, or a custom period.

The SD-WAN Manager page displays CPU and memory utilization for the selected duration. Devices collect utilization data every 10 seconds. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, the graph includes data-plane CPU and memory statistics and historical power-usage data.

View device system resource utilization using the CLI

Use CLI commands to view system, CPU, memory, disk, and QFP resource information.

The **show sdwan system status** command displays system status and CPU-utilization calculations. Before Cisco SD-WAN Release 20.9.1, utilization uses user CPU time. Starting with Cisco SD-WAN Release 20.9.1, utilization uses user and system CPU time.

Procedure

1. Enter **show sdwan system status** on the device.

Example

This example shows system status for Cisco SD-WAN Manager devices.

```
Device# show sdwan system status
System state: GREEN. All daemons up
CPU states: 10.38% user, 1.47% system, 88.04% idle
Memory usage: 32820584K total, 4488868K used, 28331716K free
Disk usage: /bootflash 5%
```

2. For Quantum Flow Processor status, enter **show platform hardware qfp active datapath utilization summary**, **show platform hardware qfp active infrastructure exmem statistics**, or **show platform resources**.

Quantum Flow Processor status includes datapath processing-load statistics, exmem memory statistics, and platform-resource status. Preserve any published sample command output with the command text unchanged in meaning.

Open a TAC case

Open a TAC case from Cisco SD-WAN Manager.

Use SD-WAN Manager to access TAC cases and open a service request in the Support Case Manager portal.

For a SD-WAN Manager troubleshooting issue, open a support case in the Support Case Manager portal. SD-WAN Manager can upload an Admin-Tech file to a specific service request when you provide the service-request number and token. Starting with Cisco vManage Release 20.9.1, you can access the Support Case Manager portal from SD-WAN Manager to create, view, or upload an Admin-Tech file.

Active Cisco single sign-on credentials are required to access the Support Case Manager wizard and cloud server.

Procedure

1. From the SD-WAN Manager menu, choose **Tools** > **TAC Cases**.
2. On the TAC Support Cases page, select **Open a Case**.
3. Enter the relevant case details.
4. Select **Create**.

The TAC Support Cases page displays the updated list of cases.

What to do next

To view TAC cases, log in to the Support Case Manager portal with Cisco SSO credentials. The TAC Support Cases page displays the case list.

Viewing the status of a Cisco Catalyst SD-WAN Validator

View the status of a Cisco Catalyst SD-WAN Validator by using the Dashboard, Geography, or Devices page.

Use one of these methods to view the status of a Cisco Catalyst SD-WAN Validator.

- View the status of a Cisco Catalyst SD-WAN Validator using the Dashboard page
- View the status of a Cisco Catalyst SD-WAN Validator using the Geography page
- View the status of a Cisco Catalyst SD-WAN Validator using the Devices page

View the status of a Cisco Catalyst SD-WAN Validator using the Dashboard page

View Validator reachability from the Dashboard page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Overview**. For Cisco vManage Release 20.6.1 and earlier, choose **Dashboard** > **Main Dashboard**.
2. For Cisco vManage Release 20.6.1 and later, select the number representing Cisco SD-WAN Validator orchestrators.

   For releases before Cisco vManage Release 20.6.1, select the upward or downward arrow next to **Cisco vBond**.
3. View the **Reachability** column in the page that opens.

View the status of a Cisco Catalyst SD-WAN Validator using the Geography page

View Validator status from the Geography page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Select **Filter**, then select **vBond** under **Types**.
3. Select the Cisco Catalyst SD-WAN Validator icon to view its status.

View the status of a Cisco Catalyst SD-WAN Validator using the Devices page

View Validator status from the Devices page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.1 and earlier, choose **Monitor** > **Network**.
2. Locate the Cisco Catalyst SD-WAN Validator by scrolling or entering Validator in the search bar.
3. Select the Validator under the **Hostname** column. The **Control Connections** page displays its controller connections.

Viewing the status of a Cisco Catalyst SD-WAN Controller

View the status of a Cisco Catalyst SD-WAN Controller by using the Dashboard, Geography, or Devices page.

Use one of these methods to view the status of a Cisco Catalyst SD-WAN Controller.

- View the status of a Cisco Catalyst SD-WAN Controller using the Dashboard page
- View the status of a Cisco Catalyst SD-WAN Controller using the Geography page
- View the status of a Cisco Catalyst SD-WAN Controller using the Devices page

View the status of a Cisco Catalyst SD-WAN Controller using the Dashboard page

View Controller reachability from the Dashboard page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Overview**. For Cisco vManage Release 20.6.1 and earlier, choose **Dashboard** > **Main Dashboard**.
2. For Cisco vManage Release 20.6.1 and later, select the number representing Cisco SD-WAN Controllers.

   For releases before Cisco vManage Release 20.6.1, select the upward or downward arrow next to **Cisco vSmart**.
3. View the **Reachability** column in the page that opens.

View the status of a Cisco Catalyst SD-WAN Controller using the Geography page

View Controller status from the Geography page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Select **Filter**, then select **vSmart** under **Types**.
3. Select the Cisco Catalyst SD-WAN Controller icon to view its status.

View the status of a Cisco Catalyst SD-WAN Controller using the Devices page

View Controller status from the Devices page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.1 and earlier, choose **Monitor** > **Network**.
2. Locate the Cisco Catalyst SD-WAN Controller by scrolling or entering a keyword in the search bar.
3. Select the Controller instance under the **Hostname** column. The **Control Connections** page displays its controller connections.

View control connections

View control connections for a device.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Select a device. For a Validator, Manager, or Controller, the Control Connections page opens by default.
3. For an edge device, select **Control Connections** in the left pane.

   The right pane displays control connections with controller devices.

The upper part of the page displays expected and actual connection counts and a graphical topology. The lower part displays search options and a table. By default, the first six connections are selected for the graph.

View devices connected to Cisco Catalyst SD-WAN Manager

View devices connected to a Cisco SD-WAN Manager server.

Procedure

1. From the SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. Under **Service Configuration**, select the hostname of the desired Cisco SD-WAN Manager server. The Manager Details page opens.
3. Alternatively, for the desired Manager instance under **Service Configuration**, select **...**, then select **Device Connected**.

View services running on Cisco Catalyst SD-WAN Manager

View enabled Cisco SD-WAN Manager services.

Procedure

1. From the SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. Under **Service Configuration**, select the hostname of the desired Cisco SD-WAN Manager server.

The page displays process IDs for the enabled Cisco SD-WAN Manager services.

Viewing device status in the overlay network

View the status of a device in the overlay network by using the Dashboard, Geography, or Devices page.

Use one of these methods to view the status of a device in the overlay network.

- View device status in the overlay network using the Dashboard page
- View device status in the overlay network using the Geography page
- View device status in the overlay network using the Devices page

View device status in the overlay network using the Dashboard page

View WAN Edge reachability from the Dashboard page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Overview**. For Cisco vManage Release 20.6.1 and earlier, choose **Dashboard** > **Main Dashboard**.
2. For Cisco vManage Release 20.6.1 and later, select the number representing WAN Edge devices.

   For releases before Cisco vManage Release 20.6.1, select the upward or downward arrow next to **WAN Edge**.

3. View the **Reachability** column in the page that opens.

View device status in the overlay network using the Geography page

View WAN Edge status from the Geography page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Select **Filter**, then select **WAN Edge** under **Types**.
3. Select the router icon to view its status.

View device status in the overlay network using the Devices page

View WAN edge device status from the Devices page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Locate the WAN Edge router by scrolling or entering a keyword in the search bar.
3. Select the router under the **Hostname** column. The **System Status** page opens by default.

Viewing device information

View basic or detailed information about a device.

Use one of these methods to view basic or detailed device information.

The Devices page displays devices newly added or synchronized through the options on the **Configuration** > **Devices** page from Cisco vManage Release 20.9.2.

- View basic device information
- View detailed device information
- Viewing device health in a table view
- Viewing device health in heatmap view

View basic device information

View basic information for a device on the Geography page.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Hover over the device icon.

3. To view more information, select the device icon twice to open the **View More Details** page, then select **Device Dashboard**, **Device Details**, **SSH Terminal**, or **Links**.

The pop-up displays system IP address, hostname, site ID, device type, and device status.

View detailed device information

View detailed information for a selected device.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Locate the WAN Edge router by scrolling or entering a keyword in the search bar.
3. Select the device under the **Hostname** column. The right pane displays **System Status** by default. Select a category in the left pane to view more details.

Viewing device health in a table view

View device health metrics in a table.

View device health metrics in a table.

Device health metrics in table view

Starting with Cisco vManage Release 20.10.1, the Monitor Device page displays device health for the last hour in table view by default.

The table includes device model, site ID, system IP address, device health, reachability, memory utilization, CPU load, RA session, and RA-session breakdown.

From Cisco Catalyst SD-WAN Manager Release 20.14.1, use the **Remote Access** filter under **Type** to display remote-access devices. Select **All Sites** and a site ID to view one site.

Table 6: Device health metrics

Health state	Reachability	Control plane	Data plane	Resources	Evaluation logic
Good	Device reachable	All control connections up	All BFD tunnels up	CPU and memory below 75%	All attributes met
Fair	Device reachable	At least one control connection up	At least one BFD tunnel up	CPU or memory above 75%	Any attribute met
Poor	Device not reachable	No control connections up	No BFD tunnels up	CPU or memory above 90%	Any attribute met

For one device, Good, Fair, and Poor correspond to QoE values 10, 5, and 0. For the average health metric, Good is at least 6.67, Fair is 3.34 through less than 6.67, and Poor is greater than 0 and less than 3.34.

Viewing device health in heatmap view

View device health as a heatmap.

View device health as a heatmap.

Device health heatmap

Starting with Cisco vManage Release 20.10.1, the heatmap displays device health as Good, Fair, or Poor colored squares.

Hover over or select a square to display device details. Select the time-interval drop-down list to filter data for an interval. Select **All Sites** and a site ID to view one site.

View device configuration

View the running or local configuration for a device.

Procedure

1. From the SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Select **WAN Edge List** or **Control Components**.
3. For the desired device, select **...**, then select **Running Configuration** or **Local Configuration**.

View the software versions installed on a device

View installed software versions for a device.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, select **Software Versions**.

View device interfaces

View status and statistics for device interfaces.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column.
3. Select **Interface** in the left pane.

4. Use **Chart Options**, **IPv4 & IPv6**, **Separated**, and a real-time, predefined, or custom period to control the graph.
5. Use the filter criteria and select or clear interfaces in the table. You can select up to 30 interfaces and rearrange columns. For a cellular interface, select its name for detailed information.

From Cisco IOS XE Catalyst SD-WAN Release 26.1.1, SD-WAN Manager can collect detailed interface statistics every minute for up to 12 hours. Longer periods use the default five-minute interval. Configure the interval using a configuration group or the CLI.

Viewing WAN interfaces

View information about transport interfaces in VPN 0.

Transport interfaces in VPN 0 connect to a WAN such as the Internet, Metro Ethernet, or MPLS. Use one of these methods to view WAN interfaces.

- View WAN interfaces using the Real Time pane
- View WAN interfaces using the Interface pane

View WAN interfaces using the Real Time pane

View WAN interface information from the Real Time pane.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Locate the device by scrolling or entering a keyword in the search bar.
3. Select the device name in the **Hostname** column.
4. On the page that opens, select **Real Time** in the left pane.
5. From the **Device Options** drop-down list in the right pane, select **Control WAN Interface Information**.

Starting with Cisco Catalyst SD-WAN Manager Release 20.12.1, the **Bind Interface** field displays the mapping between loopback and physical interfaces.

View WAN interfaces using the Interface pane

View WAN interface information from the Interface pane.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. From the **Device Groups** drop-down list, select the group to which the device belongs.
3. Select the device name in the **Hostname** column.
4. In the left pane, select **Interface**.

View interfaces in the management VPN or VPN 512

View interface information for the management VPN or VPN 512.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Locate and select the device name in the Hostname column.
3. In the left pane, select **Real Time**.
4. From the **Device Options** drop-down list, select **Interface Detail**.
5. In the **Select Filter** page, select **Show Filters** to use filters, or select **Do Not Filter**.
6. In the search bar, enter 512, which is the management VPN.

CLI equivalent: **show interface vpn 512**

View DHCP server and interface information

View DHCP server and interface information on a device.

A tunnel interface can provide DHCP server or DHCP-helper services for a service-side network.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, select **DHCP Servers** or **DHCP Interfaces**.

Table 7: DHCP device options

Device option	Command	Description
DHCP Servers	**show dhcp server**	View DHCP-server functionality enabled on the device.
DHCP Interfaces	**show dhcp interface**	View interfaces on which DHCP is enabled on an edge device or Cisco SD-WAN Controller.

View interface MTU information

View MTU information for a device interface.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, select **Interface Detail**.

View and monitor cellular interfaces

Monitor cellular-interface status, signal strength, errors, and connections.

Use Cisco SD-WAN Manager or the router LED to verify cellular signal strength and service availability.

Monitor cellular interfaces

You can view the last-seen error message for a cellular interface from Cisco SD-WAN Manager.

Verify signal strength

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. From the **Device Groups** drop-down list, select the group to which the device belongs.
3. Select the device name in the **Hostname** column.
4. Select **Real Time** in the left pane.
5. From the **Device Options** drop-down list, select **Cellular Radio**.

If signal strength is poor or absent, refer to the cellular-interface troubleshooting guidance. CLI equivalent: **show cellular status**.

Verify radio signal strength using the router LED

View the WWAN Signal Strength LED on the front of the router. The LED color and state indicate whether the LTE interface is disabled, active, dormant, or experiencing a critical issue.

Table 8: WWAN Signal Strength LED

Color	Signal strength	State	Description
Off	–	–	LTE interface disabled or not configured.
Green	Excellent	Solid or blinking	LTE enabled in dormant or active mode.
Yellow	Good	Solid or blinking	LTE enabled in dormant or active mode.
Orange	Poor	Solid or blinking	LTE enabled in dormant or active mode.

Color	Signal strength	State	Description
Red	Critical issue	Solid	LTE enabled but faulty, with no BTS connectivity or no signal.

View error messages for cellular interfaces

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column, then select **Real Time** in the left pane.
3. From the **Device Options** drop-down list, select **Cellular Status**.

The output includes a Last Seen Error column. CLI equivalent: **show cellular status**.

View cellular connections

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select the device name in the **Hostname** column, then select **Real Time** in the left pane.
3. From the **Device Options** drop-down list, select **Cellular Connection**.

Table 9: Cellular connection fields

Field	Description
Profile APN	Access-point name for cellular connections.
Up Since	Time since the connection was established.

CLI equivalent: **show cellular <interface> connection**.

View colocation cluster information

View colocation-cluster topology, health, resources, and VNF information.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select **Colocation Cluster**.
3. Select a cluster name to view topology, CPU, memory, and other cluster information.
4. Select a CSP cluster to view VNF information, including service chains, CPU, memory, disk, and management IP.
5. Select **Services** to view service groups. Select **Diagram** for a design view, select a VNF for allocated resources, or select a service group from the **Service Groups** list.

View Cisco Colo Manager health

View Cisco Colo Manager health and addressing information.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**. For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select a CSP device from the table.
3. In the left pane, select **Colo Manager**.

The right pane displays Cisco Colo Manager memory usage, CPU usage, uptime, host system IP, CCM IP, and state.

View Cisco Catalyst SD-WAN Manager cluster information using the CLI

Use the CLI to verify Manager cluster health and service status.

Procedure

On the Cisco SD-WAN Manager device for the cluster, enter **request nms cluster diagnostics**.

The command displays health and service status for the application server, messaging server, configuration database, statistics configuration database, and coordination server.

What to do next

Refer to the Cisco Catalyst SD-WAN Command Reference Guide for **request nms cluster diagnostics**.

Viewing QoS statistics

Monitor QoS performance for interfaces, tunnels, and traffic classes.

Use these topics to understand QoS queue statistics and monitor interface or tunnel traffic.

QoS queue statistics

Understand QoS queue performance and utilization metrics.

QoS queue statistics measure the performance and utilization of network-traffic queues, including transmitted and dropped packets.

QoS queue statistics monitoring

The QoS feature in SD-WAN Manager lets you monitor ingress and egress traffic classes, view transmission rates before and after policy application, and identify drops caused by policing on interfaces and tunnel endpoints. Starting with Cisco Catalyst SD-WAN Manager Release 20.18.1, statistics for a single interface can be filtered by traffic class.

Benefits of QoS queue statistics

Benefits of monitoring QoS queue statistics.

Benefits of monitoring QoS queue statistics.

- Continuous monitoring of interface, tunnel-endpoint, and traffic-class QoS statistics.
- Historical visibility for interfaces and tunnels by selecting a time interval.

Restrictions for QoS statistics

Restrictions and limitations for QoS statistics.

Restrictions and limitations for QoS statistics.

Per-tunnel QoS statistics

SD-WAN Manager supports per-tunnel QoS statistics only in controller mode.

Drop statistics

With custom QoS policer configurations that use color selection for conform, exceed, or violate actions, exceed-action or violate-action drops might not be included in drop statistics.

Supported QoS actions

Bandwidth, priority, random-detect, child-level shaping, and policing are supported. Fair-queuing is not supported. A class map without a supported action is not collected or displayed.

Real-time QoS

The Real Time view for Tunnel QoS Summary Statistics can display up to 4,000 entries.

Monitor the QoS statistics for interfaces

Monitor real-time and historical network traffic for interfaces.

Before you begin

Enable the QoS feature on routers.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a device by selecting its name in the **Hostname** column.
3. Select **QoS** to open the **QoS Monitor** page.
4. Select a time interval. Use **Custom** to define start and end dates and times.

   The **Post Policy Rate** and **Post Policy Counter** charts display interface traffic and drop rates.

Interface QoS statistics

Interpret interface QoS charts and summary fields.

Interpret interface QoS charts and summary fields.

Interface QoS charts
Table 10: Interface QoS charts

Chart	Description
Post Policy Rate	Displays rate in Kbps and PPS, including traffic passed after policy and traffic dropped by policy.
Post Policy Counter	Displays bytes and packets forwarded after policy and bytes dropped by policy.

Interface QoS summary
Table 11: Interface QoS summary

Column	Description
Interface	Interface name. Select an interface to view its traffic classes.
Pre policy TX	Traffic transmitted before policy application.
Post policy TX	Traffic transmitted after policy application.
Drop	Traffic dropped after policy application; the difference between post-policy and pre-policy transmission rates.

Monitor the QoS statistics for tunnels

Monitor real-time and historical network traffic for tunnels.

Before you begin

Enable the QoS feature on routers.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a device by selecting its name in the **Hostname** column.
3. Select **QoS** to open the **QoS Monitor** page.
4. Select **Tunnel**.
5. Select a time interval. Use **Custom** to define start and end dates and times.

   The **Post Policy Rate** and **Post Policy Counter** charts display tunnel traffic and drop rates.

Tunnel QoS statistics

Interpret tunnel QoS charts and summary fields.

Interpret tunnel QoS charts and summary fields.

Tunnel QoS charts
Table 12: Tunnel QoS charts

Chart	Description
Post Policy Rate	Displays rate in Kbps and PPS, including traffic passed after policy and traffic dropped by policy.
Post Policy Counter	Displays bytes and packets forwarded after policy and bytes dropped by policy.

Tunnel QoS summary
Table 13: Tunnel QoS summary

Column	Description
Tunnel Endpoints	Tunnel-endpoint name. Select an endpoint to view its traffic classes.
Remote System IP	IP address of the remote system.
Pre policy TX	Traffic transmitted before policy application.
Post policy TX	Traffic transmitted after policy application.
Drop	Traffic dropped after policy application; the difference between post-policy and pre-policy transmission rates.

Monitor real-time tunnel QoS statistics

View tunnel-endpoint QoS statistics in real time.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a device by selecting its name in the **Hostname** column.
3. Select **Real Time**.
4. From the **Device Options** drop-down list, select **Tunnel QoS Statistics** to filter endpoints or **Tunnel QoS Summary Statistics** to view all endpoints.

Table 14: Tunnel QoS summary fields

Column	Description
Tunnel Endpoint	Selected-device system IP, local and remote colors, remote IP, and encapsulation type.
Queued Pkts	Packets queued for the endpoint.
Queued Bytes	Bytes queued for the endpoint.
Tx Pkts	Packets transmitted through the endpoint.

Column	Description
Tx Bytes	Bytes transmitted through the endpoint.
Drop Pkts	Packets dropped during transmission.
Drop Bytes	Bytes dropped during transmission.
Last Updated	Time the statistics were generated; statistics update every 10 seconds.

3 Resource Monitoring

Topics:

- Feature History of Resource Monitoring
- Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices
- Configure Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI
- Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI

Provides the wrapper topic for resource monitoring on Cisco SD-WAN control components and WAN Edge devices.

Feature History of Resource Monitoring

Provides feature-history information for resource monitoring on Cisco SD-WAN Controllers and WAN Edge devices, including configurable usage and disk I/O watermarks, polling, events, and alarms.

Table 15: Feature history of Resource Monitoring

Feature Name	Release Information	Description
Resource Monitoring on Cisco SD-WAN Controllers and WAN Edge Devices	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	With this feature, you can configure usage watermarks for resources such as CPU, memory, and disk on Cisco SD-WAN controllers and WAN Edge devices. In addition, in Cisco SD-WAN Manager servers, you can configure watermarks to monitor disk read and write speeds. Devices poll the resource usage and notify events to Cisco SD-WAN Manager. Cisco SD-WAN Manager raises alarms to alert you about changes in resource usage, or disk read or write speed so that you can take the necessary corrective action.

Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices

Describes Monit-utility-based resource monitoring for CPU, memory, disk usage, and Cisco SD-WAN Manager disk I/O speed. Administrators can configure usage thresholds and polling intervals to receive event notifications and alarms.

Cisco SD-WAN Release 20.7.1and Cisco vManage Release 20.7.1 introduce a Monit-utility-based workflow for monitoring the usage of the CPU, memory, and disk on Cisco SD-WAN Control Components and WAN Edge devices.

Resource Monitoring Configuration and Notifications

While Cisco SD-WAN Release 20.6.x and earlier releases, and Cisco vManage Release 20.6.x and earlier releases allowed the monitoring of how these resources are being used, the monitoring and reporting was based on predefined watermarks and a default polling interval. From Cisco SD-WAN Release 20.7.1 and Cisco vManage Release 20.7.1, you can customize the watermarks and the polling interval as appropriate to the resources in your deployment.

To monitor the usage of the CPU, memory, and disk, you can configure high-usage, medium-usage, and low-usage watermarks, and how frequently a device must check and report resource usage to Cisco SD-WAN Manager. In addition, you can monitor the disk read and write speeds on Cisco SD-WAN Manager servers by configuring appropriate read and write watermarks and the polling interval. You can use CLI templates or log in to the device CLI to configure custom watermarks and polling intervals for various devices and control components, as necessary.

Default Configuration

Devices and control components have a default configuration for the usage watermarks and the polling interval for monitoring the CPU, memory, and disk usage:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

The disk read and write speeds on Cisco SD-WAN Manager do not have a default configuration and are only monitored after you configure the necessary watermarks and polling interval.

Polling, Events, and Alarms

Based on the configuration, the device or controller polls the resource usage through monit and notifies events based on the polled usage information to Cisco SD-WAN Manager. Cisco SD-WAN Manager compares the event information with the event information received for the previous polling interval. If Cisco SD-WAN Manager detects a change in resource usage, it raises an appropriate alarm.

Devices and control components notify the following events to Cisco SD-WAN Manager:

- CPU usage
- Disk Usage
- Memory Usage
- Disk read speed (Cisco SD-WAN Manager only)
- Disk write speed (Cisco SD-WAN Manager only)

The event notifications have the following severity and status based on how the polled usage value compares with the configured watermarks:

Table 16: Event severity and status

Comparison	Severity	Status
Above the high watermark	Critical	usage-critical
Between the medium and high watermarks	Major	usage-warning
Between the low and medium watermarks	Minor	usage-notice
Below the low watermark	Minor	usage-healthy

For more information on viewing and managing events, see Events.

Based on the events, Cisco SD-WAN Manager can raise the following types of alarms:

- CPU Usage
- Disk Usage
- Memory Usage
- Disk Read Speed (Cisco SD-WAN Manager only)
- Disk Write Speed (Cisco SD-WAN Manager only)

The alarms map to the event status and severity as follows:

Table 17: Alarm severity and status

Alarm	Severity	Status
Critical (Red)	Critical	usage-critical
Major (Orange)	Major	usage-warning
Minor (Yellow)	Minor	usage-notice
Minor (Green)	Minor	usage-healthy

Initially, Cisco SD-WAN Manager raises an alarm when the event status is other than usage-healthy, indicating excessive resource usage.

If a subsequent event has the same status as the event Cisco SD-WAN Manager received previously, the alarm remains unchanged.

If a subsequent event is of lesser severity and indicates a healthier usage status, Cisco SD-WAN Manager raises an appropriate alarm. The new alarm clears the earlier higher-severity alarm.

Cisco SD-WAN Manager raises the Minor (Green) alarm only when the resource usage returns from a more severe state to the usage-healthy state. The Minor (Green) alarm indicates that the resource usage has returned to a normal level from an earlier excessive level.

For more information on viewing and managing alarms, see Alarms.

Supported Devices for Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices

- Cisco SD-WAN Manager server running Cisco vManage Release 20.7.1 or later
- Cisco SD-WAN Controller running Cisco SD-WAN Release 20.7.1 or later
- Cisco SD-WAN Validator running Cisco SD-WAN Release 20.7.1 or later
- WAN Edge devices running Cisco SD-WAN Release 20.7.1 or later

CPU Utilization Calculation Note

Note

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, there have been changes in how CPU utilization is calculated and reported on Cisco IOS XE Catalyst SD-WAN devices.

Before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1: CPU utilization was calculated as an average across all CPU cores (Control Plane, Data Plane, and Service Plane).

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, CPU utilization is calculated and reported based solely on the control plane CPU cores. This CPU utilization can be viewed from the System Status option in Cisco SD-WAN Manager. See View Device System Resource Utilization in Cisco SD-WAN Manager.

Additionally, this updated CPU utilization information is also available using the show sdwan system status and show processes cpu platform profile CP CLI commands. See show sdwan system status, show processes cpu platform.

Configure Resource Monitoring on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI

Describes how to configure CPU, memory, disk, and Cisco SD-WAN Manager disk I/O resource-monitoring watermarks and polling intervals with CLI commands in a CLI template or on the device CLI.

You can configure the resource monitoring watermarks and polling interval using CLI commands in a CLI template. This section provides sample CLI configurations to configure the watermarks and polling interval for resource monitoring.

Configure CPU Usage Watermarks and Polling Interval

```
Device# config
                Device(config)# system
                Device(config-system)# alarms
                Device(config-alarms)# cpu-usage
               Device(config-cpu-usage)# high-watermark-percentage percentage
```

```
              Device(config-cpu-usage)# medium-watermark-percentage percentage

                Device(config-cpu-usage)# low-watermark-percentage percentage

                Device(config-cpu-usage)# interval seconds
```

Example:

```
Device# config
                Device(config)# system
                Device(config-system)# alarms
                Device(config-alarms)# cpu-usage
                Device(config-cpu-usage)# high-watermark-percentage 80
                Device(config-cpu-usage)# medium-watermark-percentage 70
                Device(config-cpu-usage)# low-watermark-percentage 50
                Device(config-cpu-usage)# interval 10
```

Configure Memory Usage Watermarks and Polling Interval

```
Device# config
                Device(config)# system
                Device(config-system)# alarms
                Device(config-alarms)# memory-usage
                Device(config-memory-usage)# high-watermark-percentage
percentage
                Device(config-memory-usage)# medium-watermark-percentage
percentage
              Device(config-memory-usage)# low-watermark-percentage percentage

                Device(config-memory-usage)# interval seconds
```

Example:

```
Device# config
                Device(config)# system
                Device(config-system)# alarms
                Device(config-alarms)# memory-usage
                Device(config-memory-usage)# high-watermark-percentage 80
                Device(config-memory-usage)# medium-watermark-percentage 70
                Device(config-memory-usage)# low-watermark-percentage 50
                Device(config-memory-usage)# interval 10
```

Configure Disk Usage Watermarks and Polling Interval

```
Device# config
                Device(config)# system
                Device(config-system)# alarms
                Device(config-alarms)# disk-usage file-system-path
               Device(config-disk-usage-/opt/data)# high-watermark-percentage
 percentage
              Device(config-disk-usage-/opt/data)# medium-watermark-percentage
 percentage
                Device(config-disk-usage-/opt/data)# low-watermark-percentage
 percentage
                Device(config-disk-usage-/opt/data)# interval seconds
```

Example:

```
Device# config
                Device(config)# system
                Device(config)# alarms
                Device(config-alarms)# disk-usage /opt/data
               Device(config-disk-usage-/opt/data)# high-watermark-percentage
 80
              Device(config-disk-usage-/opt/data)# medium-watermark-percentage
 70
                Device(config-disk-usage-/opt/data)# low-watermark-percentage
 50
                Device(config-disk-usage-/opt/data)# interval 10
```

Configure Disk IO Speed Watermarks and Polling Interval on Cisco SD-WAN Manager

```
sd-wan-manager# config
                sd-wan-manager(config)# system
                sd-wan-manager(config-system)# alarms
                sd-wan-manager(config-alarms)# disk-speed disk-partition
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
read-high-watermark-kBps speed
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
read-medium-watermark-kBps speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)#
 read-low-watermark-kBps speed
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
write-high-watermark-kBps speed
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
write-medium-watermark-kBps speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)#
 write-low-watermark-kBps speed
              sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval seconds
```

Example:

```
vManage# config
                sd-wan-manager(config)# system
                sd-wan-manager(config-system)# alarms
                sd-wan-manager(config-alarms)# disk-speed /dev/nvme1n1
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
read-high-watermark-kBps 1000
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
read-medium-watermark-kBps 500
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
read-low-watermark-kBps 100
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
write-high-watermark-kBps 1000
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
write-medium-watermark-kBps 500
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)#
write-low-watermark-kBps 100
                sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval 100
```

Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and WAN Edge Devices Using the CLI

Provides CLI verification commands and sample outputs for CPU, memory, disk, and disk I/O watermarks, polling intervals, and CPU usage event notifications.

Verify Configuration of CPU Usage Watermarks and Polling Interval

The following is a sample output of the show alarms cpu-usage command and shows the configured CPU usage watermarks and the polling interval:

```
Device# show alarms cpu-usage

            HIGH         MEDIUM       LOW
            WATERMARK    WATERMARK    WATERMARK
CPU USAGE   PERCENTAGE   PERCENTAGE   PERCENTAGE   INTERVAL
-----------------------------------------------------------------
cpu-usage   80           70           50           10
```

Verify Configuration of Memory Usage Watermarks and Polling Interval

The following is a sample output of the show alarms memory-usage command and shows the configured memory usage watermarks and the polling interval:

```
Device# show alarms memory-usage

              HIGH         MEDIUM       LOW
              WATERMARK    WATERMARK    WATERMARK
MEMORY USAGE  PERCENTAGE   PERCENTAGE   PERCENTAGE   INTERVAL
-----------------------------------------------------------------
memory-usage  80           70           50           10
```

Verify Configuration of Disk Usage Watermarks and Polling Interval

The following is a sample output of the show alarms disk-usage command and shows the configured disk usage watermarks and the polling interval:

```
Device# show alarms disk-usage

             HIGH          MEDIUM        LOW
FILESYSTEM   WATERMARK     WATERMARK     WATERMARK
PATH         PERCENTAGE    PERCENTAGE    PERCENTAGE   INTERVAL
-----------------------------------------------------------------
/rootfs.rw    90            75            60           5
/tmp          90            75            60           5
/opt/data     80            70            50           10
```

Verify Configuration of Disk IO Speed Watermarks and Polling Interval

The following is a sample output of the show alarms disk-speed command and shows the configured disk IO speed watermarks and the polling interval:

```
sd-wan-manage# show alarms disk-speed

                        READ                      WRITE       WRITE
             READ HIGH  MEDIUM      READ LOW      HIGH        MEDIUM      WRITE LOW
             WATERMARK  WATERMARK   WATERMARK     WATERMARK   WATERMARK   WATERMARK
DISK PATH    K BPS      K BPS       K BPS         K BPS       K BPS       K BPS
 INTERVAL
-----------------------------------------------------------------------------------
/dev/sda2    1000       500         100           1000        500         100
 100
```

View Event Notifications on a Device

The following is a sample output of the show notification stream viptela command and shows a CPU usage event:

```
sd-wan-manager# show notification stream viptela
notification
 eventTime 2021-09-08T02:57:14.91578+00:00
 cpu-usage
  severity-level minor
  host-name vm12
  system-ip 172.16.255.22
  cpu-status usage-notice
  warning System CPU usage is above 50%
  cpu-user-percentage 40.9
  cpu-system-percentage 10.6
  cpu-idle-percentage 48.50
 !
!
```

4 Connectivity Fault Management

Topics:

- Feature history: Connectivity fault management
- Ethernet connectivity fault management
- Restrictions for connectivity fault management
- How connectivity fault management works in Cisco Catalyst SD-WAN
- Configuring Ethernet connectivity fault monitoring using CLI commands

Feature history: Connectivity fault management

Feature history for connectivity fault management.

Developments in connectivity fault management, by release.

Feature name	Release information	Description
Ethernet connectivity fault management Support on Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	The Ethernet connectivity fault management functionality helps to monitor Carrier Ethernet Network links.

Ethernet connectivity fault management

Information about Ethernet connectivity fault management.

The Ethernet connectivity fault management (CFM) protocol is an operations, administration, and maintenance (OAM) framework that:

- monitors connectivity;
- enables end-to-end fault management, allowing network administrators to find and isolate connectivity failures across large-scale Ethernet networks;
- provides fault isolation for large Ethernet metropolitan-area networks (MANs) and wide-area networks (WANs).

OAM protocols help service providers to isolate failures and respond to them in a timely manner in large, complex networks with a wide user base.

Connectivity fault management monitors links between provider edge routers and customer premises equipment (CPE) by

- exchanging CFM messages between provider edge routers and CPEs, and
- enabling the provider edge router to detect link failures in the network.

Restrictions for connectivity fault management

Restrictions for connectivity fault management.

Review these restrictions before configuring or troubleshooting connectivity fault management.

Configuration by CLI

You can configure CFM only through CLI on SD-WAN Manager. Therefore, you can access CFM execution for link fault detection, verification, and isolation in the SSH terminal of your device.

UP MEPs and MIPs

UP MEPs and maintenance intermediate points (MIPs) are not supported.

Troubleshooting

CFM troubleshooting functionality, such as Layer 2 traceroute and ping by CFM, is not supported on SD-WAN Manager. You can execute this functionality only on the device.

How connectivity fault management works in Cisco Catalyst SD-WAN

How connectivity fault management monitors Carrier Ethernet links between provider edge routers and customer premises equipment.

How connectivity fault management monitors Carrier Ethernet links between provider edge routers and customer premises equipment.

How connectivity fault management works

In a network where provider edge routers and customer premise equipment (CPE) are connected through a Carrier Ethernet network, it is necessary to monitor the links for any breakage. With support for CFM on Carrier Ethernet networks, CFM messages are exchanged between provider edges and CPEs, and the CFM protocol ensures that the provider edge is aware of link failures in the network.

CFM in Cisco Catalyst SD-WAN is supported on these interface types:

- VDSL interfaces
- SHDSL interfaces
- GigabitEthernet interfaces

These components support the functioning of CFM on Cisco Catalyst SD-WAN:

- Down maintenance end points
- Ethernet CFM and Ethernet OAM interaction
- SNMP traps

Down maintenance end points

How down maintenance end points handle connectivity fault management frames.

A down maintenance end point (MEP) is a CFM demarcation point on an interface that

- participates in CFM within a maintenance domain,
- sends and receives CFM frames through the wire connected to its configured port,
- processes or drops CFM frames according to their level and whether they arrive from the relay side or the wire side, and
- transparently forwards all higher-level CFM frames.

A maintenance domain is a management space for managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to the domain and at its boundary. A maintenance association identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a maintenance association.

A maintenance end point (MEP) is a demarcation point on an interface that participates in CFM within a maintenance domain. MEPs drop all lower-level frames and forward all higher-level frames. MEPs are defined per maintenance domain (level) and service (S-VLAN or Ethernet virtual circuit (EVC)). They are at the edge of a domain, define the boundary, and confine CFM messages within that boundary.

MEPs can proactively transmit CFM continuity check messages (CCMs) and, at the request of an administrator, transmit traceroute and loopback messages.

A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. For CFM frames coming from the relay side, the down MEP drops all lower-level frames and frames that are at its level. For CFM frames coming from the wire side, the down MEP processes all frames at its level and drops lower-level frames, except for traffic going to the other lower-level down MEP. The MEP transparently forwards all CFM frames at a higher level, regardless of whether it receives them from the relay or through the wire.

To deploy a down MEP per subinterface, first create an EVC+VLAN maintenance association, configure the VLAN ID under the subinterface, and then configure the down MEP under the parent interface of that subinterface.

Ethernet CFM and Ethernet OAM interaction

How Ethernet CFM and Ethernet OAM interact through the OAM manager.

How Ethernet CFM and Ethernet OAM interact through the OAM manager.

Ethernet virtual circuit

An EVC, as defined by the Metro Ethernet Forum, is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by an edge device either to find an alternative path into the service provider network or, in some cases, to fall back to a backup path over Ethernet or another alternative service, such as asynchronous transfer mode (ATM).

OAM manager

OAM manager is an infrastructure element that streamlines interaction between OAM protocols. The OAM manager requires two interworking OAM protocols, in this case, Ethernet CFM and Ethernet OAM. Interaction is unidirectional from the OAM manager to the CFM protocol, and the only information exchanged is the user network interface (UNI) port status. These additional port status values are available:

- REMOTE_EE: Remote excessive errors
- LOCAL_EE: Local excessive errors
- TEST: Either remote or local loopback

After CFM receives the port status, it communicates that status across the CFM domain.

SNMP traps

SNMP traps generated by maintenance end points for connectivity fault management events.

SNMP traps generated by maintenance end points for connectivity fault management events.

Continuity check traps

- MEP up: Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down: Sent when a timeout or last gasp event occurs.
- Cross-connect: Sent when a service ID does not match the VLAN.
- Loop: Sent when a MEP receives its own continuity check messages (CCMs).
- Configuration error: Sent when a MEP receives a continuity check with an overlapping MPID.

Cross-check traps

- Service up: Sent when all expected remote MEPs are up in time.
- MEP missing: Sent when an expected MEP is down.
- Unknown MEP: Sent when a CCM is received from an unexpected MEP.

Configuring Ethernet connectivity fault monitoring using CLI commands

Information about configuring Ethernet connectivity fault monitoring using CLI commands.

Commands and example configurations for configuring Ethernet connectivity fault monitoring using CLI commands.

CLI commands

Use these commands to configure Ethernet CFM in a CLI profile or template:

- Enable the IEEE version of CFM:

```
Device(config)# ethernet cfm ieee
```

- Enable CFM processing globally on the device:

```
Device(config)# ethernet cfm global
```

- Enable caching of CFM data learned through traceroute messages:

```
Device(config)# ethernet cfm traceroute cache
```

- Enable Ethernet CFM syslog messages:

```
Device(config)# ethernet cfm logging
```

- Enable SNMP trap generation for Ethernet CFM continuity check events:

```
Device(config)# snmp-server enable traps ethernet cfm cc
```

- Enable SNMP trap generation for Ethernet CFM continuity check events related to the cross-check operation between statically configured MEPs and MEPs learned through CCMs:

```
csnmp-server enable traps ethernet cfm crosscheck
```

- Define an EVC and enter EVC configuration mode:

```
Device(config)# ethernet evc evc-id
```

- Define a CFM maintenance domain at a particular maintenance level and enter Ethernet CFM configuration mode:

```
Device(config)# ethernet cfm domain domain-name level level-id
```

- Include the sender ID TLVs and the attributes containing type, length, and values for neighbor devices:

```
Device(config)# sender-id chassis
```

- Configure a maintenance association within a maintenance domain and enter Ethernet CFM service configuration mode:

```
Device(config-ecfm)# service short-ma-name evc evc-name vlan vlanid direction
 down
```

- Configure offload sampling:

```
Device(config)# offload sampling sample
```

- Enable the transmission of CCMs:

```
Device(config-ecfm-srv)# continuity-check
```

- Configure the time period between CCM transmissions. The default interval is 10 seconds:

```
Device(config-ecfm-srv)# continuity-check [interval cc-interval]
```

- Configure the MEP domain and ID on the interface:

```
Device(config)# interface interface-name
Device(config-if)# cfm mep domain domain-name mpid id service service-name
```

For a detailed explanation of the purpose of each command, refer to *Configuring Ethernet CFM* in the *Carrier Ethernet Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)*.

Example configurations

This example shows how to configure CFM per subinterface for an EVC+VLAN maintenance association:

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet evc USER-SERVICE
 !
 ethernet cfm domain USER level 7
  service USER-SERVICE evc USER-SERVICE vlan 112 direction down
   continuity-check
   continuity-check interval 10s
   continuity-check loss-threshold 3
 !
 ethernet cfm logging
 !
 interface GigabitEthernet0/0/1
  no ip address
  speed 100
  no negotiation auto
  ethernet cfm mep domain USER mpid 1562 service USER-SERVICE
   cos 2
 !
 interface GigabitEthernet0/0/1.112
  description NAME 2286884663
   encapsulation dot1Q 112
   ip address 192.0.2.1 255.255.255.0
```

This example shows how to configure CFM per physical interface for a port maintenance association:

```
config-transaction
 ethernet cfm ieee
 ethernet cfm global
 ethernet cfm traceroute cache
 ethernet cfm domain USER level 1
  sender-id chassis
  service USER-SERVICE port
   continuity-check
   continuity-check interval 1m
   sender-id chassis
 !
 ethernet cfm logging
 !
 interface Ethernet0/1/0
  no ip address
  load-interval 30
  speed [10/100/1000]
  duplex [half/full]
  ethernet oam mode passive
  ethernet oam remote-loopback supported
  ethernet oam
  ethernet cfm mep domain USER mpid 101 service USER-SERVICE
   alarm notification all
 !
 interface Ethernet0/1/0.101
  encapsulation dot1Q 101
  pppoe enable group global
  pppoe-client dial-pool-number 1
  no cdp enable
  ethernet loopback permit external
```

You can use this configuration in a CLI profile or template in SD-WAN Manager.

5 Data Collection and Telemetry

Topics:

- Feature history: Data collection and telemetry
- Information about data collection and Cisco Catalyst SD-WAN telemetry
- Enable or disable data collection
- Enable or disable Cisco Catalyst SD-WAN telemetry
- Enable or disable cloud services
- Additional steps to enable data collection on an on-premises Cisco Catalyst SD-WAN Manager instance

Feature history: Data collection and telemetry

Feature history for data collection and telemetry.

Developments in data collection and telemetry, by release.

Feature name	Releases	Feature information
Manage Data Collection for Cisco Catalyst SD-WAN Telemetry	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	You can disable data collection for Cisco Catalyst SD-WAN telemetry using Cisco SD-WAN Manager. Data collection for telemetry is enabled by default.

Information about data collection and Cisco Catalyst SD-WAN telemetry

Learn about network and statistics collection and Cisco Catalyst SD-WAN telemetry.

Network statistics collection, and telemetry are processes that

- collect operational data from the devices in the network, and
- provide detailed telemetry from SD-WAN Control Components and network infrastructure.

> **Note**
>
> From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed **Control Components**.

Network and statistics collection

Network and statistics collection gathers operational data from Cisco IOS XE Catalyst SD-WAN devices. Collection is typically initiated by network events, such as connectivity issues or network flaps.

You can enable or disable this collection and customize the collection interval in minutes by using the Collection Interval field.

Starting with Cisco Catalyst SD-WAN Manager Release 20.14.1, the Data Collection tab is named Data Collection & Statistics. The tab is located at Administration > Settings > Network Statistics Configuration and Collection. Refer to Enable or disable data collection.

SD-WAN telemetry

SD-WAN telemetry gathers detailed telemetry from control components and network infrastructure. Telemetry is enabled by default when cloud services are enabled. For cloud-hosted control components, telemetry is enabled during provisioning.

To collect BFD loss, latency, and jitter metrics from controller-mode Cisco IOS XE Catalyst SD-WAN devices, use one of these methods:

- Cisco SD-WAN Manager REST APIs
- SNMP, which provides limited data

- Flexible NetFlow (FNF)

From Cisco vManage Release 20.6.1, the option to manage telemetry is available at **Administration** > **Settings** > **Data Collection**. Before Cisco vManage Release 20.6.1, the **Data Collection** tab provided only the option to enable or disable data collection.

From Cisco Catalyst SD-WAN Manager Release 20.14.1, the option is available at **Administration** > **Settings** > **Cloud Services** > **Terms & Conditions**. Refer to Enable or disable Cisco Catalyst SD-WAN telemetry.

Enable or disable data collection

Enable or disable operational data collection and configure the collection interval.

Use these steps to manage data collection in Cisco SD-WAN Manager.

Procedure

1. From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Network Statistics Configuration and Collection**.
2. In the **Collection Interval** field, enter the collection frequency in minutes.
3. Enable or disable **Additional Event Collection**.

   This option gathers operational data from network devices. It collects operational data triggered by network events like connectivity problems or network flaps.

4. Select Save.

   All platforms support up to 250 configured interfaces. For one-minute interface statistics collection, the recommended maximum is 250 interfaces.

Enable or disable Cisco Catalyst SD-WAN telemetry

Enable or disable Cisco Catalyst SD-WAN telemetry data collection.

Before you begin

Cloud Services must be enabled before you manage Cisco Catalyst SD-WAN telemetry. Cloud-hosted control components have telemetry enabled by default; telemetry is disabled by default for on-premises control components. Refer to Enable or disable cloud services.

Use these steps to manage Cisco Catalyst SD-WAN telemetry in Cisco SD-WAN Manager.

Procedure

1. From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Services**.
2. Select **Terms & Conditions**.
3. Enable or disable the required Cisco Catalyst SD-WAN telemetry data collection option.

   These options are available:

   - **SD-WAN Telemetry Basic** is enabled by default when cloud services are enabled. It allows Cisco SD-WAN Manager to collect telemetry from control components and the network.

- **SD-WAN Telemetry Advanced** is enabled by default when cloud services are enabled. It provides activated features and capabilities. Cisco SD-WAN Manager anonymizes the data and does not send sensitive overlay information to DCS.

4. Select Save.

Enable or disable cloud services

Enable or disable cloud services and authenticate the Cisco SD-WAN Manager connection.

Use these steps to manage cloud services for Cisco SD-WAN Manager.

Procedure

1. From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Services**.
2. Enable or disable **Cloud Services**.
3. If you enable Cloud Services, authenticate.

   For Cisco Catalyst SD-WAN Manager Release 20.12.1 and later, and Cisco vManage Release 20.9.4 and later releases of 20.9.x, enter your smart account credentials. Cisco SD-WAN Analytics is enabled by default. Use this option to enable or disable Cisco SD-WAN Analytics.

4. Select **Save**.

Additional steps to enable data collection on an on-premises Cisco Catalyst SD-WAN Manager instance

Configure firewall access to enable data collection from an on-premises Cisco Catalyst SD-WAN Manager instance.

Complete these steps for an on-premises Cisco Catalyst SD-WAN Manager instance.

Procedure

1. Configure the local firewall to allow outbound communication from the SD-WAN Manager through interface VPN 0 on port 443.

   Choose these destinations based on the geographic location of your Cisco SD-WAN Analytics instance.

   Table 18: Destinations for Cisco SD-WAN Analytics data collection

Location	Destinations
Americas	https://us-west.dcs.viptela.net (Cisco vManage 20.1.1 or earlier); https://us01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later); https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)

Location	Destinations
Americas (East)	https://us-east.dcs.viptela.net (Cisco vManage 20.1.1 or earlier); https://us02.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later); https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)
Europe	https://europe.dcs.viptela.net (Cisco vManage 20.1.1 or earlier); https://eu01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later); https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)
Australia	https://au01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later); https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3.1 or later)

2. From the SD-WAN Manager CLI, use **cURL -k** to verify reachability to these destinations.

6 Flow Simulation

Topics:

- Feature history: Flow simulation
- Simulate flows

Feature history: Flow simulation

Feature history for flow simulation.

Developments in flow simulation, by release.

Feature name	Release information	Description
Forwarding Serviceability	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables service path and tunnel path under the Simulate Flows function in the SD-WAN Manager template and displays the next-hop information for an IP packet. This feature enables Speed Test and Simulate Flow functions on Cisco IOS XE Catalyst SD-WAN devices.

Simulate flows

Procedure to simulate flows and view next-hop information for an IP packet.

View the next-hop information for an IP packet available on routers.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a device from the list of devices that appears.
3. Select **Troubleshooting** in the left pane.
4. Under **Traffic**, select **Simulate Flows**.
5. To specify the data traffic path, select values or enter data in the required fields:
   - **VPN**: VPN in which the data tunnel is located.
   - **Source/Interface**: Interface from which the cflowd flow originates.
   - **Source IP**: IP address from which the cflowd flow originates.

     For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
   - **Destination IP**: Destination IP address of the cflowd flow.

     For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
   - **Application**: Application running on the router.
   - **Custom Application** (created in CLI)
6. Select **Advanced Options** to configure these:
   a) In the **Path** field, select **Tunnel** or **Service** to indicate whether the data traffic path information comes from the service side of the router or from the tunnel side.
   b) In the **Protocol** field, enter the protocol number.
   c) In the **Source Port** field, enter the port from which the cflowd flow originates.
   d) In the **Destination Port** field, enter the destination port of the cflowd flow.
   e) In the **DSCP** field, enter the DSCP value in the cflowd packets.
   f) (Optional) Select the **All Paths** check box to view all possible paths for a packet.

7. Select **Simulate** to determine the next hop that a packet with the specified headers would take.

7 Monitoring Hosted Edge Services

Topics:

- Feature history: Monitoring hosted edge services
- Hosted edge services
- Restrictions for monitoring hosted edge services
- Start or stop the hosted edge services
- Monitor the hosted edge services

Feature history: Monitoring hosted edge services

Feature history of monitoring hosted edge services.

Developments in monitoring hosted edge services, by release.

Feature name	Release information	Description
Hosted edge services	Cisco Catalyst SD-WAN Manager Release 20.18.1	You can monitor hosted edge services (IOx applications) for health, associated devices, version, and IOx state using the SD-WAN Manager interface. You can also start or stop the hosted edge services.

Hosted edge services

Information about hosted edge services.

Hosted edge services are Cisco IOx applications that

- are installed on WAN edge devices, improving their features and functionality beyond the core Cisco IOS XE Catalyst SD-WAN software, and
- can include both Cisco and third-party applications.

Using SD-WAN Manager, you can

- monitor all hosted edge services installed on your edge devices for resource usage, device details, version, and more, and
- manage hosted edge services installed on your devices.

Restrictions for monitoring hosted edge services

Restrictions for monitoring hosted edge services.

Review these restrictions before monitoring hosted edge services.

Disk space calculation

If multiple hosted edge services are running on a device using any version older than Cisco IOS XE Catalyst SD-WAN Release 17.18.x, the disk space usage for some hosted edge services may not reflect correctly. Upgrade to the latest version of Cisco IOS XE Catalyst SD-WAN Release 17.18.x to ensure proper disk space usage calculation.

Multitenancy

In a multitenant environment, you can monitor hosted edge services only at the tenant level and not at the provider level.

Start or stop the hosted edge services

Procedure to start or stop a hosted edge service.

Before you begin

Deploy a hosted edge service to one or more devices in the network and activate it. Refer to the configuration instructions in the Cisco Catalyst SD-WAN Integrations guide.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Hosted Edge Services**.
2. Select a hosted edge service.

   The page shows devices running the selected hosted edge service.

   Alternatively, to manage the hosted edge service from the **Devices** page, use these steps:

   a) From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
   b) Select a device from the list.
   c) Select **App Status Info** to view hosted edge services associated with the device.
3. To start or stop a hosted edge service, select **...** adjacent to the device and select **Start edge service** or **Stop edge service**.

   Note

   You can stop a hosted edge service only if it is in **Running** state. Similarly, you can start a hosted edge service if it is in **Stopped** state. You cannot perform any operation on the hosted edge service if it is in **Deployed** or **Activated** state.

   After the device metrics are refreshed, the **Edge service state** column shows the current state of the edge service.

Monitor the hosted edge services

Procedure to monitor hosted edge services and their resource usage, state, and device details.

Monitor the devices running hosted edge services, their resource usage, status of the hosted edge services on individual devices, and so on.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Hosted Edge Services**.

   The hosted edge services view includes:

   Table 19: Hosted edge services

Field	Description
Hosted edge service name	Name of the hosted edge service installed on your edge device to provide additional features.
Edge service author	Name of the organization that developed this edge service.

Field	Description
Number of sites installed	Total number of sites where the hosted edge service is currently installed.
Number of devices installed	Total number of edge devices on which the hosted edge service is installed.

2. To monitor the hosted edge services on specific devices, use these steps:
   a) From the **Hosted Edge Services** page, select a hosted edge service name.

   The page shows the devices running the selected hosted edge service.

   Table 20: IOx states and device details

Field	Description
IOx states	IOx states are hosted edge service states that indicate whether the service is operational. • **Stopped**: Indicates the hosted edge service has stopped and is no longer operational on the device. • **Running**: Indicates the hosted edge service is accessible and operational on the device. • **Deployed**: Indicates the hosted edge service is deployed to the device and the installation is successful. • **Activated**: Indicates the network configurations are successfully added to the hosted edge services and the application is now active. Select any state to filter the network devices by the state of the hosted edge service.
Network device	Name of the network device on which the selected instance of hosted edge service is running.
Site name	Logical identifier that represents the operational grouping of the network device within the Cisco SD-WAN environment.
Resource usage health	Resource consumed by the hosted edge services. For a hosted edge service, the health status indicates: • **Good**: The hosted edge service's CPU, memory, or disk space resource usage is less than 50 percent of the allocated resources. • **Fair**: The hosted edge service's CPU, memory, or disk space resource usage lies between 50 and 75 percent of the allocated resources. • **Poor**: The hosted edge service's CPU, memory, or disk space resource usage is greater than 75 percent of the allocated resources. This reflects only the resource usage by the service. It does not reflect the total resource usage of the device.

Field	Description
Edge service state	Displays the IOx state of the hosted edge service: stopped, running, deployed, or activated.
Edge service version	The IOx application version running on the device, as defined in the package.yaml file.
Last update	Displays the latest timestamp when the device metrics were updated.

b) For a selected network device, select **...** and select **View edge service info**.

The drawer displays these details:

- **Resource usage**: Current health status along with resource consumption of CPU, RAM, and disk space.
- **Edge service details**: Current IOx state, hosted edge service version, and last data fetch details. Use the **Stop edge service** option to stop the hosted edge service instance on the device. Select **Refresh device metrics** to manually update the device metrics for the selected device.
- **Package information**: Hosted edge service name, CPU architecture, and author information.

3. To monitor the hosted edge services on a specific device from the **Devices** page, use these steps:
   a) From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
   b) Select a device from the list.
   c) Select **App Status Info**.

   The page shows the hosted edge services running on the device.

Table 21: Hosted edge services on a device

Field	Description
Edge service name	Name of the IOx application hosted on the device.
Edge service author	Name of the organization that developed the edge service.
Edge service version	The IOx application version running on the device as defined in the package.yaml file.

Field	Description
Resource usage health	Resource consumed by the hosted edge services. For a hosted edge service, the health status indicates: • **Good**: The hosted edge service's CPU, memory, or disk space resource usage is less than 50 percent of the allocated resources. • **Fair**: The hosted edge service's CPU, memory, or disk space resource usage lies between 50 and 75 percent of the allocated resources. • **Poor**: The hosted edge service's CPU, memory, or disk space resource usage is greater than 75 percent of the allocated resources. This reflects only the resource usage by the service. It does not reflect the total resource usage of the device. You can also view the health using the **Edge service resource usage health** column on the **Devices** page for all devices that have any hosted edge service.
Edge service state	Displays the IOx state of the hosted edge service: Stopped, Running, Deployed, or Activated.
CPU usage	Displays CPU resource usage in percentage.
Disk space usage	Displays disk space usage in percentage.
Memory usage	Displays memory usage in percentage.

8 Packet trace

Topics:

- Feature history: Packet trace
- Packet trace
- Guidelines for packet trace
- Restrictions for packet trace
- Configure packet trace using CLI commands
- Monitoring packet trace
- Monitoring packet trace on Cisco vEdge devices
- Monitoring packet trace on Cisco IOS XE Catalyst SD-WAN devices
- Viewing FIA statistics
- Configuration examples for packet trace

Feature history: Packet trace

Feature history for packet trace.

Developments in packet trace, by release.

Table 22: Feature history

Feature name	Release information	Description
Bidirectional Support for Packet Tracing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can configure packet tracing on edge devices.
Packet Trace Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature offers these enhancements to packet trace: • View Feature Invocation Array (FIA) statistics about a feature in a packet trace using the command **show platform packet-trace fia-statistics** • View label information for the Multiprotocol Label Switching (MPLS) feature in packet trace.

Packet trace

Information about packet trace, including packet-trace levels.

Packet trace is a feature that:

- enables you to debug packet loss on edge devices, and
- enables you to inspect forwarding behavior of traffic flows on devices in the network.

About packet trace

The packet trace feature enables you to debug packet loss on edge devices and to inspect any forwarding behavior of traffic flows on the devices in the network. You can configure packet tracer with various conditions based on which the flow of the packets is segregated and is captured for tracing. This helps you to diagnose issues and troubleshoot them more efficiently.

Packet tracer includes 2048 bytes of internal memory that is used to copy path data. This memory is overwritten during circular mode of tracing.

The Packet Trace feature provides three levels of inspection for packets–accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet-processing capability. However, packet trace limits the inspection of packets that match the **debug platform condition** statements, and is a viable option even under heavy-traffic situations in customer environments.

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, bidirectional support is added on the edge devices for a conditional debugging match filter. Conditional debugging allows you to filter out some of the debugging information on the edge device. You can check the debugging information that matches a certain interface, MAC address, or username.

Table 23: Packet trace levels

Packet trace level	Description
Accounting	Packet trace accounting provides a count of packets that enter and leave the network processor. Packet trace accounting is a lightweight performance activity, and runs continuously until it is disabled.
Summary	At the summary level of packet trace, data is collected for a finite number of packets. Packet trace summary tracks the input and output interfaces, the final packet state, the consumed packet state and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface.
Path data	Packet trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data. Path data also has two optional capabilities—packet copy and Feature Invocation Array (FIA) trace. The packet copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3, or layer 4). The FIA trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing. **Note** Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. We recommend that you use path-data level in a limited way or in situations where packet performance change is acceptable.

Guidelines for packet trace

Guidelines for configuring packet trace.

We recommend using ingress conditions when using the packet trace for a more comprehensive view of packets.

Packet trace configuration requires data plane memory. On systems where data plane memory is constrained, carefully consider how you will select the packet trace values. A close approximation of the amount of memory consumed by packet trace is provided by this equation:

memory required = (statistics overhead) + (number of packets) * (summary size + data size + packet copy size).

Restrictions for packet trace

Restrictions for packet trace.

These are the restrictions for packet trace.

Memory requirements

When the Packet Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

> **Note**
>
> The amount of memory consumed by the packet trace feature is affected by the packet trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting other router services.

Supported packet types

Only IP packets are supported. L2 (ARP) packets, bridge packets, fragmented packets, and multicast packets are not supported.

IPv6 support

IPv6 is not supported.

Packet duplication

Packet duplication is not supported.

Resubmitted packets

Any packet that goes through resubmission (for example, IPsec or GRE encrypted packets) and matches the configured filters in both the inner packet (decrypted packet) as well as the outer packet (encrypted packet) will have individual trace entries. To use the packet tracer more efficiently, you should configure as many filters as possible with the available information to debug the issue.

Controller-mode packet capture

In the routers running in controller mode, the Embedded Packet Capture (EPC) supports capturing only Ethernet traffic with Ethertype 0x0800 (IPv4). Capturing MPLS traffic with Ethertype 0x8847 is not supported. To capture MPLS traffic, use the command, **monitor capture <name> match any** to capture all traffic regardless of Ethertype. For more granular capture, use the **debug platform packet-trace copy packet both** command on FIA trace.

Configure packet trace using CLI commands

Procedure to configure packet trace using CLI commands.

Procedure

1. Enable packet trace for the traffic and specify the maximum number of packets.

Example

```
Device# debug platform packet-trace packet [number of traced packets]
```

2. Specify the matching criteria for tracing packets. Matching criteria provides the ability to filter by protocol, IP address and subnet mask, interface, and direction.

   Example

   ```
   Device# debug platform condition [interface interface name] {match
   ipv4|ipv6|mac src dst}  {both|ingress|egress} [bidirectional]
   ```

3. Enable MPLS output label trace. An MPLS output label trace is included in debug path to reduce the impact on performance.

   Example

   ```
   Device# debug platform hardware qfp active feature cef-mpls datapath mpls all
   ```

4. Enable the specified matching criteria and start packet tracing.

   Example

   ```
   Device# debug platform condition start
   ```

5. Deactivate the condition and stop packet tracing.

   Example

   ```
   Device# debug platform condition stop
   ```

6. Exit the privileged EXEC mode.

   Example

   ```
   exit
   ```

Monitoring packet trace

Information about monitoring packet trace.

Packet trace configuration is based on the AND operation of the specified conditions, with the packets matching all the specified conditions being traced.

Monitoring procedures

These topics describe how to monitor packet trace:

- Monitoring packet trace on Cisco vEdge devices
- Monitoring packet trace on Cisco IOS XE Catalyst SD-WAN devices
- Viewing FIA statistics

Monitoring packet trace on Cisco vEdge devices

Information about monitoring packet trace on Cisco vEdge devices.

Use the **show packet-trace statistics** command on Cisco vEdge devices to view the summary of all the packets matching the specified condition.

Packet trace statistics

This example displays all the conditions that are configured for packet tracing:

```
Device# show debugs
debugs packet-trace condition source-ip 10.1.1.1
debugs packet-trace condition vpn-id 0
debugs packet-trace condition interface ge0/1
debugs packet-trace condition state Stopped
```

Use the **show packet-trace statistics** command on Cisco vEdge devices to view the summary of all the packets matching the specified condition.

This example displays a packet trace statistics for the specified interface, in this case, ge 0:

```
Device# show packet-trace statistics source-interface ge0_0
packet-trace statistics 0
source-ip 10.1.15.13
source-port 0
destination-ip 10.4.0.5
destination-port 0
source-interface ge0_0
destination-interface loop0.0
decision PUNT
duration 40
```

Refer to show packet-tracer command page.

Detailed packet view

This example shows output from the **show packet-trace details** command, which is displayed for the specified trace ID 10:

```
Device# show packet-trace details 10
=================================================================================
Pkt-id     src_ip(ingress_if)     dest_ip(egress_if)     Duration     Decision
=================================================================================
10         10.1.15.15:0 (ge0_0)   12.168.255.5:0 (ge0_0)     15 us
PUNT
INGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b
 0a 01 0f 0f e0
```

```
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00
 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00
 00 00 00 00
00 00 00 00 00
EGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b
 0a 01 0f 0f e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00
 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00
 00 00 00 00
00 00 00 00 00
Feature Data
-----------------------------------
TOUCH : fp_proc_packet
-----------------------------------
TOUCH : fp_proc_packet2
-----------------------------------
TOUCH : fp_send_to_host
-----------------------------------
FP_TRACE_FEAT_PUNT_INFO:
icmp_type : 0
icmp_code : 0
qos : 7
-----------------------------------
TOUCH : fp_hw_x86_pkt_free
```

Use the **show packet-trace details** command to view detailed information for the specified trace ID. The detailed packet view output displays three sections - summary data section, packet dump section, and featured data section.

Monitoring packet trace on Cisco IOS XE Catalyst SD-WAN devices

Information about summary and detailed packet-trace views on Cisco IOS XE Catalyst SD-WAN devices.

These sections describe summary and detailed packet-trace views on Cisco IOS XE Catalyst SD-WAN devices.

Summary view

Use the **show platform packet-trace summary** command on Cisco IOS XE Catalyst SD-WAN devices to view the summary of all the packets matching the specified condition.

This example displays a packet trace summary on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace summary

Pkt   Input                     Output                    State  Reason
0     INJ.12                    Gi2                       FWD
1     Gi2                       internal0/0/rp:0          PUNT   5
2     INJ.1                     Gi2                       FWD
3     INJ.1                     Gi2                       FWD
4     Gi2                       internal0/0/rp:0          PUNT   5
5     Gi2                       internal0/0/rp:0          PUNT   5
6     INJ.1                     Gi2                       FWD
7     INJ.1                     Gi2                       FWD
8     Gi2                       internal0/0/rp:0          PUNT   5
9     Gi2                       internal0/0/rp:0          PUNT   5
10    Gi2                       internal0/0/rp:0          PUNT   5
11    INJ.1                     Gi2                       FWD
12    Gi2                       internal0/0/rp:0          PUNT   5
```

```
13    INJ.1                     Gi2                       FWD
14    INJ.1                     Gi2                       FWD
```

Detailed packet view

This example shows output from the **show platform packet-trace packet 0** command on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace packet 0

Packet: 0           CBUG ID: 4321
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 1124044721695603 ns (09/20/2022 01:47:28.531049 UTC)
    Stop    : 1124044722142898 ns (09/20/2022 01:47:28.531497 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.10.10.10
    Destination : 20.20.20.20
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x814670b0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 600 ns
  Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
    Entry       : Input - 0x81494d2c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1709 ns
  Feature: IPV4_INPUT_ARL_SANITY
    Entry       : Input - 0x814690e0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1274 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x81494d28
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 269 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x81494d34
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 384 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x814670a0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 107 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x8146709c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 36 ns
```

```
  Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x81494d40
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 38331 ns
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x81495258
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 259 ns
  Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
    Entry       : Input - 0x8146ab58
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 9485 ns
  Feature: IPV4_VFR_REFRAG
    Entry       : Output - 0x81495c6c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 520 ns
  Feature: IPV6_VFR_REFRAG
    Entry       : Output - 0x81496600
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 296 ns
  Feature: MPLS(Output)
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Label Stack Entry[1]: 0x03e850fe
      StackEnd:NO, TTL:254, EXP:0, Label:16005, is SDWAN:NO
    Label Stack Entry[2]: 0x000121fe
      StackEnd:YES, TTL:254, EXP:0, Label:18, is SDWAN:NO
  Feature: MPLS_OUTPUT_ADD_LABEL
    Entry       : Output - 0x8145e130
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 29790 ns
  Feature: MPLS_OUTPUT_L2_REWRITE
    Entry       : Output - 0x812f4724
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 23041 ns
  Feature: MPLS_OUTPUT_FRAG
    Entry       : Output - 0x8149ae5c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 785 ns
  Feature: MPLS_OUTPUT_DROP_POLICY
    Entry       : Output - 0x8149ebdc
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 14697 ns
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x814ac56c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 45662 ns
Packet Copy In
  00505683 d54f0050 56830863 08004500 00641018 0000ff01 6f450a0a 0a0a1414
  14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd abcdabcd abcdabcd
Packet Copy Out
```

```
  00505683 d4900050 5683429a 884703e8 50fe0001 21fe4500 00641018 0000fe01
  70450a0a 0a0a1414 14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd
```

Use the **show platform packet-trace summary** command to view detailed information for the specified trace ID. The detailed packet view output displays three sections–summary data section, packet dump section, and featured data section.

- Summary data section: Displays packet trace ID, ingress interface, egress interface, and the forward decision taken for the packet to traverse across the device information for the specified trace ID.
- Packet dump section: Displays ingress and egress packet information. Only the first 96 bytes of packet header details are displayed.

> **Note**
>
> The complete packet dump is not displayed because of tracer-memory limitations.

- Feature data section: Displays forwarding plane features that generate feature-specific tracing data and provides feature data decodes. These features provide debugging information to packet tracer, such as forward result, drop reason, and other behavior.

Viewing FIA statistics

Method for viewing Feature Invocation Array (FIA) statistics.

Minimum supported releases: Cisco vManage Release 20.11.1 and Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

View FIA statistics

Use the **show platform packet-trace fia-statistics** command on Cisco IOS XE Catalyst SD-WAN devices to view FIA statistics. FIA statistics provides details about the number of features, and the time details-minimum time, maximum time, and average time about a feature.

This example displays FIA statistics on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show platform packet-trace fia-statistics

Feature                                      Count  Min(ns)   Max(ns)   Avg(ns)
-----------------------------------------------------------------------------
INTERNAL_TRANSMIT_PKT_EXT                       66     4720     28400
13333
MARMOT_SPA_D_TRANSMIT_PKT_EXT                   16     4560     16920
11955
L2_SVI_OUTPUT_BRIDGE_EXT                         1     3640      3640
3640
INTERNAL_INPUT_GOTO_OUTPUT_FEATURE_EXT          16     1680      3880
2755
IPV4_INPUT_LOOKUP_PROCESS_EXT                    1     2720      2720
2720
IPV4_OUTPUT_L2_REWRITE_EXT                       1     2240      2240
2240
IPV4_OUTPUT_DROP_POLICY_EXT                      4     1040      2880
2050
IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT             1     1960      1960
```

```
1960
SSLVPN_INJECT_TX_MSG_EXT                          15      600      2440
1746
IPV4_INTERNAL_FOR_US_EXT                           1     1560      1560
1560
LAYER2_OUTPUT_QOS_EXT                             63      280      2480
1537
LAYER2_OUTPUT_DROP_POLICY_EXT                     78      120      3120
1525
LAYER2_INPUT_LOOKUP_PROCESS_EXT                   15      280      2240
1312
UPDATE_ICMP_PKT_EXT                                1     1280      1280
1280
DEBUG_COND_MAC_EGRESS_EXT                          3      840      1160
973
IPV4_INTERNAL_INPUT_SRC_LOOKUP_CONSUME_EXT         1      960       960
960
IPV4_PREF_TX_IF_SELECT_EXT                         1      800       800
800
DEBUG_COND_OUTPUT_PKT_EXT                         66       80      1640
707
IPV4_INTERNAL_ARL_SANITY_EXT                       3      240       960
666
IPV4_INTERNAL_INPUT_SRC_LOOKUP_ISSUE_EXT           1      640       640
640
IPV4_VFR_REFRAG_EXT                                5      320       920
640
EVC_EFP_VLAN_TAG_ATTACH_EXT                       15       80      1040
629
L2_SVI_OUTPUT_GOTO_OUTPUT_FEATURE_EXT              1      520       520
520
LAYER2_VLAN_INJECT_EXT                            15      120       760
504
L2_ES_OUTPUT_PRE_TX_EXT                           16        0      1000
502
DEBUG_COND_APPLICATION_IN_EXT                      1      480       480
480
DEBUG_COND_APPLICATION_OUT_CLR_TXT_EXT             3       80       720
426
DEBUG_COND_INPUT_PKT_EXT                          16       80       880
417
IPV4_OUTPUT_FRAG_EXT                               1      360       360
360
DEBUG_COND_APPLICATION_IN_CLR_TXT_EXT              1      320       320
320
DEBUG_COND_APPLICATION_OUT_EXT                     3      240       280
266
LFTS_INJECT_PKT_EXT                               16       40       480
250
LAYER2_BRIDGE_INJECT_EXT                          15       40       560
234
```

Configuration examples for packet trace

Examples of configuring and monitoring the conditions for packet tracing.

This example shows how to configure and monitor the conditions for packet tracing:

Packet-trace configuration example

```
Device# debug platform packet-trace packet 2048
Device# debug platform condition ingress
Device# debug platform condition start
Device# debug platform condition stop
Device# show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/2.3060 Gi0/0/2.3060 DROP 402
1 internal0/0/rp:0 internal0/0/rp:0 PUNT 21 2 internal0/0/recycle:0 Gi0/0/2.3060
 FWD
```

9 Viewing QoS Information

Topics:

- Feature history: Viewing QoS information
- Restrictions for QoS monitoring
- View QoS information in a chart
- View a real-time QoS information table

Feature history: Viewing QoS information

Feature history for viewing QoS information.

Developments in viewing QoS information, by release.

Feature name	Release information	Description
QoS Monitoring in SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This release extends the capability to view interface-wise QoS information through SD-WAN Manager to support Cisco IOS XE Catalyst SD-WAN devices. Before this release, you could monitor QoS information for Cisco IOS XE Catalyst SD-WAN devices only through the device CLI.

Restrictions for QoS monitoring

Restrictions and limitations for QoS monitoring.

Describes restrictions and limitations that apply to viewing QoS information in SD-WAN Manager.

Sub-interfaces

This feature is not supported for sub-interfaces.

Per-tunnel QoS

This feature is not supported when per-tunnel QoS is enabled.

View QoS information in a chart

Describes the process for generating and customizing QoS charts in Cisco SD-WAN Manager to monitor interface-specific packet speeds and drop statistics.

View QoS statistics to identify which traffic classes experienced the greatest number of drops on which devices in your network.

A QoS chart shows the packet speed and the number of packets dropped for each queue for the selected interface.

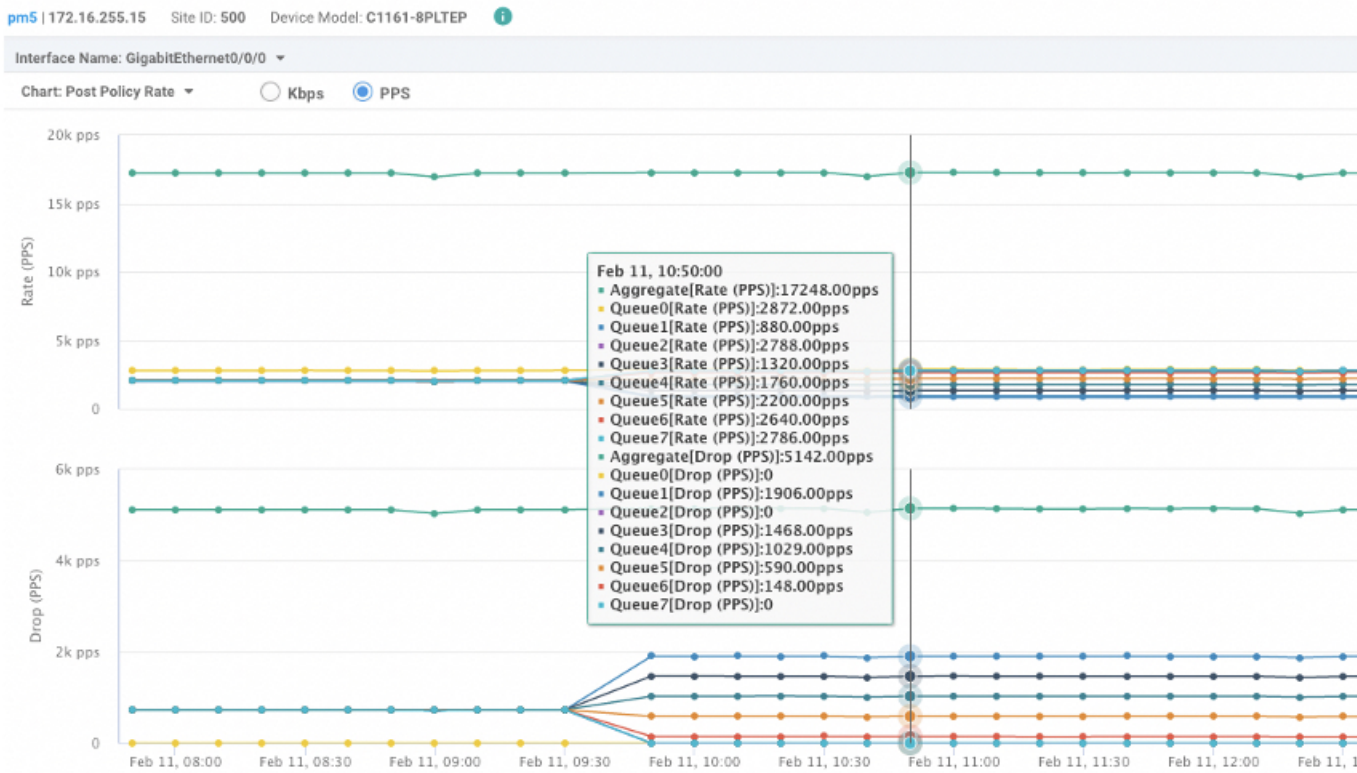
Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that appears.
3. In the left pane, select **QoS** under the **Applications** area.
4. The upper part of the right pane provides these options:
   - **Interface Name**: From the drop-down menu, choose the interface for which you want to view QoS data.
   - **Time Range**: Choose to view the information for a specified time range:
     - Real time
     - Predefined time ranges (1h, 3h, 6h, and so on)
     - Custom time range

5. From the **Chart** drop-down list, select one of these:
   - **Post Policy Rate**: This option displays the speed at which data travels per second in either kbps (default) or packets per second (PPS). This value is calculated to get the per-second speed by using the formula Post Policy Counter/10.
   - **Post Policy Counter**: This option displays the number of packets, or the number of packets in bytes, that have gone through the queue in the last 10 seconds.

- SD-WAN Manager displays the QoS chart. This example shows QoS data for a specified historical time range for the selected interface. In this chart, each data point represents 10 minutes. For longer time ranges, SD-WAN Manager aggregates data points.

  Figure 9: QoS chart



- SD-WAN Manager displays a table with the chart. The table always displays historical data even if you choose the real-time option to generate a chart. These historical tables generated below real-time charts have no connection with the real-time values in the chart.

  This example shows historical data in a table.

  Figure 10: Historical QoS table

Queue Name	Pre Policy Tx (in kbps)	Post Policy Tx (in kbps)	Drop (in kbps)
Aggregate	259230.875	199686.969	59543.344
Queue0	32538.344	32538.344	0
Queue1	32362.406	14931.094	17430.75
Queue2	32380.75	29467.031	2913.563
Queue3	32390.906	18288.25	14102.031
Queue4	32401.281	21645.594	10755.188
Queue5	32404.125	25002.75	7400.875
Queue6	32391.5	28359.969	4030.969
Queue7	32358.031	29450.25	2907.656

View a real-time QoS information table

Describes how to access and filter real-time Interface QoS statistics in tabular format in Cisco SD-WAN Manager.

View real-time QoS information in a tabular format.

Procedure

1. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that appears.
3. In the left pane, select **Real Time** under the **Security Monitoring** area.
4. From the **Device Options** drop-down list, select **Interface QoS Statistics**.

SD-WAN Manager displays a table of QoS statistics.

10 Security Monitoring

Topics:

- Feature history: security monitoring
- View traffic, CPU, and memory usage
- View the health and reachability of UTD

Feature history: security monitoring

Feature history for security monitoring.

Developments in security monitoring, by release.

Feature name	Release information	Description
Enhanced Security Monitoring on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to view the CPU, memory, and traffic usage on your device. You can also view the health of individual UTD features.

View traffic, CPU, and memory usage

View traffic, CPU, and memory usage for UTD features on a device.

View the traffic, CPU, and memory usage of UTD features on a device.

Procedure

1. From the SD-WAN Manager **Monitor** > **Devices** page, select the device.
2. Under **Security Monitoring** in the left pane, select one of these UTD features: **Intrusion Prevention**, **URL Filtering**, and so on.
3. Review the traffic counter graph.

   By default, the traffic counter graph is displayed. You can customize the time range to view traffic usage for a specific period, such as **Real Time**, 1h, 3h, or a **Custom** time range. The default time range is 24h. The time range cannot be more than 365 days.
4. To view CPU or memory usage, select one of these options:
   - **UTD Stats: CPU Usage**: View CPU usage.
   - **UTD Stats: Memory Usage**: View memory usage.

View the health and reachability of UTD

View the health and reachability of UTD features on a device.

View the health and reachability status of UTD features on a device.

Procedure

1. From the SD-WAN Manager **Monitor** > **Devices** page, select the device.
2. Under **Security Monitoring** in the left pane, select one of these UTD features, such as **Intrusion Prevention** or **URL Filtering**.

3. Review the UTD health status.

   For all features, the health of UTD is displayed as one of these statuses:

   - **Down**: UTD is not configured.
   - **Green**: UTD is healthy.
   - **Yellow**: For example, high memory usage.
   - **Red**: For example, one or more Snort instances are down.

4. If you configured UTD on the device and the status is not green, contact Cisco TAC for assistance.
5. Review these additional details for the selected UTD feature:

Table 24: UTD feature details

UTD feature	Status information
Intrusion Prevention	Package Version IPS Last Updated Reason for last update status
URL Filtering	Cloud Reachability
Advanced Malware Protection	AMP Cloud Reachability Status TG Cloud Reachability Status
Umbrella DNS Redirect	Umbrella Registered VPNs DNSCrypt

11 Underlay Measurement and Tracing Services

Topics:

- Feature history: underlay measurement and tracing services
- Underlay measurement and tracing services
- Prerequisites for underlay measurement and tracing services
- Restrictions for underlay measurement and tracing services
- Configuring underlay measurement and tracing services
- Trace and view tunnel paths on demand
- Troubleshooting underlay measurement and tracing services
- Configuration example for underlay measurement and tracing services

Feature history: underlay measurement and tracing services

Feature history of underlay measurement and tracing services.

Developments in underlay measurement and tracing services, by release.

Feature Name	Release Information	Feature Description
Underlay Measurement and Tracing Services	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	The underlay measurement and tracing services (UMTS) feature provides visibility into the exact paths that tunnels take between local and remote Cisco IOS XE Catalyst SD-WAN devices, through the underlay network (the physical devices that comprise the network).
On-demand Underlay Measurement and Tracing Services	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Control Components Release 20.18.1	UMTS can be used to discover the underlay path even when the BFD session (tunnel) is **down**.

Underlay measurement and tracing services

Information about underlay measurement and tracing services.

Underlay measurement and tracing services (UMTS) is a feature that

- provides visibility into the exact path that a tunnel takes between local and remote devices through the underlay network, including all nodes between the two devices,
- traces the exact path that a tunnel is using rather than discovering or tracing candidate paths, and
- supports monitoring, event-driven, and on-demand tracing of tunnel paths.

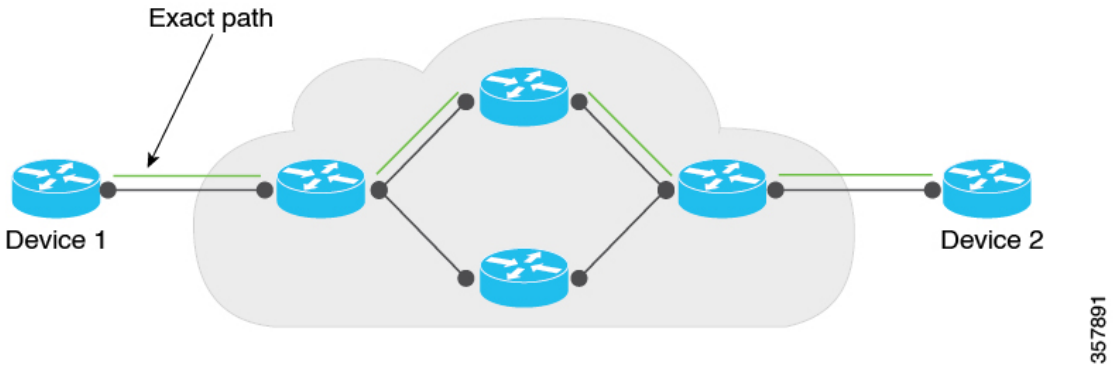
Underlay paths

When a device creates an IPsec or GRE tunnel to a remote device through the underlay network, more than one path may be possible. The number of paths and hops depends on the variability of the underlay network. The path that a tunnel takes can change over time. For example, if a tunnel uses a path that includes router A and router A later becomes unavailable, the tunnel requires a different path.

Each possible path through the underlay network is called a candidate path. The actual path that the tunnel is using at a given time is called the exact path. UMTS traces only the exact path. It does not discover or trace candidate paths.

This illustration shows an underlay network with multiple paths for a tunnel between Device 1 and Device 2, including the exact path used by the tunnel.

Figure 11: Exact path



Tracing paths

You can trace tunnel paths in a network using one of these options:

- Monitoring: Trace tunnel paths regularly according to a configured time interval.
- Event-driven: Trace tunnel paths when either of these events occurs:
  - A change in the service-level agreement (SLA) for the tunnel.
  - A change in the path maximum transmission unit for the tunnel.
- On demand: Trace tunnel paths on demand and display the results in SD-WAN Manager. Refer to Trace and view tunnel paths on demand.

Mechanism for underlay measurement and tracing services

For UMTS interval-based monitoring and event-driven monitoring, SD-WAN Manager provides monitoring configuration, including the interval and event types, as part of the overall device configuration. In accordance with the configuration, devices use a UMTS probe packet mechanism to trace the exact paths of tunnels across all hops and collect network metrics such as delay and loss. Latency is supported only hop by hop.

The devices send the resulting information to SD-WAN Manager, which sends it to SD-WAN Analytics. SD-WAN Analytics uses the information to display the exact paths of tunnels graphically in the network.

For the on-demand option, SD-WAN Manager sends a request to the devices in the network to probe the network and trace the exact paths of tunnels. This request is a NETCONF action, not a device configuration. The devices use the UMTS probe packet mechanism to trace the exact paths of tunnels across all hops and collect network metrics such as delay and loss. The devices send the resulting information to SD-WAN Manager, which displays the exact paths of tunnels graphically in the network.

Note

From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the UMTS probe works irrespective of BFD state.

Benefits of underlay measurement and tracing services

Benefit of using underlay measurement and tracing services to identify tunnel problems.

UMTS provides details of the exact path of each Cisco Catalyst SD-WAN tunnel, which can be useful in identifying problems with the tunnels.

Prerequisites for underlay measurement and tracing services

Prerequisites for viewing exact tunnel paths and UMTS visualizations.

Complete these prerequisites before viewing exact tunnel paths or UMTS visualizations.

Application and flow visibility

To view exact-path graphs in SD-WAN Analytics, you must enable application visibility and flow visibility.

> **Note**
>
> This prerequisite does not apply to on-demand viewing of graphs in SD-WAN Manager.

Data stream

Data stream must be enabled in SD-WAN Manager. From the SD-WAN Manager menu, choose **Administration** > **Settings** to trace tunnel paths on demand and display the results in SD-WAN Manager.

SD-WAN Analytics integration

SD-WAN Manager and SD-WAN Analytics must be integrated to view visualizations in SD-WAN Analytics. For information about integrating SD-WAN Analytics with SD-WAN Manager, refer to Onboard Cisco SD-WAN Analytics.

Restrictions for underlay measurement and tracing services

Restrictions for underlay measurement and tracing services.

Review these restrictions before using underlay measurement and tracing services.

IPv4 support

UMTS is supported only on Cisco Catalyst SD-WAN tunnels using IPv4 addresses.

Viewing exact paths

For interval-based and event-driven options, you can view the graphical representation of exact paths only in SD-WAN Analytics. For the on-demand option, you can view exact paths in SD-WAN Manager.

Graph limitation

SD-WAN Analytics UMTS graphs cannot distinguish between monitoring records and SLA and path maximum transmission unit events.

Jitter and loss

Jitter and loss measurements are not supported.

Configuring underlay measurement and tracing services

Methods for configuring underlay measurement and tracing services.

Configure underlay measurement and tracing services using one of these methods.

Use one of these methods to configure underlay measurement and tracing services.

- Configuration group
- CLI commands

Configure underlay measurement and tracing services using a configuration group

Procedure to configure underlay measurement and tracing services using a configuration group.

Use a configuration group to configure monitoring and event-driven underlay measurement and tracing services.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Select **...** adjacent to the configuration group name, then select **Edit**.
3. Select **System Profile**.
4. Select **Add Feature**.
5. From the **Type** drop-down list, select **Performance Monitoring**.
6. In the **Feature Name** field, enter a name for the feature.
7. In the **Description** field, enter a description for the feature.
8. Select **Underlay Measurement Track Service**.
9. To trace tunnel paths regularly according to a time interval, complete these steps:
   a. From the **Monitoring** drop-down list, select **Global**.
   b. Select the toggle button to enable the continuous monitoring option in UMTS.
   c. From the **Monitoring Interval (Minutes)** drop-down list, select a time. This option enables you to monitor the exact path during a specific time period.
10. To trace tunnel paths when triggered by an event, complete these steps:
    a. From the **Event Driven** drop-down list, select **Global**.
    b. From the **Event Type** drop-down list, select one or more event types.
    c. Select **Save**.
11. Select the **Associated Devices** tab.
12. From the list of devices, select one or more devices, then select **Deploy**.
13. On the **Process Overview** page, select **Next**.

    The **Selected Devices to Deploy** page displays the devices selected previously.
14. Select or clear the check boxes next to the devices, then select **Next**.
15. On the **Summary** page, select **Deploy** to deploy the configurations on the devices.

    With the **Monitor** option enabled in SD-WAN Manager, time-series data for the exact path can be generated and displayed in SD-WAN Analytics.

    To learn about using configuration groups, refer to Configuration Groups and Feature Profiles.

Configure underlay measurement and tracing services using CLI commands

Procedure to configure underlay measurement and tracing services using CLI commands.

Use CLI templates to configure continuous monitoring and event types for exact paths.

> **Note**
>
> By default, CLI templates execute commands in global config mode.

This procedure configures interval-based monitoring and event-driven UMTS monitoring of tunnel paths.

Procedure

1. Monitor the exact paths of tunnels continually at a specific time interval.

```
sdwan
umts
  monitor
  periodicity seconds
  local-color-all
  remote-color-all
  remote-system-ip-all
```

   The tunnel periodicity range is from 10 to 4294967295 (2^32 - 1) seconds.

2. Monitor the exact paths of tunnels when triggered by a change in a tunnel's service-level agreement (SLA) or path maximum transmission unit.

```
sdwan
event
  event-type event-type
  local-color-all
  remote-color-all
  remote-system-ip-all
```

Here is a complete configuration example:

```
sdwan
umts
 monitor
 periodicity 1800
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event
 event-type tunnel-sla-change
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
```

```
 event-type tunnel-pmtu-change
 local-color-all
 remote-color-all
 remote-system-ip-all
!
```

Trace and view tunnel paths on demand

Procedure to trace and view exact tunnel paths on demand.

You can configure UMTS to trace exact paths at intervals or when triggered by an event. Refer to Configuring underlay measurement and tracing services.

Alternatively, you can trace tunnel paths on demand and view the paths using this procedure.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select **...** next to the corresponding device name, then select **Underlay Discovery**.
3. Enter the parameters required to retrieve the exact path details.
4. Select **Start**.

   A graph with details about the exact path that network traffic is taking is displayed.

What to do next

These options also let you trace and view exact paths on demand in SD-WAN Manager:

- From the SD-WAN Manager menu, choose **Monitor** > **Tunnels**, select **...** next to the corresponding tunnel name, then select **Underlay Discovery**.
- From the SD-WAN Manager menu, choose **Monitor** > **Applications** page, select **...** next to the corresponding application name, then select **Underlay Discovery**.
- On the **Site Topology** page, select a device or tunnel name, then select **Underlay Discovery** in the right pane.

Troubleshooting underlay measurement and tracing services

Common troubleshooting topics for underlay measurement and tracing services.

These topics describe common troubleshooting situations for underlay measurement and tracing services.

Troubleshooting topics

- Zero IP address
- Timeout error

Zero IP address

Problem, causes, and solution for a zero IP address in an exact path.

Troubleshoot a zero IP address in an exact path.

Problem

SD-WAN Manager displays hops with a zero IP address (0.0.0.0) in the exact path.

Possible causes

- Intermediate hops in the public internet might not respond because Internet Control Message Protocol (ICMP) time exceeded messages are disabled or blocked by a firewall. In such cases, hops are shown with a zero IP address.
- The destination edge device might be a Cisco vEdge device, which does not support UMTS.

Solution

Zero IP addresses in the exact path do not imply functional problems with the tunnel. Verify that the zero IP address is caused by one of the reasons described in the Possible causes section.

Timeout error

Problem, causes, and solution for a UMTS timeout error.

Troubleshoot a timeout error during an on-demand UMTS session.

Problem

A timeout error is displayed after you start a UMTS session on demand in SD-WAN Manager.

Possible causes

- You are not using the minimum required releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a or later for Cisco IOS XE Catalyst SD-WAN devices, and Cisco Catalyst SD-WAN Control Components Release 20.10.1 or later.
- Network connectivity issues exist.

Solution

Check the causes listed in the Possible causes section, and try the trace again.

Configuration example for underlay measurement and tracing services

Configuration example for monitoring and event-driven underlay measurement and tracing services.

This example displays the configuration for the **Monitoring** and **Event-Driven** options configured in a Cisco IOS XE Catalyst SD-WAN device.

Monitoring and event-driven configuration

```
sdwan
umts
 monitor
 periodicity 1800
 local-color-all
 remote-color-all
 remote-system-ip-all
 !
 event
 event-type tunnel-sla-change
 local-color-all
 remote-color-all
```

```
 remote-system-ip-all
 !
 event-type tunnel-pmtu-change
 local-color-all
 remote-color-all
remote-system-ip-all
!
```

12 Viewing Network Topology

Topics:

- Feature history: Viewing network site topology
- Information about viewing site topology
- Supported devices for site topology visualization
- Prerequisites for site topology visualization
- View the network site topology

Feature history: Viewing network site topology

Feature history for viewing network site topology.

Developments in viewing network site topology, by release.

Feature name	Release information	Description
Site Topology Visualization in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can now view the topology diagram of a site in Cisco SD-WAN Manager.
Site Topology Visualization in Cisco SD-WAN Manager (Phase II)	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	You can view information about the health of devices and tunnels in the topology.

Information about viewing site topology

Information about the site topology diagrams generated by Cisco SD-WAN Manager.

A topology diagram is a visualization of site topology that displays

- Device information: The topology diagram displays all devices deployed at a selected site. It displays the model and health status of each device. When you place the cursor over a device name, you can view the hostname and system IP address of that device. When you select a device name, you can view detailed device information in the right navigation pane. From this pane, you can navigate to the device dashboard to view more details.
- Transport information: The topology diagram displays VPN 0 and all transport interfaces connected to a device, including interface and protocol details. When you place the cursor over a transport interface name, you can view the average upstream and downstream speed during the last three hours.
- Service VPN information: The topology diagram displays the ID and name of the service VPNs. When you select the drop-down arrow adjacent to the name of a service VPN, you can view the protocol, interfaces, and average upstream and downstream speed during the last three hours.

  The topology diagram displays a maximum of 12 service VPNs. If there are more than 12 service VPNs, select **More** to see the complete list of service VPNs in the right navigation pane.
- Circuit health information: The color of the link between the circuit and the transport interface indicates the circuit health.

SD-WAN Manager generates a topology diagram for each site with Cisco IOS XE Catalyst SD-WAN devices associated with a configuration group.

Site topology data

If a site ID changes, for example from 100 to 200, both 100 and 200 appear in the site topology view. The old site ID disappears after approximately 30 minutes.

The global topology uses site data from the site table API. The site table shows only edge information. If the SD-WAN Manager site ID does not match the site ID of any edge device, data for all sites is not displayed.

Topology display and controls

- If a Cisco IOS XE Catalyst SD-WAN device is associated with a configuration group but is not deployed, the topology diagram displays only the hostname and system IP address. If the device is associated with a configuration group and is also deployed, the topology diagram displays complete device details, including LAN and WAN details.
- If a site has devices that are not associated with a configuration group, the topology diagram displays the standalone devices with only the hostname and system IP address.
- There is no limit on the number of devices shown in the topology diagram for each site. However, if a site has multiple devices, the connections between the devices are not shown.
- Adjust the zoom level of the topology diagram by selecting the zoom-in and zoom-out icons. You can also view the topology diagram in full screen by selecting the full-screen icon.
- Select the refresh icon to regenerate the topology diagram and view the latest data.
- View health-metric details by selecting the legend icon.

Supported devices for site topology visualization

Devices that support site topology visualization.

Cisco IOS XE Catalyst SD-WAN devices

Prerequisites for site topology visualization

Prerequisites for viewing site topology.

Complete these prerequisites before viewing site topology.

Configuration group deployment

Associate devices to a configuration group.

Device monitoring access

Viewing site topologies requires a role-based access control (RBAC) permission for the device monitoring.

View the network site topology

Procedure to view the network site topology from the Devices page or Geography page.

You can view the network site topology on the **Devices** page or on the **Geography** page.

Procedure

1. View the network site topology on the **Devices** page:
   a) From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
   b) Find the corresponding Cisco IOS XE Catalyst SD-WAN device in the table and select the value in the **Site ID** column adjacent to the device name.

      Alternatively, select the device name in the **Hostname** column, and then select the **Site ID** value on the device dashboard.

SD-WAN Manager displays the topology of the site.

2. View the network site topology on the **Geography** page:
   a) From the SD-WAN Manager menu, choose **Monitor** > **Geography**.
   b) Select a device in the map.
   c) Select the **Site ID** value.

   SD-WAN Manager displays the topology of the site.

13 Monitoring the Network

Topics:

- View WLAN output
- View client details
- View WiFi configuration
- View VRRP information
- View VNF status
- View Cisco umbrella information
- View tunnel health in table view
- View tunnel health in heatmap view
- View data plane tunnel loss statistics
- View traffic loss for application-aware routing
- View the top 100 tunnel connections
- View tunnel connections for a device
- View TLOC loss, latency, and jitter information
- View SFP information
- View PKI trustpoint information
- View Cisco Catalyst SD-WAN Validator information
- View NMS server status
- View network-wide path insight
- View multicast information
- View loss percentage, latency, jitter, and octet information for tunnels
- View logging information
- View license information
- View SAIE flows
- View Cisco Catalyst SD-WAN Controller policy
- View ACL information
- Monitor NAT DIA tracker configuration on IPv4 interfaces
- View control connections in real time
- View cloud express information
- View cflowd information
- View BGP information
- BFD protocol
- View ARP table entries
- View AppQoE information
- View the system clock
- Run a traceroute
- View routing information

- Rediscover network
- Feature history of network monitoring
- Determine the status of network sites
- View a configuration commit list
- Run site-to-site speed test
- Check application-aware routing traffic
- View internet outages

View WLAN output

Configure the Wireless SSID tab to view WLAN output along with the associated VLAN ID.

Use the Wireless SSID tab to view the WLAN output along with the VLAN ID assoicated.

Minimum Supported Release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IR1800 device from the list of devices.
3. Select **Real Time** in the left pane.
4. In the **Device Options** drop-down box, type **Wireless SSID**.

Option	Description
Wireless SSID	View the WLAN output.

View client details

Configure wireless client monitoring to view client details along with their MAC addresses using the Wireless Clients tab.

View client details along with their MAC addresses using the Wireless Clients tab.

Minimum Supported Release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IR1800 device from the device list.
3. Select **Real Time** in the left pane.
4. In the **Device Options** drop-down list, choose **Wireless Clients**.

Option	Description
Wireless Clients	View the client details along with their MAC addresses.

View WiFi configuration

Configure the monitoring view to display WiFi configuration information for routers that support wireless LANs.

View WiFi configuration details for Cisco Catalyst SD-WAN routers that support wireless LANs (WLANs), including access point information, radio frequency parameters, and SSID parameters for virtual access points (VAPs).

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.
3. Select **WiFi** in the left pane.

The right pane displays the WiFi configuration and statistics for the selected device.

What to do next

- The AP Information bar displays access point information and the Clients Details button. Select **Clients Details** to view information about clients connected to the access point during the selected time period.
- The upper part of the pane displays radio frequency parameters for access points and SSID parameters for virtual access points (VAPs).
- The lower part displays VAP receive and transmit statistics in graphical format. Select a predefined or custom time period to view the data for that period.
- Use the VAP statistics graph legend to select a VAP interface and view information for that interface only. Select the VAP interface again to return to the previous view.

View VRRP information

Configure access to VRRP information through the device monitoring interface.

Use this procedure to access real-time VRRP information for troubleshooting or monitoring purposes on your network devices.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.
3. Select **Real Time** from the left pane.
4. Select **Device Options**, and choose **VRRP Information**.

View VNF status

Configure monitoring of VNF status to determine which VNF to use when designing a network service.

Reviewing VNF status can help you to determine which VNF to use when you are designing a network service.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a CSP device from the table.
3. From the left pane, click **VNF Status**.
4. In the table, select the VNF name.

The right pane displays information about the selected VNF. You can monitor network utilization, CPU utilization, memory utilization, and disk utilization using the graphs.

What to do next

- Use Chart Options to select the type of data to display and the time period.
- The graph displays the selected VNF information, and the legend allows you to select a VNF to view its information.
- The VNF table lists information about all VNFs. By default, the first six VNFs are selected and displayed in the graph.
- Select or clear the check box next to a VNF to include or exclude it from the graph. You can display information for a maximum of six VNFs at a time.
- Click a column title to change the sort order.
- Use the filter criteria to filter the VNF table.

View Cisco umbrella information

Configure monitoring to view Cisco Umbrella device registration status and related information on network devices.

View Cisco Umbrella registration status and device information to monitor and verify the connection status of devices with Cisco Umbrella services.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose the following.

Device option	Command	Description
Umbrella Device Registration	`show umbrella deviceid`	Displays Cisco Umbrella registration status for Cisco IOS XE Catalyst SD-WAN devices.

View tunnel health in table view

Provides information about viewing tunnel health metrics and Quality of Experience data in the Monitor Tunnels table interface.

Minimum supported release: Cisco vManage Release 20.10.1

In the **Monitor Tunnels** window the table shows information about the health of tunnels created in the last hour, displaying a maximum of 10,000 tunnels.

The tunnel information includes tunnel health, state, Quality of Experience (QoE), average latency, average loss, average jitter, local IP address, and remote IP address.

You can also view the tunnel health on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

Tunnel health metrics

The average health metric of tunnels is calculated as follows:

Table 25: Tunnel health metrics

Health	QoE	Status	Evaluation Logic
Good	QoE >= 8	UP	All attributes met
Fair	5 <= QoE < 8	UP	All attributes met
Poor	0 < QoE< 5	DOWN	Any attributes met

View tunnel health in heatmap view

Provides a grid-based visualization of tunnel health status using colored squares that display connection quality as Good, Fair, or Poor.

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, a grid of colored squares displays the tunnel health as **Good**, **Fair**, or **Poor**. Hover over or click a square to display additional details about a tunnel at a specific time. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

To view the tunnel health for a single site, click **All Sites** and select the site ID to enter the single-site view.

View data plane tunnel loss statistics

Provides instructions for accessing and viewing data plane tunnel loss statistics on Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose **Tunnel Statistics**.

View traffic loss for application-aware routing

Introduces methods for viewing traffic loss in application-aware routing using the Application-Aware Routing pane.

To view traffic loss for application-aware routing, see the Application-Aware Routing pane under **Monitor** > **Overview**in Cisco SD-WAN Manager. In Cisco vManage Release 20.6.x and earlier, see **Dashboard** > **Main Dashboard**.

You can also use the **show app-route statistics** command to view traffic loss.

View the top 100 tunnel connections

Configure viewing of tunnel connection details and monitoring data plane tunnels between Cisco Catalyst SD-WAN devices.

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Tunnels**.

- The Tunnels table lists the following information about all tunnel end points:
  - Health State Quality of Experience (QoE) score.
  - The QoE score rates the quality of experience of an application that a network can deliver for a period of time.
  - Local IP and remote IP Average latency, loss, and jitter data
- The health of a tunnel is defined based on the following criteria:
  - Good: If the QOE score is between 8 and 10, and the tunnel status is 1/1.
  - Fair: If the QOE score is between 5 and 7, and the tunnel status is 1/1.
  - Poor: If the QOE score is between 1 and 4, or the tunnel status is 0/1.

> **Note**
>
> The tunnel information is available in Cisco SD-WAN Manager as a separate menu starting from Cisco vManage Release 20.7.1.

View tunnel connections for a device

Procedure for viewing tunnel connections for a device.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network**.
2. Select a device from the list.
3. In the left pane, click **TLOC** under **WAN**.

   The right pane displays information about the device's tunnel connections.

4. (Optional) Use the **Chart Options** drop-down list to select the type of data to display.

   Select a predefined or custom time period to view the data for that period.

5. (Optional) Use the filter in the search bar to filter the tunnel table.

   The tunnel table displays the average latency, loss, and jitter for all tunnel endpoints. By default, the first six tunnels are selected, and the graph displays information for the selected tunnels.

6. (Optional) Select or clear the check box next to a tunnel to include or exclude it from the graph.

   You can select and view information for a maximum of 30 tunnels at a time.

7. (Optional) Click **Application Usage** to view SAIE flow information for the TLOC.

   Note

   - Beginning with Cisco vManage Release 20.8.1, the Application Usage column and links are removed from the **Monitor** > **Devices** > **WAN – Tunnel** window.

     After you configure on-demand troubleshooting for a device, you can view SAIE usage data based on the selected filters or by application family, sorted by usage.

   - In Cisco vManage Release 20.7.1 and earlier, the SAIE flow is called the deep packet inspection (DPI) flow.

   For information about configuring on-demand troubleshooting, see On-Demand Troubleshooting. For information about viewing SAIE flows, see View SAIE Flows.

View TLOC loss, latency, and jitter information

Configure monitoring to view TLOC loss, latency, and jitter information for network devices.

View aggregated average loss, latency, and jitter information for all TLOC colors to monitor network performance and troubleshoot connectivity issues.

- Beginning with Cisco vManage Release 20.8.1, the **Application Usage** column and the **Application Usage** links are removed from the **Monitor** > **Devices** > **WAN – Tunnel** window.

  After you have configured on-demand troubleshooting for a device, you can view SAIE usage data based on the selected filters or based on application families sorted by usage.

  For more information on configuring on-demand troubleshooting, see On-Demand Troubleshooting. For more information on viewing SAIE flows, see View SAIE Flows.

- 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.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices that is displayed.

3. In the left pane, select **TLOC** under the **WAN** area.

The right pane displays the TLOC loss, latency, and jitter information for the selected device.

- The upper part displays the selected data in a graph. Use Chart Options to choose the data type and time period. Select a TLOC color in the graph legend to display information for that TLOC only.
- The lower part displays a table with the average jitter, loss, and latency data for all TLOCs. By default, the first six TLOC colors are selected. Select or clear the check box next to a TLOC color to include or exclude it from the graph. You can select up to 30 TLOCs at a time.
- Use the Search Options filter to search the TLOC table.
- Select **Application Usage** for a TLOC to view its SD-WAN Application Intelligence Engine (SAIE) flow information.

View SFP information

Configure SFP information monitoring to view detailed status, diagnostic data, and measurement information for router interfaces.

View SFP information to monitor the status and performance of small form-factor pluggable transceiver modules on router interfaces.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose one of the following commands:

Device option	Command	Description
SFP Detail	`show interface SFP detail`	Displays detailed SFP status and digital diagnostic information.
SFP Diagnostic	`show interface SFP detail`	Displays SFP digital diagnostic information.
SFP Measurement Value	`show interface SFP detail`	Displays SFP measurement data.
SFP Measurement Alarm	`show interface SFP detail`	Displays SFP alarm information for the measurements.

View PKI trustpoint information

Configure the system to view PKI trustpoint related information including the validity from the Monitor Devices menu.

Use the View PKI Trustpoint tab to view PKI Trustpoint related information including the validity.

Minimum Supported Release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Control Components Release 20.13.1.

Procedure

1. From the Cisco SD-WAN Manager Menu, choose **Monitor** > **Devices**.
2. Choose a device from the list of devices that appear.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose **PKI Trustpoint**.

Option	Description
PKI Trustpoint	View PKI Trustpoint related information.

View Cisco Catalyst SD-WAN Validator information

Configure device monitoring to view Cisco Catalyst SD-WAN Validator orchestrator information including proxy mappings, statistics, and valid Cisco SD-WAN Manager instances.

View detailed information about Cisco Catalyst SD-WAN Validator orchestrator operations to monitor network performance and troubleshoot connectivity issues.

\

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands:

Device option	CLI Command	Description
Orchestrator Reverse Proxy Mapping	`show orchestrator reverse-proxy-mapping`	Displays the proxy IP addresses and port numbers that are configured for use by reverse proxy.
Orchestrator Statistics	`show orchestrator statistics`	Displays statistics about the packets that a Cisco Catalyst SD-WAN Validator has transmitted and received in the process of establishing and maintaining secure DTLS connections to a Cisco IOS XE Catalyst SD-WAN devices in the overlay network.
Orchestrator Valid vManage ID	`show orchestrator valid-vmanage-ID`	Lists the chassis numbers of the valid Cisco SD-WAN Manager instance in the overlay network.

View NMS server status

Verify the operational status of a Cisco SD-WAN Manager NMS server through the device monitoring interface.

Use this procedure when you need to verify the status of the NMS server on a Cisco SD-WAN Manager device to ensure proper network monitoring functionality.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a Cisco SD-WAN Manager device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose **NMS Server Running**.

Device option	Command	Description
NMS Server Running	`show NMS-server running`	Displays whether a Cisco SD-WAN Manager NMS server is operational. This device option is available from Cisco vManage Release 20.6.1.

View network-wide path insight

Provides information about network-wide path insight resources and documentation.

For information about network-wide path insight, see *Cisco Catalyst SD-WAN Network-Wide Path Insight User Guide*.

View multicast information

Configure multicast monitoring to view topology information, tunnels, and routing data through Cisco SD-WAN Manager.

View detailed multicast information including topology, tunnels, reverse-path forwarding, replicators, and OMP routes to monitor and troubleshoot multicast operations in your network.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the multicast commands.

Device option	Command	Description
Multicast Topology	`show multicast topology`	View topology information about the Multicast Domain
OMP Multicast Advertised Autodiscover or OMP Multicast Received Autodiscover	`show OMP multicast multicast-auto-discover`	View peers that support Multicast
Multicast Tunnels	`show multicast tunnel`	View information about IPsec tunnels between Multicast peers
Multicast RPF	`show multicast RPF`	View Multicast reverse-path forwarding information
Multicast Replicator	`show multicast replicator`	View Multicast replicators
OMP Multicast Advertised Routes or OMP Multicast Received Routes	`show OMP multicast-routes`	View Multicast routes that OMP has learned from PIM join messages

The selected multicast information displays in the Real Time view, showing relevant data based on the chosen command.

View loss percentage, latency, jitter, and octet information for tunnels

Configure tunnel monitoring to view loss percentage, latency, jitter, and octets for tunnels in a single chart option in Cisco SD-WAN Manager.

View the loss percentage, latency, jitter, and octets for tunnels in a single chart option in Cisco SD-WAN Manager.

You can choose the **Real Time** option or other time frames to view tunnel information in the graph.

Starting fromCisco IOS XE Catalyst SD-WAN Release 17.15.1a, you can also view tunnel information for **Packet Duplication**.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.
3. In the left pane, select **Tunnel** under the WAN area.

   The right pane displays information about all tunnel connections.
4. In the right pane, select **Chart Options** to choose the format in which you want to view the information.

   Choose **Loss Percentage/Latency/Jitter/Octets** for troubleshooting tunnel information.

The upper part of the right pane contains the following elements:

- Graph: Displays data for each tunnel over time.
- Legend: Identifies the tunnels shown in the graph. Select a tunnel to view data for only that tunnel. Each tunnel uses a unique color for its lines and data points.

The lower part of the right pane contains the following elements:

- Search bar: Includes Search Options, which lets you filter the table using Contains or Match criteria.
- Tunnel table: Lists jitter, latency, loss percentage, and other data for all tunnel endpoints. By default, the table selects the first six tunnels, and the graph displays data for those selected tunnels.
  1. Use the column drop-down lists to enable or disable descriptions.
  2. Select the check box next to a tunnel to select or deselect it. You can select and view data for a maximum of six tunnels at a time.

View logging information

Configure device monitoring to view logging information and syslog message settings on network devices.

Use this procedure when you need to access real-time logging information from network devices for monitoring and troubleshooting purposes.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options** and choose the logging command.

Device option	Command	Description
Logging	`show logging`	Displays the settings for logging syslog messages.

View license information

Configure license monitoring by viewing license information on a device through the Real Time monitoring interface.

View license information to monitor the licenses for software packages used by Cisco Catalyst SD-WAN.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose one of the following commands:

Device option	Command	Description
Smart License <info>	`show licenses`	Display the licenses for the software packages used by Cisco Catalyst SD-WAN.

View SAIE flows

View SD-WAN Application Intelligence Engine (SAIE) flow information including source IP address, destination IP address, and port details.

You can view SAIE flow information in both graphical format and in a table that shows application families sorted by usage. You can filter the data by VPN, Local TLOC, and traffic source, and view detailed information about applications and their source IP addresses.

The displayed peak usage for one time interval might be higher than the usage shown for another interval within the same time period. This can occur when the statistics database has not yet made all data available to Cisco SD-WAN Manager. Cisco SD-WAN Manager displays the available data and plots it on the corresponding axis.

Before you begin

1. For Cisco vManage Release 20.6.1 and later, add the required devices to the on-demand troubleshooting list:
   - Choose **Tools** > **On Demand Troubleshooting**.
   - In Cisco vManage Release 20.6.1 and earlier releases, access **On Demand Troubleshooting** from the **Monitor** menu.

2. Ensure that no Cisco or third-party APIs stop on-demand troubleshooting. Such API calls prevent the system from compiling the required information.
3. To improve application visibility, the device data collection process generates aggregated application-usage statistics. This reduces the size of the statistics files processed by the management plane and improves SAIE data collection efficiency.

Note

- In Cisco vManage Release 20.7.1 and earlier releases, SAIE flows are called deep packet inspection (DPI) flows.
- In Cisco vManage Release 20.7.1 and earlier releases, **SAIE Applications** is called **DPI Applications**.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Under **Applications** in the left pane, click **SAIE Applications**.

   The right pane displays SAIE flow information for the selected device.
3. Select **Filter** and choose the required VPN and Local TLOC.
4. Starting from Cisco Catalyst SD-WAN Manager Release 20.14.1, under **Traffic Source**, select **LAN traffic**, **Remote access traffic**, or both.
5. Select **Search** and choose a predefined or custom time period.

   Note

   Filtering **Local TLOC : Dia** is supported only for Cisco vEdge devices.

6. View the SAIE flow information in the graph.
   - Select an application family in the graph legend to display information for that flow.
   - Select the **Total Network Traffic** check box to display the flow as a proportion of total network traffic.
7. View the SAIE flow information in the table below the graph.
   - Review the applied filter criteria.
   - Review the application families sorted by usage. By default, the top six application families are selected.
   - Select or clear the check box next to an application family. You can select a maximum of six application families at a time.
   - Select an application family to view the applications within the family.
   - Select an application to view the source IP addresses of devices accessing the application. The **Traffic per TLOC** pie chart displays traffic distribution across TLOCs.

- Drag a column title to rearrange the table columns.

View Cisco Catalyst SD-WAN Controller policy

Outlines the process for viewing centralized data, application-aware, and cflowd policies pushed from Cisco Catalyst SD-WAN Controller to Cisco IOS XE Catalyst SD-WAN devices.

A centralized data policy is configured and applied on Cisco Catalyst SD-WAN Controller and distributed to edge devices through OMP updates. The policy applies to the edge devices included in the site list associated with the policy.

Centralized data policy examines packet header fields, including source and destination addresses, source and destination ports, protocol, and DSCP values. For matching packets, the policy can modify the next hop in various ways or apply a policer. The router performs policy matching and the resulting actions as it transmits or receives data traffic.

To view policy information from Cisco Catalyst SD-WAN Controller on a device, perform the following steps:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose one of the command below:

Device option	Command	Description
Policy from vSmart	`show sdwan policy from-vsmart`	Displays a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco Catalyst SD-WAN Controller has pushed to the Cisco IOS XE Catalyst SD-WAN devices.

View ACL information

Outlines how to view ACL information on local routers within the Cisco Catalyst SD-WAN overlay network.

Localized data policy, also known as access control lists (ACLs), is configured directly on a local router. It controls data traffic transmitted between routers over the Cisco Catalyst SD-WAN overlay network.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Select **Real Time** in the left pane.

4. Select **Device Options**, and choose one of the following commands:

Command	Description
`show policy access-list-names`	View names of configured ACLs
`show policy access-list-associations`	View Interfaces to which ACLs are applied
`show policy access-list-associations`	View count of packets affected by ACLs

Monitor NAT DIA tracker configuration on IPv4 interfaces

Configure monitoring of NAT DIA tracker configuration on IPv4 interfaces to view tracker information and status.

This task allows you to monitor and view information about DIA tracker configuration on transport interfaces.

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1.

You can view information about both single endpoint tracker and dual endpoint tracker configurations.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Select **Real Time**.
4. From the **Device Options** drop-down list, choose the appropriate tracker option.
   - For single endpoint tracker, choose **Endpoint Tracker Info**.
   - For dual endpoint tracker, choose **Endpoint Tracker Group Info**.

View control connections in real time

Configure a real-time view of the control plane connections on a Cisco vEdge device.

This task allows you to display a real-time view of the control plane connections on a Cisco vEdge device.

The control plane connection screen updates automatically every 15 seconds

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device.

3. Select **Troubleshooting** in the left pane.
4. Under the Connectivity area, select **Control Connections (Live View)**.

The upper part of the right pane shows figures that illustrate the operational control plane tunnels between the edge device, Cisco Catalyst SD-WAN, and Cisco SD-WAN Controller. The lower part of the lower pane contains a table that shows details for each of the control plane tunnels, including the IP address of the remote device and the status of the tunnel end points, including the reason for the failure of an end point.

View cloud express information

Configure monitoring to view Cloud Express information on devices through the real-time interface.

View Cloud Express information to monitor SaaS application performance and gateway quality metrics on devices.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands:

Device option	Command	Description
Cloud Express Applications	show sdwan cloudexpress applications	Displays the best path that Cloud onRamp for SaaS has selected for each configured SaaS application on Cisco IOS XE Catalyst SD-WAN devices.
Cloud Express Gateway Exits	`show sdwan cloudexpress gateway-exits`	Displays the Quality of Experience (QoE) measurements received from gateway sites, for Cloud onRamp for SaaS on Cisco IOS XE Catalyst SD-WAN devices.
Cloud Express Local Exits	`show sdwan cloudexpress local-exits`	Displays the list of applications enabled for Cloud onRamp for SaaS probing on Cisco IOS XE Catalyst SD-WAN devices, and the interfaces on which the probing occurs.

View cflowd information

Configure monitoring of Cflowd traffic flow information on routers in the overlay network using Cisco SD-WAN Manager.

View Cflowd flow information to monitor traffic flowing through routers in the overlay network. This allows you to access flow data exported to a collector that can be processed by an IPFIX analyzer.

Cflowd monitors traffic flowing through routers in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. For a traffic flow, Cflowd periodically sends template reports to a flow collector. These reports contain information about the flow and data extracted from the IP headers of the packets in the flow.

To configure Cflowd in a router, use centralized data policy to define a Cflowd template that specifies the location of a Cflowd collector and timers that control the flow collection.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices displayed.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands or options, as relevant:

Option	Description
Cflowd Template (**show app cflowd template**)	View the Cflowd template. Device option is displayed on Cisco vEdge devices.
Cflowd Collector (**show app cflowd collector**)	View Cflowd Collector information. Device option is displayed on Cisco vEdge devices.
Cflowd Flows (**show app cflowd flows**, **show app cflowd flow-count**)	View Cflowd flows. Device option is displayed on Cisco vEdge devices.
Cflowd Statistics (**show app cflowd statistics**)	View Cflowd statistics. Device option is displayed on Cisco vEdge devices.
cFlowd Flows/DPI (**show cflowd flows**)	View Cflowd traffic flow information and SAIE flow information. From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **cFlowd Flows/DPI** field is added for applying filters for monitoring specific SAIE applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Device option is displayed on Cisco IOS XE Catalyst SD-WAN devices.

Option	Description
cFlowd ipv6 Flows/DPI (**show cflowd flows**)	View Cflowd IPv6 traffic flow information and SAIE flows. From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1, the **cFlowd ipv6 Flows/DPI** field is added for applying filters for monitoring specific SAIE applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Device option is displayed on Cisco IOS XE Catalyst SD-WAN devices.

The selected Cflowd information displays, showing the relevant flow data, templates, collector information, or statistics based on your selection.

View BGP information

Configure BGP monitoring to view connection status, neighbors, and learned routes on routers.

View BGP information to monitor BGP configuration on routers and verify routing functionality on the service side of the device.

You can configure the BGP on routers to enable routing on the service side (site-local side) of the device, thus providing reachability to networks at the devices' local sites.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands as relevant:

Option	Description
BGP Summary (**show BGP summary**	View BGP connection status.
BGP Neigbors (**show BGP neighbor**)	View BGP neighbors.
BGP Routes (**show BGP routes**)	View routes learned by BGP.

The selected BGP information displays in the Real Time monitoring view, showing the current status, neighbors, or routes as requested.

BFD protocol

Describes a network protocol that detects link failures between routers and measures data loss and latency on data tunnels.

The BFD protocol is a network detection protocol that:

- detects link failures between routers.
- measures data loss and latency on data tunnels to determine the status of devices at either end of a connection.
- runs automatically on secure IPsec and GRE connections between routers to provide data plane resiliency.

BFD role in Cisco Catalyst SD-WAN solution

For data plane resiliency, Cisco Catalyst SD-WAN implements the BFD protocol. BFD runs automatically on the secure IPsec and GRE connections between routers. These connections carry data plane traffic and operate independently of the DTLS tunnels that the control plane uses.

BFD is enabled by default on all connections between Cisco vEdge device, and you cannot disable it.

However, you can adjust the Hello packet and dead time intervals. If the timers on the two ends of a BFD link differ, BFD negotiates the timers and uses the higher value to determine the transmission rate.

BFD operation process

Outlines the BFD operation process, including session establishment using TLOC information, periodic Hello packet exchanges, link failure detection, and the impact on route management within Cisco SD-WAN devices.

Summary

1. After a Cisco vEdge device comes up and establishes control connections, Cisco SD-WAN Controller advertises peer TLOC information to the Cisco vEdge device.
2. Based on this TLOC information and other configuration settings, Cisco vEdge device establish BFD sessions with all or some of the peer TLOCs.
3. BFD periodically sends Hello packets, every 1 second by default, to determine whether the session remains operational.
4. If BFD does not receive a specified number of Hello packets, it considers the link failed and brings the BFD session down. The default multiplier time is 7 seconds.
5. When a BFD session goes down, the router removes any route that points to a next hop over that IPsec tunnel from the forwarding table (FIB). The route remains in the route table (RIB).

Workflow

BFD session states

BFD sessions have three valid states:

- Down: The connection to another vEdge router is not operational.
- Init: The connection is reachable but not yet operational.
- Up: The connection to another vEdge router is operational.

Each device sends an echo request to its peer and sends an echo response for each request it receives. In the echo response, the device includes its current BFD state. The peer uses this state to determine whether it needs to change its own BFD state.

The following table shows how BFD session states change based on peer responses:

BFD Session State on Device	BFD State sent by Peer in Echo Response	BFD Status Change on Device
Up	Up or Init	Up (no change)
Up	Down	Down
Init	Up or Init	Up
Init	Down	Init (no change)
Down	Down	Init
Down	Init	Up
Down	Up	Down (no change)

Cisco SD-WAN, the number of TLOCs advertised to Cisco SD-WAN Controller determines the total number of BFD sessions. When a cEdge router establishes a control connection with Cisco SD-WAN Controller, it advertises its TLOC to the controller. The controller then propagates the TLOC information to all other Cisco devices in the network. The Cisco devices use this information to establish IPsec sessions with each other, which enables the BFD sessions to come up.

```
device# show sdwan bfd summary
sessions-total         1
sessions-up            1
sessions-max           12
sessions-flap          38
poll-interval           123400
```

The Cisco SD-WAN Manager dashboard displays the following results:

1. Control Connection Down: When the Cisco device loses its control connection to Cisco SD-WAN Controller, the total number of BFD sessions (`sessions-total`) becomes zero, and the number of active sessions (`sessions-up`) also becomes zero. Consequently, the BFD column displays `0/0`.
2. Underlay Issue: If the control connection to Cisco SD-WAN Controller remains up but an underlay issue causes the connectivity or IPsec session between two Cisco peer devices to go down, the total number of BFD sessions (`sessions-total`) remains 1.

   However, the number of active sessions (`sessions-up`) becomes zero. In this case, the BFD column displays `0/1`.

To understand the `restrict` and `max-control-connection` options, consider an overlay with two sites, each with two TLOCs, such as `private1` and `private2` on both ends. When all TLOCs remain up, the total number of BFD sessions (`sessions-total`) remains 4, and the number of active sessions (`sessions-up`) also remains 4. The BFD column therefore displays `4/4`.

- Restrict option: If the control connection to Cisco SD-WAN Controller remains up but you configure the TLOC color with the `restrict` option, the total number of BFD sessions (`sessions-total`) remains 3. The number of active sessions (`sessions-up`) also becomes 3. The BFD column therefore displays `3/3`.
- `max-control-connections 0` option: If the control connection to Cisco SD-WAN Controller remains up but you configure one TLOC on one site with

  ```
  max-control-connections
                0
  ```

  , the total number of BFD sessions (`sessions-total`) remains 3. The number of active sessions (`sessions-up`) also becomes 3. The BFD column therefore displays `3/3`.

When a BFD session goes down, traffic cannot flow between those TLOCs. If you identify traffic disruption between a pair of TLOCs or notice an increase in the session flap count, use the **show BFD sessions** or **show BFD history** commands to check the status of your BFD sessions. These commands help you determine whether the device has established all expected BFD sessions.

View BFD session information

Configure access to BFD session information and history for monitoring connection status between routers.

View BFD session information to monitor the status of Bidirectional Forwarding Detection sessions between routers and detect connection failures.

BFD sessions between routers start automatically when the devices come up in the network. BFD which runs on secure IPsec connections between the routers, is used to detect connection failures between the routers.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list, choose one of the following commands as relevant:
   - **BFD Sessions**: To view real-time BFD sessions
   - **BFD History**: To view BFD session history

View ARP table entries

Configure viewing of ARP table entries to display the mappings between network and physical addresses stored in the ARP table.

View the entries in the ARP table to examine the mappings between network layer addresses such as IPv4 addresses and link layer addresses such as Ethernet or MAC addresses.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that displays.
3. Select **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **ARP**.

   CLI equivalent: **show ARP**

View AppQoE information

Configure monitoring to view AppQoE information on devices using the Cisco SD-WAN Manager interface.

This task allows you to monitor and view AppQoE information on devices through the Cisco SD-WAN Manager interface.

Minimum release: Cisco vManage Release 20.9.1

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose one these commands.

Device option	Command	Description
AppQoE Active Flow Details	show sdwan appqoe flow flow-id [flow_id]	Displays the details of a single specific flow.
AppQoE Expired Flows Summary	show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows.
AppQoE Active Flows Summary	show sdwan appqoe flow VPN-id [vpn_id] server-port [server_port]	Displays flows for a specific VPN.
AppQoE Expired Flow Details	show sdwan appqoe flow closed flow-id [flow_id]	Displays the AppQoE Expired Flow details for a single specific flow.

View the system clock

Configure the system to display the system clock date and time on a device through the vManage interface.

Use this procedure to check the system clock on any device in your network through the Cisco SD-WAN Manager interface.

Minimum supported release: Cisco vManage Release 20.9.1

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose the following command:

Device option	Command	Description
System Clock	show clock	Displays the system clock date and time.

Run a traceroute

Configure traceroute functionality to trace the path that probe packets take through a network to reach a destination device.

Use traceroute to identify the path that probe packets take through the network to reach a destination device and troubleshoot connectivity issues.

From Cisco vManage Release 20.10.1, access the **Trace Route** option using one of these methods:

- Choose **Monitor** > **Devices**, click **...** next to the device name, and choose **Trace Route**.
- On the **Site Topology** page, select a device or tunnel name, and select **Trace Route** in the right navigation pane.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, select the device name in the **Hostname** column.
3. Select **Troubleshooting** in the left pane.
4. In the **Connectivity** area, select **Trace Route**.
5. In the **Destination IP** field, enter the IP address of the corresponding device in the network.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.
6. From the **VPN** drop-down list, choose the VPN that you want to use to reach the device.
7. From the **Source/Interface for VPN** drop-down list, choose the interface that you want to use to send the traceroute probe packets.
8. Select **Advanced Options**.
9. In the **Size** field, enter the size of the traceroute probe packets in bytes.
10. Select **Start** to run the traceroute to the requested destination.

The lower part of the right pane displays the following information:

- The raw output that shows the path that the traceroute probe packets take to reach the destination.
- A graphical representation that shows the path that the traceroute probe packets take to reach the destination.

View routing information

Configure access to routing information through the Cisco SD-WAN Manager interface to monitor network routing tables and protocols.

View routing information to monitor IP routes, forwarding tables, multicast FIB details, OMP peers and routes, and OSPF and PIM protocol status on network devices.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose one of the following commands AS relevant:

Device Options	Command	Description
IP Routes	show IP routes show ipv6 routes	Displays information about the IP route table entries. Displays the IPv6 entries in the local route table.
IP FIB	show IP FIB show ipv6 FIB	Displays information about forwarding table entries. Display the IPv6 entries in the local forwarding table.
IP MFIB Summary	show IP MFIB summary	Displays information about a summary of active entries in the multicast FIB.
IP MFIB OIL	show IP MFIB OIL	Displays information about outgoing Interfaces from the multicast FIB.
IP MFIB Statistics	show IP MFIB stats	Displays information about statistics for active entries in the multicast FIB.
OMP Peers	show OMP peers	Displays OMP peers and their peering sessions.
OMP Summary	show OMP summary	Displays information about the OMP sessions running between Cisco SD-WAN Controller and the routers.
OMP Received Routes or OMP Advertised Routes	show OMP routes show sdwan OMP routes	Displays OMP routes. From Cisco vManage Release 20.11.1, you can download OMP route details in JSON or CSV formats for Cisco IOS XE Catalyst SD-WAN devices.
OMP Received TLOCs or OMP Advertised TLOCs	show OMP tlocs	Displays OMP TLOCs.
OSPF Interfaces	show OSPF interface	Displays information about the Interfaces running OSPF.
OSPF Neighbors	show OSPF neighbor	Displays information about the OSPF neighbors.

Device Options	Command	Description
OSPF Routes	show OSPF routes	Displays routes learned from OSPF.
OSPF Database Summary	show OSPF database-summary	Displays a summary of the OSPF link-state database entries.
OSPF Database	show OSPF database	Displays information about the OSPF link-state database entries.
OSPF External Database	Not applicable	Display OSPF external routes. External routes are OSPF routes that are not within the OSPF AS (domain).
OSPF Processes	show OSPF process	Display the OSPF processes.
PIM Interfaces	show PIM interface	Displays information about interfaces running PIM.
PIM Neighbors	show PIM neighbor	Displays information about PIM neighbors.
PIM Statistics	show PIM statistics	Displays information about PIM-related statistics.
Interface Detail	show ipv6 interface	Displays information about IPv6 interfaces on Cisco Cisco IOS XE Catalyst SD-WAN devices. From Cisco vManage Release 20.6.1, this device option is available on all Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

Rediscover network

Configure network rediscovery to locate new devices in the overlay network and synchronize them with Cisco SD-WAN Manager.

Use network rediscovery to locate new devices that have been added to the overlay network and ensure they are properly synchronized with Cisco SD-WAN Manager for management and monitoring.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Rediscover Network**.
2. Choose a device or devices by checking the check box next to the device model.

   To find the device you are looking for scroll through the device table. Alternatively, choose a device group from the **Device Groups** drop-down list to see devices that belong to a specific device group.
3. To confirm resynchronization of the device data, select **Rediscover**.
4. In the **Rediscover Network** dialog box, select **Rediscover**.

The selected devices are rediscovered and synchronized with Cisco SD-WAN Manager, making them available for management and monitoring operations.

Feature history of network monitoring

Lists the development milestones and release information for network monitoring, including feature description.

This table describes the developments of this feature, by release.

Table 26: Feature history

Feature name	Release information	Description
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature provides a single chart option in Cisco SD-WAN Manager for viewing tunnel information, such as packet loss, latency, jitter, and octets.
Another Real Time Monitoring Support for Routing, License, Policy, and Other Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature adds support for real-time monitoring of numerous device configuration details, including routing, policy, Cloud Express, Cisco SD-WAN Validator, TCP optimization, SFP, tunnel connection, license, logging, and Cisco Umbrella information. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device. There are many device configuration details for Cisco SD-WAN Manager. However, only a subset of the device configuration details are added in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	This feature adds support for real-time monitoring for AppQoE and other device configuration details. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device. This feature adds support for real-time monitoring of AppQoE and other device configuration details in Cisco SD-WAN Manager.
Internet Outages	Cisco IOS XE Catalyst SD-WAN Release 17.9.2a Cisco Catalyst SD-WAN Control Components Release 20.9.2	The Internet Outages feature powered by Cisco ThousandEyes WAN Insights displays the internet outages on a map at the affected locations and end points.

Feature name	Release information	Description
Download Output of OMP Routes	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can download the output of the OMP Received Routes or OMP Advertised Routes real-time data for Cisco IOS XE Catalyst SD-WAN devices.
View Packet Duplication Information for Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.15.1aCisco Catalyst SD-WAN Manager Release 20.15.1	This feature provides a single chart option in Cisco SD-WAN Manager for viewing packet duplication information for tunnels.
View Tunnel Health on Multiple Remote Devices and Circuits	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature, add multiple remote devices and circuits to view the tunnel health data in the line chart. You can add a maximum of five devices at a time and the tunnel health data is displayed for each path.

Determine the status of network sites

Configure monitoring to determine the status of network sites within the Cisco Catalyst SD-WAN overlay network.

Determine the status of network sites to monitor the data connection states across your Cisco Catalyst SD-WAN overlay network.

A site is a particular physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each device at a site is identified by the same site ID.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. Locate the **Site BFD Connectivity** dashlet, which displays the state of data connections of a site.

   When a site has multiple edge devices, this dashlet displays the state of the entire site and not for individual devices. The **Site BFD Connectivity** dashlet displays three states:

   - Full WAN Connectivity: Total number of sites where all BFD sessions on all devices are in the up state.
   - Partial WAN Connectivity: Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
   - No WAN Connectivity: Total number of sites where all BFD sessions on all devices are in the down state. These sites have no data plane connectivity.

   Click any of these to view more details. The details are displayed in a pop-up window.

3. For the desired row, click **...** and choose **Device Dashboard**, **SSH Terminal**, or **Real Time**.

You will be redirected to the appropriate window based on your selection.

You can now monitor the status of network sites and view detailed information about their connectivity states.

View a configuration commit list

Configure device monitoring to view the configuration commit list on a device using Cisco vManage.

View the configuration commit list to monitor and track configuration changes made to a device.

Minimum supported release: Cisco vManage Release 20.9.1

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that is displayed.
3. Select **Real Time** in the left pane.
4. Select **Device Options**, and choose the following command:

Device option	Command	Description
Configuration Commit List	show configuration commit list	Displays the configuration commit list.

Run site-to-site speed test

Configure a site-to-site speed test to measure download and upload speeds between source and destination devices.

Use this task to test the network performance between two devices by measuring the download and upload speeds across tunnel interfaces.

Before you begin

Ensure that **Data Stream** is enabled under **Administration** > **Settings** in Cisco SD-WAN Manager.

Follow these steps to run a site-to-site speed test:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Connectivity** area, click **Speed Test**.
5. Specify the following parameters:
   - **Source Circuit**: From the drop-down list, choose the color of the tunnel interface on the local device.

- **Destination Device**: From the drop-down list, choose the remote device by its device name and system IP address.
- **Destination Circuit**: From the drop-down list, choose the color of the tunnel interface on the remote device.

6. Click **Start Test**.

The right pane shows the results of the speed test, the download, and upload speed between the source and destination. The download speed shows the speed from the destination to the source, and the upload speed shows the speed from the source to the destination in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table in the lower part of the right pane.

Note

From Cisco vManage Release 20.10.1, you can also access the Speed Test option as follows:

- On the **Monitor** > **Devices** page, select **...** adjacent to the device name and choose **Speed Test**.
- On the **Monitor** > **Applications** page, select **...** adjacent to the application name and choose **Speed Test**.
- On the **Site Topology** page, select a device name, and then select **Speed Test** in the right navigation pane.

Check application-aware routing traffic

Configure application-aware routing traffic monitoring to visualize traffic flow from source to destination devices.

This task allows you to check application-aware routing traffic from the source device to the destination device:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device from the list of devices that appears.
3. Select **Troubleshooting** in the left pane.
4. In the right pane, click **App Route Visualization** under **Traffic**.
5. From the **Remote Device** drop-down list, choose a destination device.
6. (Optional) Select **Traffic Filter**. Choose **No Filter** or **SAIE**.

   No Filter is chosen by default.

> **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.

7. Select **Go**.

   The lower part of the screen displays the traffic visualization data.

8. From the Chart Options drop-down list, choose one of these: Loss Percentage, Latency/Jitter, Octets.
9. (Optional) Choose a predefined or a custom time period on the left to view data for the specified time period.

You can now view and analyze application-aware routing traffic data between the selected source and destination devices. The visualization displays traffic metrics based on your selected chart options and time period.

From Cisco vManage Release 20.10.1, the **App Route Visualization** option is also accessible from the **Monitor** > **Applications** page. Click **...** adjacent to the application name and choose **App Route Visualization**.

View internet outages

Guides you to access and interpret the Internet outages map, which displays global Internet health statistics, including outage counts, affected locations, and impacted end points for the past 24 hours.

From the Cisco SD-WAN Manager menu, choose **Analytics** > **Internet Outages**.

The Internet outages map displays details about global Internet health over the last 24 hours, including number of outages, affected locations, and affected end points.

14 Insecure Configuration Management

Topics:

- Feature history for insecure configuration management
- Resilient infrastructure
- Enable insecure configuration management
- View insecure configurations

Feature history for insecure configuration management

Lists the development milestones and release information for insecure configuration management, including feature description.

This table describes the developments of this feature, by release.

Table 27: Feature history

Feature name	Release information	Description
Insecure configuration management	Cisco Catalyst SD-WAN Manager Release 26.1.1.1 Cisco IOS XE Catalyst SD-WAN Release 26.1.1	Provides centralized visibility and actionable remediation for insecure feature configurations to strengthen network security in Cisco Catalyst SD-WAN.

Resilient infrastructure

Describes Cisco's resilient infrastructure framework and explains how the Insecure Configurations tab in Cisco Catalyst SD-WAN provides visibility, guidance, and remediation insights.

Cisco's resilient infrastructure significantly strengthens the security posture of network devices. This multi-layer framework reduces the attack surface and protects sensitive data by modernizing security capabilities.

Core objectives

- Strengthen security: Ensures devices remain inherently secure against evolving threats.
- Reduce attack surface: Deprecates and removes obsolete capabilities to eliminate exploitation risks.
- Protect data: Deploys advanced security features to safeguard sensitive information.

For more information on resilient infrastructure, see <sd-wan playbook>

Insecure configurations tab overview

Configurations that no longer meet current security requirements and increase the risk of exploitation are considered insecure. The Insecure Configurations tab in Cisco Catalyst SD-WAN enables administrators to identify and remediate these vulnerabilities. It offers centralized visibility and actionable insights into insecure settings across devices, configuration groups, and templates managed by Cisco SD-WAN Manager.

Benefits of visibility into insecure configurations

- **Centralized visibility**

  Offers a consolidated dashboard to track insecure configurations present in the network.

- **Actionable guidance**

  Provides remediation steps for each detected insecure configuration, helping maintain compliance and security.

- **Operational assurance**

  Enables administrators to identify, prioritize, and resolve insecure settings before critical operations such as upgrades.

Enable insecure configuration management

Explains how to enable Insecure Configuration Mode in Cisco SD-WAN Manager, including steps for new deployments, upgrades, and cloud settings.

Use these steps to enable insecure configuration management.

For new networks: Insecure configuration mode is disabled by default. Administrators cannot deploy insecure configuration commands unless explicitly enabled.

For existing networks upgrading to Cisco Catalyst SD-WAN Manager Release 26.1.x: Insecure configuration mode will remain enabled. Administrators can review and remediate any insecure configurations already in use, then disable the mode if desired.

To view additional tabs such as Field Notices and Security Advisories, Cloud Services must be enabled in Admin Settings.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Admin** > **Settings** > **Insecure Configuration Mode**.
2. Click **enable**.

View insecure configurations

Explains how to view devices, configuration groups, and device templates with insecure configurations in Cisco SD-WAN Manager.

Use these steps to view and manage insecure configurations in Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Advisories**.
2. Select the **Insecure Configurations**.
3. Select **Devices** to view devices with insecure configurations.
4. Select **Configuration Groups** to view insecure configuration groups in your network.
5. Select **Device Templates** to view templates running insecure configurations.

What to do next

Review each insecure configuration by clicking its link to navigate directly to the relevant remediation section and apply the recommended fix. A periodic scan happens every 30 minutes to ensure the latest insecure configuration details are displayed.

15 Secure Cisco Catalyst SD-WAN with Live Protect

Topics:

- Feature history for Live Protect
- Live Protect for Cisco Catalyst SD-WAN
- Benefits of Live Protect
- Vulnerability Shield lifecycle
- Configure Live Protect for Cisco SD-WAN Control Components using Cisco SD-WAN Manager
- Disable Live Protect using Cisco SD-WAN Manager
- Monitor Live Protect

Feature history for Live Protect

Lists the development milestones and release information for OMP, including feature description.

This table describes the developments of this feature, by release.

Feature name	Release information	Description
Live Protect for Cisco SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.18.3	Live Protect allows customers to deploy compensating controls (called “Vulnerability Shields”) that protect Cisco products from Common Vulnerabilities and Exposures (CVEs) disclosed in Cisco Security Advisories. An advisory may disclose one or more CVEs, and a Vulnerability Shield may protect against one or more of those CVEs without requiring a device reload or service interruption. Because Vulnerability Shields may not address all vulnerabilities present in a software release and are intended as a temporary measure in place of the software fix, upgrading to the latest release containing the relevant software fixes is the recommended approach to address vulnerabilities in the long term Customers can deploy Vulnerability Shields in Monitoring mode or Enforcing mode. Live Protect allows customers to monitor, enforce, and deactivate Vulnerability Shields until they are retired when a software upgrade or patch is applied, designed to help customers achieve a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risk until software upgrades or patches are deployed.

Live Protect for Cisco Catalyst SD-WAN

Explains Live Protect within Cisco Catalyst SD-WAN, highlighting its core features, functional overview, and how it integrates with existing SD-WAN infrastructure.

Live Protect is a security capability that

- enables compensating controls and vulnerability mitigation without software upgrades or reboots,
- allows you to manage Vulnerability Shields through Cisco SD-WAN Manager to protect against known vulnerabilities before patching.

Deployment modes

You can deploy Vulnerability Shields in two modes:

- Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action.
- Protecting (Enforce) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities.

Benefits of Live Protect

Outlines the key advantages of deploying Live Protect, including enhanced security measures, operational simplicity, reduced risk, and improved network visibility for Cisco Catalyst SD-WAN deployments.

- Zero-downtime remediation: Provides temporary mitigation against vulnerabilities without requiring software upgrades or device reboots, designed to ensure continuous network availability until remediation.
- Dynamic security: Allows real-time enforcement of security policies.
- Flexible deployment: Allows you to deploy Vulnerability Shields in Monitoring mode to provide visibility into potential exploit attempts without enforcement, or in Enforce mode to actively apply mitigation policies and reduce exposure to known vulnerabilities.
- Centralized management: Allows you to manage Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components through Cisco SD-WAN Manager.
- Visibility: Provides hit statistics to help monitor Vulnerability Shield activity.

Vulnerability Shield lifecycle

Explains the lifecycle of Vulnerability Shields for Cisco Catalyst SD-WAN.

Vulnerability Shields are designed to provide interim mitigation for vulnerabilities on Cisco Catalyst SD-WAN Control Components releases. You may temporarily use a Vulnerability Shield until you upgrade to a software release that contains the fix or install another applicable, supported Vulnerability Shield.

Lifecycle policy scope

Outlines the lifecycle policy governing the publication, support, and retirement of Vulnerability Shields for Cisco Catalyst SD-WAN control components.

This lifecycle policy defines how Cisco publishes, supports, and retires Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components and Cisco IOS XE Catalyst SD-WAN devices .

This lifecycle applies to:

- Cisco Catalyst SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller
- The Live Protect Agent (Tetragon) integrated into the control-component software image
- Cloud-hosted and cloud-tethered Cisco Catalyst SD-WAN deployments

The lifecycle policy does not apply to:

- Cisco IOS XE Catalyst SD-WAN devices

- Air-gapped Cisco Catalyst SD-WAN deployments

Vulnerability Shield availability

Describes the lifecycle, deployment, and support policies for Vulnerability Shields used to protect Cisco Catalyst SD-WAN Control Components.

Cisco associates each Vulnerability Shield with a Cisco security advisory. A Vulnerability Shield can address one or more Common Vulnerabilities and Exposures (CVEs) identified in the advisory. Cisco SD-WAN Manager displays High and Critical security advisories and identifies the applicable Vulnerability Shields for affected Cisco Catalyst SD-WAN Control Components .

Availability and support policy

Policy item	Rule
Version support	Cisco creates Vulnerability Shields for the SD-WAN release that is current when the shield is published and for the two immediately preceding releases in each supported release train that includes Live Protect. In most cases, the current release already contains the fix for the vulnerability, so shields are created only for the two preceding releases. However, if an actively exploited vulnerability is disclosed before fixed software is available, Cisco may also create a shield for the current release.
Availability period	Cisco announces the download and support period when it publishes a Vulnerability Shield. The six-month period begins when Cisco releases a software fix for the vulnerability.
End of support	At the end of the six-month period, Cisco removes the Vulnerability Shield from download and ends support. Although the installed Vulnerability Shield is no longer supported, if it remains installed it will continue to operate until you manually remove it.
Software upgrades	Upgrading the SD-WAN devices and control-component software removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, reinstall the appropriate Vulnerability Shield or deploy another applicable Vulnerability Shield.

Vulnerability Shield lifecycle

Stage	Description
Day 0 – Publication	Cisco publishes the Vulnerability Shield, makes it available for download, and announces its six-month download and support period.
Day 1 – Deployment	Deploy the Vulnerability Shield in Monitoring, Protecting (Enforce), or Disabled mode. Cisco SD-WAN Manager applies the selected mode to all applicable Cisco Catalyst SD-WAN Control Components.

Day 2 – Operation	Cisco SD-WAN Manager displays the installed Vulnerability Shield and its operating mode. The Vulnerability Shield continues protecting the applicable SD-WAN control components, even if it is no longer supported by Cisco, until you remove it or upgrade the software.
Day N – Upgrade or end of support	A software upgrade removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, deploy the appropriate, supported Vulnerability Shield again, if any.

Note

After the six-month download and support period ends, an installed Vulnerability Shield continues operating in its existing mode until you manually remove it. Although Cisco no longer provides support or downloads for the shield, it is not automatically removed from the control component.

Note

Live Protect and its Vulnerability Shields may not fully mitigate risks during the device boot process, during which systems may remain temporarily exposed until security policies are initialized. They also do not mitigate the risk of system instability, including boot loops, resulting from incompatible Vulnerability Shields. Although Cisco uses commercially reasonable efforts to develop effective security technologies, Cisco does not represent or warrant that its offerings will provide absolute security or protect all files, systems, networks, or endpoints against all malware, malicious attacks, or other threats.

Configure Live Protect for Cisco SD-WAN Control Components using Cisco SD-WAN Manager

Provides step-by-step instructions for configuring Live Protect using Cisco SD-WAN Manager.

Use these steps to deploy and configure Live Protect Vulnerability Shields in Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Monitor** > **Advisories** > **Security Advisories**.
2. Select **Control Components** or **Devices** to display the relevant information for your infrastructure.
3. Select a specific security advisory to view its details.
4. Select **Affected Control Components**.
5. Choose **Deploy Shield**.

This shield is deployed to all applicable control components associated with the selected advisory. Individual control component selection for deployment is not supported.

6. Choose the desired mode:
   - Monitoring: Observes activity and logs events without blocking traffic.
   - Protecting (Enforce): Enforces security policies to actively block exploit attempts.

> **Note**
>
> Shields provide temporary mitigation for identified vulnerabilities until affected components are upgraded to a software version that includes remediation.
>
> Cisco strongly recommends upgrading to a software release containing the fix as soon as possible.

Disable Live Protect using Cisco SD-WAN Manager

Provides instructions for disabling a Live Protect shield.

Use these steps to disable a Live Protect shield.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Compliance** > **Advisories**.
2. Select the advisory for which you want to deactivate the shield.
3. Select **...** and choose **Disable Shield**.

Monitor Live Protect

Describes how to monitor live protect to ensure effective operation and proactive threat detection in Cisco Catalyst SD-WAN environments.

You can monitor Live Protect through shield status and event statistics.

View shield status for Live Protect

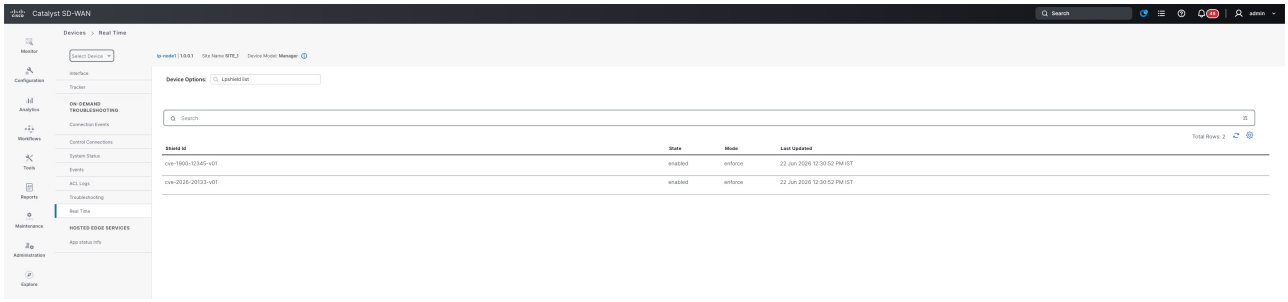
Demonstrates how to access shield status information, enabling users to verify Live Protect's real-time protection state across the Cisco Catalyst SD-WAN fabric.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Monitor** > **Devices**.
2. Select a device to open the Device360 page.
3. Select **real-time monitoring** from the drop-down list and choose **Lpshield List**.

The Lpshield List view displays the installed shield status on the selected device.

Figure 12: View shield status



View event statistics for Live Protect

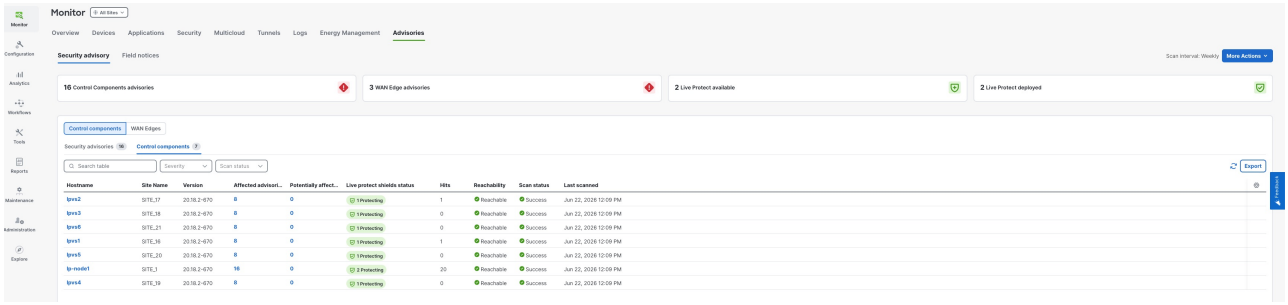
Explains how to access and analyze Live Protect event statistics, providing visibility into security events and supporting ongoing monitoring and troubleshooting for Cisco Catalyst SD-WAN solutions.

Procedure

1. From the Cisco SD-WAN Manager menu, go to **Monitor** > **Advisory**.
2. Select **Control Components**.

   The Hits field displays the event statistics for the deployed shields.

   Figure 13: View event statistics



16 Application Performance and Site Monitoring

Topics:

- Feature history of application performance and site monitoring
- Application performance and site monitoring
- Restrictions for application performance and site monitoring
- Configuring application performance and site monitoring
- Monitor application health
- Troubleshoot application performance and site monitoring

Feature history of application performance and site monitoring

Lists the development milestones and release information for application performance and site monitoring, including feature description.

This table describes the developments of this feature, by release.

Table 28: Feature history

Feature name	Release information	Description
Application Performance and Site Monitoring	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	You can monitor and optimize the application health and performance on all sites or a single site using Cisco SD-WAN Manager.

Application performance and site monitoring

Provides information about application health monitoring capabilities and metrics for performance assessment across sites.

The **Application Health** window displays various views of application performance data across different scopes and formats to help monitor application health status.

Application health display options

The **Application Health** window displays the following:

- All applications running in all sites: table view and heat map view.
- All applications running at a specific site: table view and heat map view.
- Single application running in all sites: table view and heat map view.
- Single application running at a specific site: aggregated line chart and per path table view.

Applications health metrics

The applications health is calculated as follows:

Table 29: Application health status based on QoE values

Health	QoE
Good	QoE >= 8
Fair	QoE 5~8
Poor	QoE < 5

Restrictions for application performance and site monitoring

Outlines the limitations and unsupported applications for performance monitoring in Application Performance and Site Monitoring.

Performance monitoring is supported only for IPv4 traffic.

These applications are not supported:

- airplay
- cisco-collab-control
- cisco-ip-camera
- cisco-jabber-control
- cisco-phone-control
- citrix
- clearcase
- conference-server
- conferencing
- espn-browsing
- espn-video
- exec
- FTP (all)
- google-downloads
- icloud
- isakmp
- isatap-ipv6-tunneled
- l2tp
- modbus
- oscar-filetransfer
- pcoip
- sixtofour-ipv6-tunneled
- skinny
- sunrpc
- telepresence-control
- tftp (all)
- vnc-http
- web-analytics
- webex-app-sharing

- webex-control
- webex-media
- windows-azure
- yahoo-voip-over-sip

Configuring application performance and site monitoring

Procedures, using different methods, for configuring application performance and site monitoring.

Use one of these methods to configure application performance and site monitoring:

- Configure application performance and site monitoring using configuration groups
- Configure application performance and site monitoring using a CLI add-on template

Configure application performance and site monitoring using configuration groups

Configure application performance and site monitoring using Cisco SD-WAN Manager by setting up Performance Monitoring under System Profile in a configuration group.

This task enables application performance and site monitoring functionality through configuration groups, allowing you to monitor application behavior and site performance metrics across your SD-WAN network.

You can enable application performance and site monitoring by configuring **Performance Monitoring** under **System Profile** in a configuration group.

Before you begin

Enable NBAR on all LAN interfaces to allow application performance and site monitoring to recognize applications.

If you configure an Application-Aware Routing (AAR) policy, NBAR is automatically enabled. If you do not configure an AAR policy, enable NBAR on all LAN interfaces using a CLI add-on template. Use the **ip NBAR protocol-discovery** configuration to enable NBAR on all LAN interfaces.

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure Performance Monitoring in a system profile.
   a) Enter Application Performance Monitoring information.

Table 30: Monitoring

Field	Description
Monitoring	To enable monitoring, check the check box. You can enable monitoring only in Global mode. Enabling monitoring displays a list of application groups. Fourteen application groups are enabled by default. You can disable or enable more applications based on your requirements. Check the check box adjacent to an application group to enable monitoring.

b) Enter Underlay Measurement Track Service information.

Table 31: Underlay Measurement Track Service

Field	Description
Monitoring	Click **Monitoring** drop-down list, and choose **Global** to trace tunnel paths regularly according to a configured time interval. Click the toggle button to enable the continuous monitoring option in UMTS.
Monitoring Interval (Minutes)	In the **Monitoring Interval (Minutes)** field, choose a time. This option enables you to monitor exact path at a specific time period.
Event Driven	Click the **Event Driven** drop-down list, and choose **Global** to trace tunnel paths when triggered by one of the events as per the event type.
Event Type	Click the **Event Type** drop-down list, and choose an event type. The event types are: • **SLA Change**: Change in the service-level agreement (SLA) parameter for the tunnel. • **PMTU Change**: Change in the Path MTU (PMTU) parameter for the tunnel.

3. To save the configuration, click **Save**.

What to do next

Refer to Deploy a Configuration Group.

Configure application performance and site monitoring using a CLI add-on template

Provides configuration steps for enabling application performance monitoring using the CLI Add-on feature template in Cisco SD-WAN Manager.

You can enable application performance monitor using the CLI Add-on feature template in Cisco SD-WAN Manager.

If you configure an Application-Aware Routing (AAR) policy, NBAR is automatically enabled. If you do not configure an AAR policy, enable NBAR on all LAN interfaces using a CLI add-on template. Use the **ip nbar protocol-discovery** configuration to enable NBAR on all LAN interfaces.

This example shows the application performance monitoring configuration.

```
class-map match-any APP_PERF_MONITOR_APPS_0
    match protocol attribute application-group amazon-group
    match protocol attribute application-group box-group
    match protocol attribute application-group concur-group
    match protocol attribute application-group dropbox-group
    match protocol attribute application-group google-group
```

```
    match protocol attribute application-group gotomeeting-group
    match protocol attribute application-group intuit-group
    match protocol attribute application-group ms-cloud-group
    match protocol attribute application-group oracle-group
    match protocol attribute application-group salesforce-group
    match protocol attribute application-group sugar-crm-group
    match protocol attribute application-group webex-group
    match protocol attribute application-group zendesk-group
    match protocol attribute application-group zoho-crm-group
class-map match-any APP_PERF_MONITOR_FILTERS
    match class-map APP_PERF_MONITOR_APPS_0

performance monitor context APP_PM_POLICY profile sdwan-performance
    exporter destination local-sdwan source NULL0
    traffic-monitor art-aggregated class-and APP_PERF_MONITOR_FILTERS
interval-timeout 300 sampling-interval 100
    traffic-monitor media-aggregated class-and APP_PERF_MONITOR_FILTERS
interval-timeout 300 sampling-interval 100

performance monitor apply APP_PM_POLICY sdwan-tunnel
performance monitor apply APP_PM_POLICY color-all-dia
performance monitor apply APP_PM_POLICY sdwan-sig
```

Monitor application health

Provides application monitoring capabilities across all sites and single sites with health status visualization through table and heatmap views.

The Applications window provides multiple views for monitoring application health across sites. Use these views to monitor all applications across all sites or focus on a specific site, application, or combination of both.

Viewing all applications across all sites

View the health and QoE of all applications across all sites.

By default, the Applications window opens in the All Sites view.

To view application health across all sites:

1. Select **All Sites** at the top of the page.
2. Select the **All Sites** radio button.

The All Sites view displays information for all applications across all sites for the last one hour.

The Health column displays the health of each application. Hover over the health icon to view the application health status as Good, Fair, or Poor. The application health is based on Quality of Experience (QoE).

To view application health in a heatmap, click the toggle button to switch to Heatmap view.

The heatmap displays application health as colored squares that represent Good, Fair, or Poor health. Hover over or click a square to view additional application details for a specific time. Select **View details** to view detailed application information.

Use the time interval drop-down list to change the displayed time interval.

Viewing all applications for a single site

View the health of all applications on a specific site.

To view the health of all applications on a specific site:

1. Select **All Sites** at the top of the page.
2. Select the **Single Site** radio button.
3. Select the site that you want to monitor.

The Applications window displays the health information for all applications on the selected site.

Viewing a single application across all sites

To view the health of a specific application across all sites:

1. Select **Site ID** to open single-site monitoring.
2. Select the application name to view application-specific details.

Viewing a single application on a single site

Monitor the health and QoE of a specific application on a selected site over time.

A line graph displays the application's health over a selected period. Use the time drop-down list to select 1, 3, 6, 12, or 24 hours.

The table below the graph lists the paths that processed application traffic during the selected period. Select individual paths to display their QoE lines on the graph. You can select up to five paths at a time, and the graph displays a line for each selected path.

To focus on a specific point in time, drag the handles at the top of the graph. When you change the time interval, the table automatically refreshes to display health information for the selected interval.

Viewing application health in table view

Lists the application health information displayed in the table view of the Application Health window.

The **Application Health** window displays application health in a table format and provides QoE-based health metrics across sites.

The Application Health window provides the following views:

- All applications for all sites: View a selected list of applications enabled through the performance monitoring feature or a CLI add-on template across all sites.
- All applications for a single site: View a selected list of applications enabled through the performance monitoring feature or a CLI add-on template for a single site.
- All sites for a single application: View all sites for a selected application enabled through the performance monitoring feature or a CLI add-on template. The table sorts the sites by the status in the **Health** column.

In the table, the **Health** column displays the application health. Hover over the health icon to view the Good, Fair, or Poor status. The application health uses QoE as its measurement.

Select the application name to view application-specific details. For a single application across all sites, select a **Site ID** to open single-site monitoring.

Select the toggle button to switch to the application heatmap view.

Viewing application health in heatmap view

Provides information about viewing application health data in the Application Health window using heatmap visualization.

The **Application Health** window displays application health in a heatmap across applications, sites, and time intervals.

The **Application Health** window provides the following views:

- All applications for all sites: View the health of all applications across all sites for different time intervals.
- All applications for a single site: View the health of applications enabled through the performance monitoring feature or a CLI add-on template for a selected site.
- All sites for a single application: View the health of a single application across all sites for different time intervals.

In the heatmap view, colored squares represent application health as **Good**, **Fair**, or **Poor**. Hover over or select a square to view application details for a specific time. Select **View details** to view detailed application information. Select the time interval from the drop-down list to change the displayed time interval.

Select the **Toggle** button to switch to the application table view.

Troubleshoot application performance and site monitoring

Documents commands and procedures for troubleshooting application performance and site monitoring metrics.

To check the basic network metrics used to calculate application QoE, run the **show performance monitor cache monitor APP_PM_POLICY-art_agg detail format record** and **show performance monitor cache monitor APP_PM_POLICY-media_agg detail format record** commands.

```
Device# show performance monitor cache monitor APP_PM_POLICY-art_agg detail
format record

 Monitor: APP_PM_POLICY-art_agg
 Data Collection Monitor:
  Cache type:                              Synchronized (Platform cache)
  Cache size:                                  112500
  Current entries:                                  6
  High Watermark:                                   6
  Flows added:                                      6
  Flows aged:                                       0
  Synchronized timeout (secs):                    300

FLOW DIRECTION:                            Output
TIMESTAMP MONITOR START:                   14:10:00.000
FLOW OBSPOINT ID:                          4294967298
INTERFACE OVERLAY SESSION ID OUTPUT:       0
IP VPN ID:                                 65535
APPLICATION NAME:                          layer7 share-point
connection server resp counter:            1477
connection to server netw delay sum:       10822  < --- SND_ samples
connection to server netw delay min:       100
connection to server netw delay max:       103
connection to client netw delay sum:       3559 < --- CND_ samples
connection to client netw delay min:       20
connection to client netw delay max:       198
connection application delay sum:          936
connection application delay min:          0
connection application delay max:          122
connection responder retrans packets:      2    <---- lost_samples
connection to server netw jitter mean:     0
connection count new:                      108      < ---- SND/CND_total
connection server packets counter:         2018     <---- total_samples

Latency(SND  ms) = SND_ samples/ SND/CND_total
Latency(CND  ms) = CND_ samples/ SND/CND_total
Loss ratio = lost_samples /total_samples
```

17 Managing Alarms

Topics:

- Feature history of alarms
- Alarms
- Viewing alarms
- Set alarm filters
- Filter alarm search results
- Export alarms
- Alarm notifications
- Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands
- Verify login rate alarms
- Safety barriers

Provides information about system monitoring capabilities including alarms, events, and logs.

Feature history of alarms

Lists the development milestones and release information for alarms, including feature description.

This table describes the developments of this feature, by release.

Table 32: Feature history

Feature	Release information	Description
Optimization of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature optimizes the alarms on Cisco SD-WAN Manager by automatically suppressing redundant alarms. This allows you to easily identify the component that is causing issues. You can view these alarms from the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
Grouping of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The enhancements are added to alarms: • Alarms are filtered and grouped for devices and sites based on severity. • View alarm details for a single site in the **Overview** dashboard. • View alarms for a particular device by clicking the … icon in the **Monitor>Devices** window. • View the top five alarms for a particular site in the **Monitor>Overview** window by choosing the **Site Topology** view icon and clicking the site. • View events related to an alarm in the **Related Event** column in the alarms filter.
Heatmap View for Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the alarms as **Critical**, **Major**, or **Medium & Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of alarms in a severity level.

Feature	Release information	Description
Alarm Notifications Using WebHooks	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Configure a WebHook URL in Cisco SD-WAN Manager to receive alarm notifications in Webex or Slack.
Alarm Notifications Using Custom WebHooks Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.x Cisco Catalyst SD-WAN Manager Release 20.16.1	Configure alarm notifications using custom webhooks over management VPN 512 for increased security in a single-tenant or a multitenant setup.
Cloud OnRamp for SaaS Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	A Cisco IOS XE Catalyst SD-WAN device triggers three new alarms. These alarms indicate the status of CoR-SaaS application paths. This feature adds a **path-status** field to the **cloudexpress-application-change** notification. Alarms are categorized into into Major, Medium and Minor based on the path status (unreachable, reachachable, disabled).
Policy Download Failure Alarm	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download fails.
Safety barriers	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Safety barriers protect the Cisco SD-WAN Controller during resource constraints by monitoring CPU, memory, and disk usage. When thresholds are exceeded, safety barriers generate alarms and restrict services that can further impact resource availability.

Alarms

Describes the alarm system that Cisco SD-WAN Manager uses to consolidate and display network events from overlay network devices.

An alarm is a consolidated notification mechanism that

- consolidates major and critical events from device notifications in the overlay network
- provides filtered and correlated event information through Cisco SD-WAN Manager, and
- displays detailed information about events from control components and routers.

Alarm generation and suppression

When something of interest happens on an individual device in the overlay network, the device reports it by sending a notification to Cisco SD-WAN Manager.

When a site is down, Cisco SD-WAN Manager reports these alarms:

- Site down
- Node down
- TLOC down

Cisco SD-WAN Manager can display alarms for each affected component. Depending on the size of your site, this can result in multiple redundant alarms. For example, when a node goes down, Cisco SD-WAN Manager might display an alarm for the node and separate alarms for each TLOC on that node.

From Cisco vManage Release 20.5.1, Cisco SD-WAN Manager suppresses redundant alarms. For example, when all TLOCs on a node go down, Cisco SD-WAN Manager suppresses the individual TLOC alarms and displays only the node alarm.

For multitenant configurations, each tenant displays alarms only for the sites in its tenancy.

Example of an alarm suppression

This table shows alarm suppression behavior in different scenarios:

Scenario	Alarms displayed	
	Cisco vManage Release 20.5.1	**Previous releases**
Link 1 down **Link 2 up.**	bfd-TLOC-1_down	bfd-TLOC-1_down
Link 1 down	bfd-site-1_down	bfd-site-1_down
Link 2 down	bfd-node-1_down, bfd-TLOC-1_down, and bfd-TLOC-2_down are suppressed by the site alarm.	bfd-TLOC-1_down
Link 1 up	bfd-site-1_up	bfd-site-1_up
Link 2 down	bfd-node-1_up bfd-TLOC-1_up bfd-TLOC-2_up	bfd-TLOC-1_up

Alarm states

Provides information about alarms generated when a state or condition changes in the overlay network, including alarm states, severity levels, and detailed field descriptions.

Cisco SD-WAN Manager assigns alarms a severity based on the impact of the condition.

- Critical (red): Indicates serious events that impair or shut down the operation of an overlay network function.
- Major (yellow): Indicates serious events that affect, but do not shut down, the operation of a network function.
- Medium (blue): Indicates events that might impair the performance of a network function.

- Minor (green): Indicates events that might diminish the performance of a network function.

> **Note**
>
> From Cisco vManage Release 20.11.1, the Medium alarms appear in green and the Minor alarms appear in blue.

Alarms lifecycle

Alarms listed as Active generally have a severity of Critical or Major.

When the condition associated with an alarm clears, most alarms clear automatically. For example, when a network element recovers, Cisco SD-WAN Manager sets the alarm's active field to false and lists the alarm as Cleared. The alarm severity generally changes to Medium or Minor.

Alarm fields

Outlines the fields present in alarm messages, including status indicators, device identifiers, timestamps, severity levels, possible causes, and unique identifiers, while detailing API usage for acknowledgment and batch processing improvements in Cisco SD-WAN alarms.

Alarm messages can contain these fields:

Table 33: Alarm fields

Field	Description
Acknowledged	Indicates whether the user has viewed and acknowledged the alarm. Cisco SD-WAN Manager uses this field to distinguish between alarms that have already been reported and those that have not yet been addressed. To acknowledge an alarm, use the following API post call: https://vmanage-ip-address:8443/dataservice/alarms/markviewed Specify the data as: {“uuid”: [<uuids of alarms to acknowledge>]}
Active	Indicates whether the alarm remains active. When a network element recovers and an alarm clears automatically, Cisco SD-WAN Manager sets this field to false.
Cleared By	Displays the UUID of the alarm that cleared the current alarm.
Cleared Time	Displays the time when Cisco SD-WAN Manager cleared the alarm. This field is present only when the active field is false.
Component	Identifies the software component associated with the alarm.
Devices	Lists the system IP addresses or router IDs of the affected devices.

Field	Description
Entry Time	Displays the time when Cisco SD-WAN Manager raised the alarm, in milliseconds and expressed as UNIX time.
Message	Displays a short message that describes the alarm.
Possible Causes	Lists the possible causes of the event.
Rule Name Display	Displays the name of the alarm. Use this name when querying for alarms of a particular type.
Suppressed	Indicates whether another alarm suppresses this alarm.
Tenant	Indicates the tenant ID.
Severity	Displays the severity of the alarm: critical, major, medium, or minor.
Severity Number	Displays the integer value for the severity: 1 (critical), 2 (major), 3 (medium), or 4 (minor).
UUID	Displays the unique identifier for the alarm.
Values	Displays a set of values for all affected devices. These values vary for each alarm and provide additional information beyond the values in the devices field.
Values Short Display	Displays a subset of the values field that summarizes the affected network devices.

Viewing alarms

Provides information about viewing alarms from the Cisco SD-WAN Manager dashboard and the Alarms screen, including filtering options and command-line methods.

View alarms from theCisco SD-WAN Manager dashboard by clicking the bell icon in the upper-right corner. Cisco SD-WAN Manager groups alarms into Active and Cleared categories.

View alarms from the Notifications pane in Cisco SD-WAN Manager

From Cisco vManage Release 20.11.1, when you click the bell icon at the top-right corner, the **Notifications** pane is displayed.

Click the gear icon to filter or group alarms based on these criteria:

- Object: Groups alarms by the device that generated the alarm.
- Severity: Groups alarms by alarm severity.
- Type: Groups alarms by alarm type.

By default, alarms are displayed for the last 24 hours.

Chart and table timestamps may not align if Cisco SD-WAN Manager's system clock is not synchronized with NTP or its time zone is configured incorrectly.

View alarms from the alarms screen in Cisco SD-WAN Manager

Alternatively, use these steps to view alarms from the **Alarms** screen in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.

   The alarms are displayed in graphical and tabular formats.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

2. To view more details for a specific alarm, click **...** for the desired alarm, and then click **Alarm Details**.

   The **Alarm Details** window opens and displays the probable cause of the alarm, impacted entities, and other details.

From Cisco vManage Release 20.11.1, a new column called **Related Event** is added to the alarms page. This column displays events related to an alarm that occur around the time the alarm is generated.

View alarms using CLI commands

- To display detailed information about each alarm, with each alarm separated by a new line, use the **show sdwan alarms detail** command.

```
vm5#show sdwan alarms detail

alarms 2023-06-01:00:38:46.868569
 event-name     geo-fence-alert-status
 severity-level minor
 host-name      Router
 kv-pair        [ system-ip=:: alert-type=device-tracking-stop
alert-msg=Device Tracking stopped in Geofencing Mode latitude=N/A
longitude=N/A geo-color=None ]
-----------------------------------------------------

alarms 2023-06-01:00:38:47.730907
 event-name     system-reboot-complete
 severity-level major
 host-name      Router
 kv-pair        [ ]
-----------------------------------------------------

alarms 2023-06-01:00:39:00.633682
 event-name     pki-certificate-event
 severity-level critical
 host-name      Router
 kv-pair        [ trust-point=Trustpool event-type=pki-certificate-install
valid-from=2008-11-18T21:50:24+00:00 expires-at=2033-11-18T21:59:46+00:00
is-ca-cert=true subject-name=cn=Cisco Root CA M1,o=Cisco issuer-name=cn=Cisco
 Root CA M1,o=Cisco serial-number=2ED20E7347D333834B4FDD0DD7B6967E ]
-----------------------------------------------------
```

- To display alarm information, such as the timestamp, event name, and severity, in a tabular format use the **show sdwan alarms summary** command.

```
vm5#show sdwan alarms summary

time-stamp                      event-name
         severity-1
-------------------------------------------------------------------------------------
2023-06-01:00:38:46.868569      geo-fence-alert-status
         minor
2023-06-01:00:38:47.730907      system-reboot-complete
```

```
         major
2023-06-01:00:39:00.633682      pki-certificate-event
         critical
2023-06-01:00:39:00.644209      pki-certificate-event
         critical
2023-06-01:00:39:00.649363      pki-certificate-event
         critical
2023-06-01:00:39:00.652777      pki-certificate-event
         critical
2023-06-01:00:39:00.658387      pki-certificate-event
         critical
2023-06-01:00:39:00.661119      pki-certificate-event
         critical
2023-06-01:00:39:00.665882      pki-certificate-event
         critical
2023-06-01:00:39:00.669655      pki-certificate-event
         critical
2023-06-01:00:39:00.674912      pki-certificate-event
         critical
2023-06-01:00:39:00.683510      pki-certificate-event
         critical
2023-06-01:00:39:00.689850      pki-certificate-event
         critical
2023-06-01:00:39:00.692883      pki-certificate-event
         critical
2023-06-01:00:39:00.699143      pki-certificate-event
         critical
2023-06-01:00:39:00.702386      pki-certificate-event
         critical
2023-06-01:00:39:00.703653      pki-certificate-event
         critical
2023-06-01:00:39:00.704488      pki-certificate-event
         critical
2023-06-01:00:39:01.949479      pki-certificate-event
         critical
2023-06-01:00:40:38.992382      interface-state-change
         major
2023-06-01:00:40:39.040929      fib-updates
         minor
2023-06-01:00:40:39.041866      fib-updates
         minor
```

Set alarm filters

Configure alarm filters to view alarms generated by specific sites or devices based on selected criteria.

Filter alarms based on object type, site or device, severity, type, and status to view alarms that match the specified criteria.

Cisco vManage Release 20.11.1, you can set filters to search for alarms generated by specific sites or devices. Cisco Catalyst SD-WAN Managerdisplays alarms in graphical and tabular formats. The heatmap view is available from CiscoCisco Catalyst SD-WAN Manager Release 20.12.1.

Procedure

1. From the Cisco Catalyst SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
2. Select **Filters**.
3. Enter or select the desired filter criteria:

- Object Type: Choose either **Site** or **Device**.
- Object List: Choose **Site ID** or **Device IP**. You can choose more than one site or device.
- Severity: Choose one or more alarm severity levels.
- Type: Choose one or more alarm names.
- Status: Choose the required alarm status value.

4. To add a filter, select the **+** button. You can add up to five filters. To delete a filter, select the **Bin** icon.

   The **Custom Filter Condition** enables you to filter alarms using the OR condition and the numbers of defined filters. For example, 1 OR 2 OR 3.

5. Click **Apply Filters** to view alarms that match the filter criteria.

Cisco Catalyst SD-WAN Manager displays alarms in graphical (heatmap) and tabular formats. The heatmap view is available from Cisco Catalyst SD-WAN Manager Release 20.12.1.

Filter alarm search results

Filter alarm search results by entity, severity, object, alarm type, message, status, and related event.

You can further filter the alarms shown in the search results table.

Procedure

---

1. From the Cisco Catalyst SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
2. Select the **Filter** icon in the search box.
3. Enter or select the desired filter criteria:
   - Impacted Entities: Enter text to search for in entity names.
   - Impacted Entities Details: Select a detailed listing of entity characteristics.
   - Severity: Specify one or more severity levels.
   - Object: Choose either the Site or Device object type.
   - Alarm Type: Specify one or more alarm types.
   - Message: Enter message text to include in the search.
   - Status: Choose active, cleared, or both types of alarm. Active alarms are currently on the device but have not been acknowledged.
   - Related Event: Select the related events to include in the search.
4. Select **Search** to find alarms that match the filter criteria.

Review the matching alarms in the search results table. You can add up to five filters. To delete a filter, select the **Bin** icon.

Export alarms

Provides the ability to export all alarm data to a CSV file for analysis and record-keeping purposes.

To export data for all alarms in CSV format, select **Export**.

Cisco SD-WAN Manager downloads the data from the alarms table to your browser's default download location. The CSV file uses the filename format <alarms-mm-dd-yyyy.csv>, where mm, dd, and yyyy represent the month, day, and year when you downloaded the file.

You can also find the alarm data displayed in the graph in the downloaded file.

For example, if the graph displays the following alarm data at 15/Feb/2022 3:30 AM–Critical: 2, Major: 274, Medium: 4, and Minor: 405–the downloaded file contains the same alarm data for the 15/Feb/2022 3:00 AM to 3:29 AM time range.

Alarm notifications

Guides configuration and management of alarm email notifications, including setup, sending, viewing, editing, and deleting notifications, to ensure prompt alert delivery and administration.

You can configure and manage alarm notifications in Cisco SD-WAN Manager, including email and webhook delivery settings. You can also specify the alarm conditions and devices that trigger notifications and view, edit, or delete configured notifications.

Enable email notifications

You can configure Cisco SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

The email is sent from Cisco SD-WAN Manager Public-IP of VPN0 (Transport Interface) as a source interface.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Alarm Notifications**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Select the **Email Settings** check box.
4. Select the security level for sending email notifications. You can select **None**, **SSL**, or **TLS**.
5. In the SMTP Server field, enter the name or IP address of the SMTP server that receives the email notifications.
6. In the SMTP Port field, enter the SMTP port number. Use the following default ports:
   - 25 for no security
   - 465 for SSL
   - 587 for TLS
7. In the From address field, enter the full email address to use as the sender of email notifications.
   a) In the Reply to address field, enter the full email address to use in the Reply-To field of the email. You can use a noreply address, such as `noreply@cisco.com`.
8. Select the **Use SMTP Authentication** check box to enable SMTP authentication with the SMTP server.

Enter the username and password for SMTP authentication. Cisco SD-WAN Manager appends the default user email suffix to the username and hides the password as you enter it.

9. Select **Save**.

Send alarm notifications

Before you begin

Ensure that Email Notifications are enabled under **Administration** > **Settings**, check whether **Alarm Notifications** is enabled and, **Email Settings** check box is checked.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, select the toggle button to enable cloud services.

From Cisco Catalyst SD-WAN Manager Release 20.15.1, configure Slack or Webex webhooks to receive alarm notifications.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms** or choose **Monitor** > **Alarms**.
2. Select **Alarm Notifications**. The table displays the configured alarm notifications.
3. Select **Add Alarm Notifications**.
4. In the **Notification Name** field, enter a name for the email notification. The name can contain up to 128 alphanumeric characters.
5. Expand the **Alarm Type** filter and configure the following parameters:
   a. Expand the **Alarm Type** filter and configure the following parameters:
      - From the **Object Type** drop-down list, choose the site or device for which you want to receive alarms.
      - From the **Object List** drop-down list, choose the site ID or device based on the selected object type.
      - From the **Severity** drop-down list, choose the alarm severity.
      - From the **Types** drop-down list, choose the alarm type.
6. Expand the **Delivery Method** filter and configure one or both of the following delivery methods:
   a) Select the **Email** check box to send an email when an alarm notification event occurs.
      1. In the **Email** field, enter one or more email addresses.
      2. (Optional) Select **Add New Email List** and enter an email list.
      3. In the **Email Threshold** field, enter the maximum number of emails to send per minute. Enter a value from 1 through 30. The default value is 5.

   b) Select the **WebHook** check box to send an HTTP callback to a webhook channel when an alarm notification event occurs.
      1. From the **Choose a Channel for Webhook** drop-down list, choose the webhook channel to receive alarm notifications:
         - Cisco Webex
         - Slack
         - Custom
      2. In the **WebHook URL** field, enter the URL of the webhook server.

To create a webhook URL for Slack, see the Sending messages using incoming webhooks section at *api.slack.com*.

To create a webhook URL for Webex, see Incoming Webhooks in Webex App Hub.

3. In the **WebHook Threshold** field, enter the maximum number of notifications to send to the webhook URL per minute. Notifications generated beyond this threshold are not delivered.

   For example, if you set **WebHook Threshold** to 2, the system sends a maximum of two notifications to the webhook URL per minute.

4. (Optional) Starting with Cisco Catalyst SD-WAN Manager Release 20.16.1, if you choose **Custom** from the **Choose a Channel for Webhook** drop-down list, configure the following additional parameters:

Field	Description
Username	Enter a username for authentication.
Password	Enter a password for authentication.
Network Connectivity	
Source VPN	From the drop-down list, choose a source VPN. • **0**: Transport VPN • **512**: Management VPN. Configure these fields if you have specified the tenant to manage the webhook notification services. These fields do not appear if they are managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet (VXLAN tunnel VPN IP subnet) where the webhook server is located. • (Optional) **Destination VPN**: Enter the destination VPN of the webhook server.

> **Note**
>
> Starting Cisco IOS XE Catalyst SD-WAN Release 26.2.1, when you configure tenant-managed notification rules using the `/dataservice/notifications/rule` API, the VPN and VPN IP Subnet fields are mandatory if source VPN is set to 512.
>
> For more information, see Update Notification Rule.

7. Select **Add**.

Viewing email notifications

Use these steps to view email notifications.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms** or **Monitor** > **Alarms**.
2. Select **Alarm Notifications**. The table displays the configured alarm notifications.
3. For the notification you want to view, click the **View** icon to the right of the row.
4. After you finish viewing the notification, click **OK**.

Edit an email notification

Use these steps to edit an email notification.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms** or **Monitor** > **Alarms**.
2. Select **Alarm Notifications**.

   A list of configured notifications is displayed in the table.
3. For the desired email notification, select the **Edit** icon.
4. When you are done editing the notification, select **Update**.

Delete an email notification

Use these steps to delete an email notification.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms** or **Monitor** > **Alarms**.
2. Select **Alarm Notifications**. The table displays the configured alarm notifications.
3. For the email notification you want to delete, click the **Trash Bin** icon.
4. In the confirmation dialog box, select **OK**.

Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands

Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands to enable alarms when login attempts reach a specified threshold.

This procedure enables an alarm when the number of logins to the Cisco SD-WAN Manager reaches a specified threshold.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

By default, CLI templates execute commands in global config mode.

Procedure

1. Enter system configuration mode.

   Example

   ```
   system
   ```

2. Enter alarms configuration mode.

   Example

   ```
   alarms
   ```

3. Configure a login-rate threshold.

   The **interval** keyword indicates the time span in which to count logins to Cisco SD-WAN Manager. The **num-logins** keyword specifies the number of logins within the specified interval that trigger an alarm.

   See login-rate for information about the ranges for each parameter.

   The **login-interval** and **num-logins** keywords do not have default values.

The login-rate alarm threshold is configured.

This example shows a login-rate threshold configuration that generates an alarm after three login attempts occur within 60 seconds:

```
system
 alarms
  login-rate
   interval 60
   num-logins 3
  !
 !
!
```

Verify login rate alarms

Details how to verify login rate alarms by using commands to check alarm configurations, review the history of failed login attempts, and identify system-login-rate alarm events.

Use these commands to verify login rate alarms.

To verify the login rate alarm configuration, use the **show running-config system alarms** command:

```
vmanage# show running-config system alarms
system
 alarms
  login-rate
    interval 60
      num-logins 3
      !
    !
  !
```

To view the history of failed login attempts, use the **show alarms history** command:

```
vmanage# show alarms history | inc aaa-user
07/10     16:07:18       aaa-login-anomaly    major    user-name:test
remote:host:192.0.2.1
07/10     16:07:10       aaa-login-anomaly    major    user-name:test
remote:host:192.0.2.1
07/10     16:07:00       aaa-user-locked      major    user-name:test
remote:host:192.0.2.1
```

To view alarms configured by the **login-rate** command, showing when the number of logins to Cisco SD-WAN Manager exceeds a configured threshold, use the **show alarms history** command, and view alarms of type **system-login-rate**:

```
vmanage# show alarms history

DATE    TIME        TYPE                    SEVERITY    DETAILS
---------------------------------------------------------------
07/10   16:08:05   system-login-rate     minor    num-logins:3 time-interval:60
 login-message:3 logins were done in 0 hours 1 minutes 8 seconds
07/10   16:08:05   system-login-change    minor    user-name:admin
user-id:145
```

Safety barriers

Explains resource protection mechanisms that prevent system-wide critical failures on Cisco Catalyst SD-WAN Controller controllers during high resource utilization.

Safety barriers protect Cisco Catalyst SD-WAN Controllers when system resources, such as CPU, memory, or disk space, reach high utilization. The feature safeguards system resources by restricting certain operations and generating alarms in Cisco SD-WAN Manager. These actions help maintain system stability and prevent critical system failures.

Default behavior

To enable safety barriers, enter:

```
Device(config)# system safety-barriers
```

Before Cisco Catalyst SD-WAN Manager Release 26.2.1, safety barriers were disabled by default. Cisco Catalyst SD-WAN Manager applies CPU and memory restrictive actions only after you configure the safety barriers.

From Cisco Catalyst SD-WAN Manager Release 26.2.1, Cisco enables safety barriers by default. To disable safety barriers, enter:

```
vSmart(config)# no system safety-barriers
```

This feature operates automatically to manage daemon resources and improve system stability under high load, with no additional configuration required. To disable safety barriers, you can use CLI or CLI template. For example,

```
vSmart(config) # no system safety-barriers
```

When you disable safety barriers, Cisco SD-WAN Manager does not apply the CPU and memory restrictive actions.

Safety barrier alarms

For more information about safety barrier alarms, see the Alarm Details section in *Cisco IOS XE Catalyst SD-WAN Alarms Guide*.

CPU barrier

Cisco SD-WAN Manager generates a CPU Barrier alarm when CPU utilization exceeds 80 percent for 300 seconds.

When the CPU barrier becomes active, Cisco SD-WAN Manager takes the following actions:

- Delays system and policy configurations from Cisco SD-WAN Manager and retries them for five minutes before reporting a failure.
- Rejects the following `show` commands:
  - **show omp tlocs**
  - **show omp services**
  - **show omp routes**
  - **show omp ipv6-routes**
  - **show omp peer**
  - **show omp l2-statuses**
  - **show omp l2-services**
  - **show omp l2-routes**
  - **show tenant omp**
  - **show internal/support omp rib vroute**
  - **show internal/support omp rib-list**
  - **show internal/support ttmd groups**
  - **show internal/support ttmd links**
  - **show internal/support ttmd tlocs**
- Rejects the **clear omp all** command.

Disk barrier

Cisco SD-WAN Manager generates a Disk Barrier alarm when disk utilization exceeds 80 percent for five seconds.

When the disk barrier becomes active, Cisco SD-WAN Manager cleans up core files and admin-tech files based on their age. The files are deleted in this order:

1. Admin techs and image files in home directories older than 2 days,
2. crash files in /var/crash/ older than 30 days,
3. admin tech files in /var/admin-tech older than 30 days,
4. crash files in /var/crash/ older than 7 days,
5. admin tech files in /var/admin-tech older than 7 days,
6. crash files in /var/crash/ older than 2 days
7. admin tech files in /var/admin-tech older than 2 days.

Memory barrier

Cisco SD-WAN Manager generates a Memory Barrier alarm when memory utilization exceeds 80 percent for 300 seconds.

When the memory barrier becomes active, Cisco SD-WAN Manager takes these actions:

- Prevents new control connections for new edge sites added to the overlay.
- Rejects attempts to clear control connections.
- Prevents new OMP peerings.
- Prevents new RIB-in entries for existing peers.
- Prevents configuration of Control Policy sequences that use **Set TLOC**, **Set TLOC-List**, or **Set Service**.

18 Managing events

Topics:

- Feature history of events
- Events
- Viewing events
- Set event filters
- Filter event search results
- Export events
- Monitor event notifications

Feature history of events

Lists the development milestones and release information for events, including feature description.

This table describes the developments of this feature, by release.

Table 34: Feature history

Feature Name	Release Information	Description
Event Notifications Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for event notifications, for Cisco IOS XE Catalyst SD-WAN devices.
Monitoring Event Trace for OMP Agent and SD-WAN Subsystem	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables monitoring and controlling the event trace function for a specified SD-WAN subsystem. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems.
Grouping of Events	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	The enhancements added to events include: • Events are filtered and grouped based on severity for devices and sites. • View events for a particular device by clicking the … icon in the **Monitor** > **Devices** window. • View the top five events for a particular site in the **Monitor** > **Overview** window by choosing the **Site Topology** view icon and clicking the site.
Heatmap View for Events	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the events as **Critical**, **Major**, or **Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of events in a severity level.
Policy Enforcement Status	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download is successful.

Events

Explains how overlay network devices report events through Cisco SD-WAN Manager, SNMP traps, and syslog, including event storage and time-zone behavior.

When an event occurs on a device in the overlay network, the device reports it through the following mechanisms:

- Cisco SD-WAN Manager: The device sends a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager filters the notifications, correlates related events, and consolidates major and critical events into alarms.

- SNMP: The device sends an SNMP trap to the configured trap target. For each SNMP trap, the device also generates a corresponding notification message.
- Syslog: The device generates a system logging (syslog) message and stores it in a syslog file in the `/var/log` directory on the local device and, if configured, on a remote device.

Notifications are messages that devices send to the Cisco SD-WAN Manager server.

> **Note**
>
> Cisco SD-WAN Manager displays all task logs, including activity, administration, and device logs, in UTC. UTC is the default and only supported time zone for these logs, regardless of the target file or local time zone settings.

A Cisco IOS XE Catalyst SD-WAN device can store a maximum of 256 events. When the device reaches this limit, it drops the oldest events. Cisco SD-WAN Manager might not receive events that the device drops.

Viewing events

: Explains multiple approaches to view events, including using SD-WAN Manager, executing CLI commands, and monitoring failover events, to ensure comprehensive event access and visibility.

Use one of these methods to view events.

- Viewing events using Cisco SD-WAN Manager
- Viewing events using CLI Commands
- Viewing failover events

Viewing events using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.

   The screen displays events in both graphical and tabular format.

   Chart and table timestamps may not align if Cisco SD-WAN Manager's system clock is not synchronized with NTP or its time zone is configured incorrectly.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays the events.

2. Select **...** and choose **Device Details** to view detailed information about any event generated on a device.

Viewing events using CLI Commands

Provides information about viewing events using CLI commands.

To view information about the device on which an event occurred, use the **show sdwan notification stream** command.

The output includes the following information:

- The first line displays the time when the system generated the message (`eventTime`). The system displays the time in UTC, not in the device's local time.
- The second line identifies the event.
- The third line displays the severity level.

- The remaining lines provide additional information about the event.

For example:

```
Device# show sdwan notification stream
notification
 eventTime 2020-03-03T02:50:04.211317+00:00
sla-change
  severity-level major
  host-name SanJose
  system-ip 4.4.4.103
  src-ip 10.124.19.15
  dst-ip 10.74.28.13
  proto ipsec
  src-port 12426
  dst-port 12346
  local-system-ip 4.4.4.103
  local-color default
  remote-system-ip 4.4.4.106
  remote-color biz-internet
  mean-loss 17
  mean-latency 13
  mean-jitter 19
  sla-classes None
  old-sla-classes Voice-And-Video
!
```

Viewing failover events

Provides procedures to view events in the monitoring interface and details about failover events.

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

Failover events notify you when a SIM failover occurs. A SIM failover occurs when the active cellular link loses connectivity and the device switches from the current SIM or carrier to the other SIM or carrier.

When a SIM failover occurs, the device sends a sim-fail-over event to Cisco SD-WAN Manager.

Set event filters

Configure event filters to view events based on object type, site or device, severity, and event name.

Filter events to view events that match specific criteria.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Select the **Filters** option.
3. Enter or select the desired filter criteria:
   - Object Type: Choose either **Site** or **Device**.
   - Object List: Choose the site ID or device IP. You can choose more than one site or device.
   - Severity: Choose one or more event severity levels.
   - Type: Choose one or more event names.

   Select the **+** icon to add up to five filters. Select the **Bin** icon to delete a filter.

The **Custom Filter Condition** enables you to filter events using the OR condition and the numbers of defined filters. For example, 1 OR 2 OR 3.

4. Click **Apply Filters** to view events that match the filter criteria.

Cisco SD-WAN Manager displays filtered events in graphical (heatmap) and tabular formats. The heatmap view is available from Cisco Catalyst SD-WAN Manager Release 20.12.1.

Filter event search results

Filter event search results by event time, hostname, system IP, name, severity, and details.

You can further filter the events shown in the search results table.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Select the **Filter** icon in the search box.
3. Enter or select the desired filter criteria:
   - Event Time: Choose the event time from the drop-down list.
   - Hostname: Choose the hostname from the drop-down list.
   - System IP: Choose the system IP of the device to view generated events.
   - Name: Choose one or more event names.
   - Severity: Choose the event severity level. Events generated by Cisco IOS XE Catalyst SD-WAN devices are classified as follows:
     - Critical: Action needs to be taken immediately.
     - Major: The problem needs immediate attention but is not critical enough to bring down the network.
     - Minor: The message is informational only.
   - Details: Choose the relevant event details from the drop-down list.
4. Select **Search** to find events that match the filter criteria.

Export events

Provides instructions for exporting event data to a CSV file format.

To export data for all events to a file in CSV format, select **Export**.

Cisco SD-WAN Manager downloads data from the events table to the default download location of your browser. The data is downloaded as a CSV file with the name <events-mm-dd-yyyy.CSV>, where mm, dd, and yyyy are the month, day, and year that the file was downloaded.

Monitor event notifications

Provides information about monitoring and controlling event trace functions for SD-WAN subsystems using the monitor event-trace command.

To monitor and control the event trace function for a specified SD-WAN subsystem, use the **monitor event-trace** command in privileged EXEC mode.

Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems. For more information on the commands, see monitor event-trace sdwan and show monitor event-trace sdwan.

19 System and Network Logs

Topics:

- Feature history of logs
- Set ACL log filters
- Audit logging
- Viewing the logs of configuration template activities
- Syslog messages
- Cisco SD-WAN Manager log files
- Viewing the log of certificate activities
- Traffic logs
- Binary Trace for Cisco Catalyst SD-WAN Daemons

Information about system and network logs.

Feature history of logs

Lists the development milestones and release information for logs, including feature description.

This table describes the developments of this feature, by release.

Table 35: Feature history

Feature name	Release information	Description
Compare template configuration changes using Audit Logs	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces a Config Diff option for audit logs of device templates and feature templates. The Config Diff option compares the current and previous configurations to show the configuration changes made to the template. You can use the Config Diff option to view configuration changes when a template is not attached to a device.
Enhancements to Audit Logging	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature introduces enhanced audit logging to monitor unauthorized login activity.
Manage Log Size	Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature allows you to temporarily increase the log size for troubleshooting purposes.
Binary Trace for Cisco Catalyst SD-WAN Daemons	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Binary trace enhances the troubleshooting of Cisco Catalyst SD-WAN daemons. Binary trace logs messages from the daemons in a binary format. Messages are logged faster in the binary format, improving the logging performance, using less storage space than in the ASCII format. The binary trace CLI allows you to set the debug levels for additional process modules compared to the debug command. From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, binary trace is supported for the following Cisco Catalyst SD-WAN daemons: • fpmd • ftm • ompd • vdaemon • cfgmgr

Set ACL log filters

Configure filters to view access control list (ACL) logs for routers in Cisco SD-WAN Manager.

Filter ACL logs to view specific access control list activities for routers in your network.

Use the ACL Log screen to view logs for access lists (ACLs) configured on a router. Routers collect ACL logs every 10 minutes.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **ACL Log**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **ACL Log**.
2. Select **Filter**.
3. In the VPN field, choose the entity, for which you are collecting ACL logs, from the drop-down list.

   You can choose only one VPN.
4. Select **Search** to search for logs that match the filter criteria.

Cisco SD-WAN Manager displays a log of activities in table format.

Audit logging

Audit logging

View audit log information

Configure audit log viewing to monitor and review system activities in both table and graphical formats.

View audit log information to monitor system activities, track configuration changes, and maintain system accountability.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Audit Log**.

   Note

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Audit Log**.

   Cisco SD-WAN Manager displays a log of activities both in tabular and graphical format.
2. Optional: Select **Filter** and choose one or more modules to filter the view.

   You can choose more than one **Module** type.
3. Optional: Select **Export**, to export data for all audit logs to a file in CSV format.

Cisco SD-WAN Manager downloads all data from the audit logs table to an Excel file to a CSV format. The file is downloaded to your browser's default download location and is named Audit_Logs.CSV.

4. Optional: To view detailed information about any audit log, for the desired row in the table, select **...** and choose **Audit Log Details**.

   The **Audit Log Details** dialog box opens, displaying details of the audit log.

5. Optional: To view configuration changes made to a **Template** type **Module**, for the desired row in the table, select **...** adjacent to a log row for a template module, and choose **Config Diff**.

   > **Note**
   >
   > You can view changes to previous and current configurations made only where the module type is template.

   The Config Difference pane displays a side-by-side view of the differences between the configuration that was originally in the template and the changes made to the configuration. To view the changes inline, select **Inline Diff**.

6. Optional: To view the updated configuration on the device, select **Configuration**.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco SD-WAN Release 20.6.1, the **Audit Logs** option displays the actions performed for template and policy configuration changes.

   To view the previous and current configuration for an action, select **Audit Log Details**. Cisco SD-WAN Manager collects audit logs when you create, update, or delete device or feature templates and localized, centralized, or security policies. The audit logs display changes in the API payloads for templates and policies, regardless of whether you attach them to devices.

Protection against unauthorized login activity

Provides information about audit logs and enhanced login monitoring capabilities for tracking unauthorized login activities.

Cisco SD-WAN Manager displays a log of activities both in table and graphical format. These logs enable traceability which is essential in co-management environments and for governance purposes. It provides insights in the form of events which are generated based on the audit logs. From Cisco Catalyst SD-WAN Manager Release 20.12.1, the audit logs are enhanced to capture high login frequency and failed login attempts to Cisco SD-WAN Manager.

Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands

Configure a login-rate alarm threshold for Cisco SD-WAN Manager using CLI commands to enable alarms when login attempts reach a specified threshold.

This procedure enables an alarm when the number of logins to the Cisco SD-WAN Manager reaches a specified threshold.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

By default, CLI templates execute commands in global config mode.

Procedure

1. Enter system configuration mode.

Example

```
system
```

2. Enter alarms configuration mode.

   Example

   ```
   alarms
   ```

3. Configure a login-rate threshold.

   The **interval** keyword indicates the time span in which to count logins to Cisco SD-WAN Manager. The **num-logins** keyword specifies the number of logins within the specified interval that trigger an alarm.

   See login-rate for information about the ranges for each parameter.

   The **login-interval** and **num-logins** keywords do not have default values.

The login-rate alarm threshold is configured.

This example shows a login-rate threshold configuration that generates an alarm after three login attempts occur within 60 seconds:

```
system
 alarms
  login-rate
   interval 60
   num-logins 3
  !
 !
!
```

Verify a login-rate alarm threshold for Cisco SD-WAN Manager

To verify the login rate alarm configuration, use the **show running-config system alarms** command.

```
vmanage# show running-config system alarms
system
 alarms
  login-rate
    interval 60
      num-logins 3
      !
    !
  !
```

Monitor system login rate alarms

To view alarms configured by the login-rate command, showing when the number of logins to Cisco SD-WAN Manager exceeds a configured threshold, use the **show alarms history** command, and view alarms of type system-login-rate .

```
vmanage# show alarms history

DATE     TIME         TYPE                    SEVERITY    DETAILS
-----------------------------------------------------------------
07/10   16:08:05   system-login-rate      minor    num-logins:3 time-interval:60
```

```
 login-message:3 logins were done in 0 hours 1 minutes 8 seconds
07/10   16:08:05   system-login-change    minor    user-name:admin
user-id:145
```

Configure lockout policy for Cisco SD-WAN Manager using CLI commands

Configure a lockout policy for Cisco SD-WAN Manager using CLI commands to prevent login attempts after failed authentication thresholds are reached.

Configure a lockout policy to prevent new login attempts after reaching a threshold of failed attempts, enhancing security by temporarily blocking access attempts.

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

> **Note**
>
> By default, CLI templates execute commands in global config mode.

Procedure

1. Enter system configuration mode.

   Example

   ```
   system
   ```

2. Enter aaa configuration mode.

   Example

   ```
   aaa
   ```

3. Configure the lockout policy, which prevents new login attempts after reaching a threshold of failed attempts.

   Example

   ```
   lockout-policy lockout-interval lockout-duration fail-interval fail-duration fail-attempts fail-count
   ```

   The **fail-attempts** keyword indicates the number of failed attempts to log in. The **fail-interval** keyword indicates the time span in which to count failed login attempts. The **lockout-interval** keyword specifies how long Cisco SD-WAN Manager waits before allowing new login attempts. See aaa lockout-policy for information about the ranges and defaults for each parameter.

   For example, the following configuration prevents additional login attempts for 600 seconds (10 minutes) when five failed login attempts occur within 60 seconds:

   ```
   system
    aaa
     lockout-policy
      lockout-interval 600
      fail-interval    60
   ```

```
    fail-attempts    5
   !
  !
!
```

What to do next

Verify the lockout policy configuration, using the **show running-config system aaa lockout-policy** command.

Viewing the logs of configuration template activities

Provides steps to view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices.

To view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Select **WAN Edge List** or **Controllers**, and choose a device.
3. For the desired device, click **...** and choose **Template Log**.

Syslog messages

Provides information about system logging messages generated by Cisco Catalyst SD-WAN devices to report events of interest in the overlay network.

When an event of interest occurs on a device in the overlay network, the device generates a system logging (syslog) message and records it in a syslog file under the `/var/log` directory on the local device and, if configured, on a remote host.

On Cisco Catalyst SD-WAN devices, you can log event notification syslog messages to files on the local device, a remote host, or both. On the local device, the system stores syslog files in the `/var/log` directory.

Configure system logging

Cisco Catalyst SD-WAN devices enable logging of syslog messages with a priority level of error to the local device by default. The device stores the log files in the `/var/log` directory.

By default:

- The maximum size of each log file is 10 MB.
- The device stores up to 10 log files.
- When the device reaches the maximum number of files, it deletes the oldest file before creating a new file.

To modify the default syslog settings from Cisco Catalyst SD-WAN, use the Logging feature template.

From the CLI, use the logging disk or logging server commands to configure local or remote syslog logging.

View syslog messages using Cisco SD-WAN Manager

Use these steps to view syslog messages using Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** and ensure that **Data Stream** is enabled.
2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** and select a device.

   For Cisco vManage Release 20.6.x and earlier, choose **Monitor** > **Network** and select a device.
3. In the left pane, select **Troubleshooting**.
4. In the Logs area, click **Debug Log**.
5. In the Log Files field, select the log file that you want to view.

   The lower part of the screen displays the contents of the selected log file.

View syslog messages using CLI commands

To view the contents of a syslog file, use the **show log** command.

For example:

```
Device# show log auth.log tail 10
```

The command displays the most recent entries from the specified log file.

View system logging settings

To view the configured system logging settings for a device, use the **show logging** command.

For example:

```
Device# show logging
System logging to host  in vpn 0 is disabled
Priority for host logging is set to: emerg

System logging to disk is disabled
Priority for disk logging is set to:  err
File name for disk logging is set to:  /var/log/vsyslog
File size for disk logging is set to:  10 MB
File recycle count for disk logging is set to:  10

Syslog facility is set to: all facilities
```

System log files

Cisco Catalyst SD-WAN devices record syslog messages at or above the configured priority level in files in the /var/log directory.

The following log files are available:

Log file	Description
auth.log	Contains login, logout, superuser access, and authorization events.
kern.log	Contains kernel messages.
messages	Contains consolidated syslog messages from all sources.

vconfd	Contains configuration-related syslog messages.
vdebug	Contains debug messages for modules with debugging enabled and syslog messages above the configured priority level. Debug logging supports different levels depending on the module. For example, `sysmgr` supports On and Off, while `chmgr` supports Off, Low, Normal, and High. You cannot send debug messages to a remote host. To enable debugging, use the Debug operational command.
vsyslog	Contains syslog messages generated by Cisco Catalyst SD-WAN processes (daemons) above the configured priority level. The default priority is informational (severity level 6). Therefore, messages with severity levels from emergency (0) through notice (5) are saved by default.

Cisco Catalyst SD-WAN software does not use the following standard Linux log files for logging:

- cron.log
- debug
- lpr.log
- mail.log
- syslog

Syslog message characteristics

The device does not rate-limit writes to syslog files. When the device generates a large number of syslog messages in a short period, it buffers the messages in a queue until it can write them to the syslog file. The device does not drop the overflow messages.

When the device generates identical syslog messages consecutively, it records only one copy of the message and indicates the number of times the message occurred.

The maximum length of a syslog message is 1024 bytes. The device truncates messages that exceed this limit.

AAA and netconf syslog messages

Cisco Catalyst SD-WAN devices record AAA authentication and Netconf CLI access and usage messages in the auth.log and messages files.

When Cisco SD-WAN Manager logs in to a Cisco vEdge device to retrieve statistics and status information or push files to the device, the device generates AAA and Netconf log messages. Over time, these messages can fill the log files.

To prevent these messages from filling the log files, you can disable AAA and Netconf syslog messages:

```
Device(config)# system aaa logs
Viptela(config-logs)# audit-disable
Viptela(config-logs)# netconf-disable
```

Syslog message format

Cisco Catalyst SD-WAN software generates syslog messages in the following format:

```
facility.source
date - source - module - level - MessageID: text-of-syslog-message
```

Syslog message format changes

The syslog format for Viptela daemons changed in Cisco Catalyst SD-WAN Manager Release 20.15.x.

Before Cisco Catalyst SD-WAN Manager Release 20.15.x:

```
%<FACILITY>-<host>-<MNEMONIC>-<SEVERITY>-<SEVERITY-name>-<SEVERITY>-<MessageId>:
<MESSAGE TEXT>
```

Example:

```
Dec 11 09:36:27.358: %Cisco-SDWAN-NR-C8200-1N-4T-FTMD-5-NTCE-1000026:
**HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src: 192.168.104.16/0 Dst: 192.168.104.20/0
Proto: 1 TOS: 0 LogReason: SDWAN_SERV_ICMP_EXCEPT_TS Count: 1 Bytes: 114
```

Starting with Cisco Catalyst SD-WAN Manager Release 20.15.x:

```
%<FACILITY>-<SEVERITY>-<MNEMONIC>: <MESSAGE TEXT>
```

Example:

```
Dec 20 18:47:33.237: %SDWAN-5-FTMD: **HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src:
10.1.17.14/12346 Dst: 192.168.60.100/12346 Proto: 17 TOS: 192 LogReason:
SDWAN_SERV_UDP Count: 1 Bytes: 171 Ingress-Interface: GigabitEthernet2
Egress-Interface: GigabitEthernet2
```

Syslog message acronyms

Acronym	Meaning
confd	CLI configuration process
FTM	Forwarding table manager
FP	Forwarding process
RTM	Route table manager
TTM	Tunnel table manager

For a list of syslog messages generated by Cisco Catalyst SD-WAN software, see Syslog Messages in the Appendix.

Cisco SD-WAN Manager log files

Describes SD-WAN Manager log files, the format, and so on.

Cisco SD-WAN Manager records logs that meet or exceed the default or configured priority level in the /var/log/nms directory on the local device.

Some of these files include:

- vmanage-server.log
- vmanage-appserver.log
- vmanage-server-olap.log
- vmanage-server-device-config.log
- vmanage-server-rest.log

Log format

Logs generated by Cisco Catalyst SD-WAN software use this format:

```
                Date - Log Level - Restful API Tracing ID - Host Name - Class
 - Thread - Tenant ID [Optional]
                 - message
```

Here is an example of a log entry using the local6 facility at the 'INFO' level:.

```
04-Apr-2023 10:22:27,969 CST INFO [af7c0465-1fca-4e6d-8d39-6c03b1357b4b]
[vmanage_scale1] [VmanageSyslogLogger] (default task-3459) |default|
deviceAction: Request for action
```

Manage log size

From Cisco Catalyst SD-WAN Manager Release 20.16.1, you can temporarily increase the log size to 250 MB for troubleshooting purposes.

Use the Cisco Catalyst SD-WAN REST API call provided in the Cisco Developer Documentation.

When you restart Cisco SD-WAN Manager, the log size reverts to 16 MB by default.

Configure Cisco SD-WAN Manager logs

Cisco SD-WAN Manager enables information-level logging to the local device's hard disk by default. Cisco SD-WAN Manager stores the log files in the local `/var/log/nms` directory.

By default, each log file can grow up to 16 MB. Cisco SD-WAN Manager rolls over the log files and stores up to 10 files per day. When it creates the 11th file, it deletes the oldest file to make room for the new log file.

You can configure the following log files:

- vmanage-server
- vmanage-server-statistics
- vmanage-server-olap
- vmanage-server-deviceconfig-template
- vmanage-server-device-config

Viewing logs

Viewing logs using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Managermenu, choose **Tools** > **Operational Commands**

   .
2. To collect logs from all Cisco SD-WAN Managers in the system, click **Generate Admin Tech for Manager** > **Logs**, and then click **Generate**.
3. To collect logs from a specific Cisco SD-WAN Manager, select the **...** under **Actions**, choose **Generate Admin Tech** > **Logs**, and then click **Generate**.
4. Click **Show admin-tech List** to view the download progress. You can access the log file after Cisco SD-WAN Manager generates it.

Viewing logs using CLI commands

To view a Cisco SD-WAN Manager log file use the **show log** command.

```
Device# show log nms/vmanage-server.log
```

> **Note**
>
> All task logs, including activity, administration, and device logs, use the UTC timezone. UTC is the default and only supported timezone for these logs, regardless of the Cisco SD-WAN Manager or local timezone settings.

Viewing the log of certificate activities

Provides information about viewing the status of certificate-related activities using the Cisco SD-WAN Manager Configuration Certificates window.

To view the status of certificate-related activities, use the **Configuration** > **Certificates** window in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager toolbar, select the **Tasks** icon.

   Cisco SD-WAN Manager displays a list of all running tasks, along with the total number of successful and failed tasks.

2. Select a task row to view its details.

   Cisco SD-WAN Manager opens a status window that displays the task status and details about the device on which the task was performed.

Traffic logs

Traffic logs

Traffic logs

Describes a network flow monitoring tool that allows authorized users to access and visualize filtered firewall connection event logs.

Traffic logs is a network flow monitoring tool that

- is integrated into Cisco SD-WAN Analytics
- allows authorized users to access and visualize filtered firewall connection event logs derived from voluminous flow records, and
- enables users to submit queries specifying criteria such as time frame, site name, and devices to get logs on-demand.

From Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager displays Cisco SD-WAN Analytics in a dynamic navbar within the converged user interface.

When you enable Cisco SD-WAN Analytics, the dynamic navbar displays the Traffic Logs tab. Select the tab to open the Cisco SD-WAN Analytics page.

Click any other Cisco SD-WAN Manager menu or tab to return to Cisco SD-WAN Manager.

Benefits of traffic logs

Lists the key advantages and capabilities provided by traffic log functionality.

Traffic logs deliver comprehensive visibility and analysis capabilities for network flow data, enabling efficient processing and filtering of large-scale datasets through cloud-based analytics solutions.

- Provides detailed visibility into raw flow logs, including firewall connection events and related attributes.
- Supports scalable processing and analysis of high-volume flow data.
- Enables users to filter logs of interest to quickly narrow down large datasets, even across millions of records.
- Uses SD-WAN Analytics to provide both the frontend and backend as a cloud-based solution.

Restrictions for traffic logs

Outlines the limitations and constraints that apply when requesting and exporting traffic logs from the fabric.

- Only one request can run at a time across the fabric. All users of the fabric must wait for the request to complete.
- The fabric has rate limits. You can make 24 requests and 24 exports within a 24-hour period. The limits apply across all users of the fabric.
- You can query a maximum of five devices at a time.
- You can filter data for a maximum duration of seven days.
- Log queries can fetch data only from the last month.
- Exports are limited to 1,048,576 rows to ensure compatibility with tools such as Excel.

Generate traffic logs using Cisco SD-WAN Manager

Configure traffic log generation to view network activity and analyze firewall events within a specified time period and network scope.

Generate traffic logs to monitor network activity, analyze security events, and review firewall policy enforcement across your SD-WAN infrastructure.

Procedure

1. Select **Logs**.
2. In the query builder section, specify the mandatory filters:
   - Time period
   - Site(s) (maximum five)
   - Device(s) (maximum five)
   - EVE Process Name
3. Select **Get Logs**.

   If available, the last traffic logs request would be fetched and visualized by default.

   For the firewall attribute columns to be populated, you need to set NGFW policies up in Cisco SD-WAN Manager.

   Table 36: Traffic log fields

Field	Description
EVE Policy Name	Name of the EVE policy associated with the traffic event.

Field	Description
EVE Action	Action reported for the traffic event, such as allow or block.
EVE Reason	Reason reported for the EVE action, such as eve_allow or eve_block.
EVE Process Name	Client process or application identified by EVE.
EVE Process Confidence	Confidence score (0–100%) that EVE identified the process correctly.
EVE Threat Confidence	Probability band (Very High, High, Medium, Low, or Very Low) indicating the threat likelihood of the identified process.
EVE Threat Confidence Level	Confidence score (0–100%) indicating the likelihood that the identified process contains a threat.
Event Time (in UTC)	Displays the exact date and time thta the event was logged, recorded in Coordinated Universal Time (UTC) for standardization.
Site	Displays the physical location, office, or branch where the event was generated.
Hostname	Displays the name given to a device on a network, which can be used to identify it. It can be up to 128 characters long.
System IP	Displays the IP address assigned to the system or device that generated the event log.
VPN ID	Displays an identifier (such as a number or string) representing the specific VPN tunnel or connection involved in the event.
Source IP	Displays the IP address from which the network traffic originated.
Destination IP	Displays the IP address to which the network traffic was sent.
Source Port	Displays the port number used by the source device in the network communication
Destination Port	Displays the port number used by the destination device in the network communication.
Protocol	Displays the communication protocol used for the network session.
Application Name	Displays the name of the application or service associated with the network traffic
Username/SGT	Displays the account name or ID of the user associated with the event, if available.

Field	Description
Firewall Rule	Displays the specific rule within the firewall that matched and processed the event.
FW Policy	Displays the name or identifier of the firewall policy that applies to the traffic or event.
FW Action	Displays the action taken by the firewall for this event.

What to do next

Select **Export** to download the results for offline analysis.

If you wish to troubleshoot traffic logs, contact Cisco TAC for assistance.

Binary Trace for Cisco Catalyst SD-WAN Daemons

Provides information about binary trace support for Cisco Catalyst SD-WAN daemons and their troubleshooting capabilities.

Binary trace collects messages from process modules and records them in binary format. You can configure the binary trace level to control which messages it records, and you can view the recorded messages to trace and troubleshoot process execution errors.

Binary trace improves run-time performance by recording messages in binary format faster than in ASCII format. The binary format also uses storage more efficiently. When you view or save the trace to a file, the system decodes the messages from binary format to ASCII format.

Supported Cisco Catalyst SD-WAN Daemons

Cisco Catalyst SD-WAN Daemons	Supported from release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Note

Starting from Cisco Catalyst SD-WAN Control Components Release 20.15.1, when using the

```
debug vdaemon all
```

command, a warning will be displayed about the potential impact on the network performance.

Configure binary trace level

Configure the binary trace level for one or all modules of a Cisco Catalyst SD-WAN process on a specific hardware slot.

This task enables you to set appropriate trace levels for debugging and monitoring specific Cisco Catalyst SD-WAN processes running on hardware slots.

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

1. Enable privileged EXEC mode.

   Enter your password if prompted.

   ```
   Device> enable
   ```

2. Configure the trace level for one or all modules of a process running on the specified hardware slot.

   set platform software trace *process slot module level*

   Example

   ```
   Device# set platform software trace fpmd R0 config debug
   ```

   - *process*: Specify a Cisco Catalyst SD-WAN process: `fpmd`, `ftm`, `ompd`, `vdaemon`, or `cfgmgr`.
   - *slot*: Specify the hardware slot where the process logs messages.
   - *module*: Configure the trace level for one or all modules of the process.
   - *level*: Select one of the following trace levels:
     a. debug: Logs debug messages.
     b. emergency: Logs emergency messages.
     c. error: Logs error messages.
     d. info: Logs informational messages.
     e. noise: Logs the maximum possible message level.
     f. notice: Logs notice messages.
     g. verbose: Logs verbose debug messages.
     h. warning: Logs warning messages.

View binary trace level

Provides commands to view the binary trace levels for modules of a Cisco Catalyst SD-WAN process executing on a specific hardware slot.

To view the binary trace levels for the modules of a Cisco Catalyst SD-WAN process on a specific hardware slot, use the **show platform software trace level process slot** command.

For example:

```
Device# show platform software trace level fpmd R0
```

where `process` can be `fpmd`, `ftm`, `ompd`, `vdaemon`, or `cfgmgr`, and `slot` specifies the hardware slot.

Viewing messages logged by Binary Trace for a Cisco Catalyst SD-WAN process

Provides commands to view messages logged by Binary Trace for specified processes on Cisco Catalyst SD-WAN devices.

To view messages logged by binary trace for a specific Cisco Catalyst SD-WAN process, use the **show logging process process-name [filtering-options]** command.

For example:

```
Device# show logging process fpmd internal fru R0 reverse
```

where `process-name` specifies the process whose logs you want to view. You can specify a single process or a comma-separated list of processes, such as `fpmd, ftm`.

If you do not specify filtering options, the command displays binary trace level information and higher severity levels collected during the last 10 minutes.

View messages logged by binary trace for all Cisco Catalyst SD-WAN processes

Provides commands to display logs of all Cisco Catalyst SD-WAN processes and their modules in chronological order using binary trace.

To view messages logged by binary trace for all Cisco Catalyst SD-WAN processes and their modules, use the **show logging profile sdwan [filtering-options]** command.

For example:

```
Device# show logging profile sdwan start last boot
```

If you do not specify filtering options, the command displays binary trace level information and higher severity levels collected during the last 10 minutes.

20 Reports

Topics:

- Feature history of reports
- Reports
- Restrictions for reports
- Run a report
- Configure email settings
- View and manage Reports
- Generate CPU, memory, energy report
- Generate energy management report
- Generate upgrade pre-check report

Feature history of reports

Lists the development milestones and release information for Reports, including feature description.

This table describes the developments of this feature, by release.

Table 37: Feature history

Feature name	Release information	Description
Reports	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Reports provide a summarized view of the health and performance of the sites, devices, and tunnels in your network. You can schedule a report, download it as a PDF document, and receive it as an email. The **Reports** menu has been added to Cisco SD-WAN Manager. You can schedule a report, download it as a PDF document, and receive it as an email. The **Reports** menu has been added to Cisco SD-WAN Manager.
Additional report types and formats	Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature introduces several new report types, including Security reports, which are available in CSV or PDF format.
CPU, memory and energy report	Cisco Catalyst SD-WAN Manager Release 26.1.1.1	This feature introduces a new CPU, Memory and Energy Report in addition to the preexisting reports.
Link SLA Change Report	Cisco Catalyst SD-WAN Manager release 26.2.1	The Link SLA Change Report tracks historical SLA metric changes and identifies if events were caused by packet loss, latency, or jitter.
Upgrade pre-check report	Cisco Catalyst SD-WAN Manager release 26.2.1	This feature introduces a new upgrade pre-check report in addition to the preexisting reports.

Reports

Explains the reporting capabilities available in Cisco SD-WAN Manager for monitoring network health and performance.

A report is a document that provides information about the health of sites, devices, and tunnels in Cisco SD-WAN Manager

Report types

These reports are available in Cisco SD-WAN Manager:

- Executive Summary Report
- Link Availability Report
- Site Availability Report
- Link Utilization Report
- Link SLA Report

  From Cisco Catalyst SD-WAN Manager Release 26.2.1 the Link SLA Report is renamed to Link Performance Report.
- Application Usage Report

- IPS Event Collection Report
- Firewall Enforcement Report
- Malware File Collection Report
- Internet Browsing Report
- All Applications Report

  The All Applications Report is available only on a Converged dasboard. For more information about Converged dashboard, see Converged Dashboard for SD-WAN Analytics and SD-WAN Manager.
- CPU, Memory, Energy Report

  (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 26.1.x)
- Upgrade Pre-check Report

  (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 26.2.1)
- Link SLA Change Report

  (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 26.2.1)

  The Link SLA Change report provides historical data on changes to SLA metrics over time. It includes an SLA Change Reason field, which identifies whether an event was triggered by packet loss, latency, or jitter to facilitate precise root cause analysis.

You can generate these reports in PDF or CSV formats. You can generate up to 100 reports in PDF format, while CSV has no limit.

Restrictions for reports

Outlines restrictions for using reports in single-tenant and multitenant deployments.

Reports support both single-tenant and multitenant deployments. In a multitenant environment, users can access reports only through the tenant dashboard.

From Cisco Catalyst SD-WAN Manager Release 20.18.1, NMS service status is changed to an on-demand model.

- The command **request NMS all status** shows **Enabled: false** and **Status: not running** when inactive.

Run a report

Configure a report to generate network data and analytics for specific sites and time ranges.

Generate reports to analyze network performance, monitor site-specific data, and obtain insights for network management decisions.

Before you begin

Ensure you configure email settings in Cisco SD-WAN Manager for scheduling reports. This step is necessary only if you want the report to be emailed.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports** > **Reports**.
2. Click **Report Templates**.

3. Choose a report and click **Generate** on the report.

Field	Description
Report Name	Enter a name for the report.
Sites	Choose the sites for which you want to generate the report.
File Type	Choose a file type in which to render the report.
Time Range	Choose the time range for which you want to generate the report. Default: 7 days
Schedule	Choose one of the schedule options. • **Run Now**: Run the report immediately. • **Run Later (One-Time)**: To run the report once, enter the start date and start time. • **Run Recurring**: To run the report periodically, enter the start date and start time, and choose a frequency from the **Repeats** drop-down list.
Delivery	• **Email Report**: Send the report via email. • **Email**: Enter up to five email addresses.

4. Click **Generate Report**.

Configure email settings

Configure email notification settings to enable alarm notifications through SMTP server configuration.

Configure email settings to enable the system to send alarm notifications through an SMTP server.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Alarm Notifications**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Check the **Email Settings** check box.
4. Choose the security level for sending the email notifications.

   The security level can be **None**, **SSL**, or **TLS**.
5. In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.
6. In the **SMTP Port** field, enter the SMTP port number.

   For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
7. In the **From address** field, enter the full email address to be used as the sender of email notifications.
8. In the **Reply to address** field, enter the full email address to include in the Reply-To field of the email.

This address can be a no-reply address, such as noreply@cisco.com.

9. Check the **Use SMTP Authentication** check box to enable SMTP authentication to the SMTP server.

   If you enable SMTP authentication and do not select an SMTP port (port 25), Cisco SD-WAN Manager internally sets the SSL protocol property when it sends the email notification. This ensures the email is sent securely.

   Enter the username and password for SMTP authentication. The default user email suffix is appended to the username. The password you enter is hidden.

10. Click **Save**.

Email settings are configured and the system can now send alarm notifications through the specified SMTP server.

View and manage Reports

Outlines how to view and manage generated reports

You can manage generated reports by viewing, downloading, editing, rerunning, cancelling, or deleting them.

View generated reports

Use these steps to view all generated reports using filter options and search functionality.

View and filter generated reports to locate specific reports based on schedule, status, time frame, or keywords.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.

   The **My Reports** page displays all the generated reports. Use the filter options (schedule, status, and time frame) in the **Summary** pane or enter a keyword in the search bar to view the reports of your interest.

Download a report

Use these steps to download completed reports.

Download a completed report for local access and analysis.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **...** adjacent to the corresponding report name and choose **Download**.

Edit a report

Configure report parameters to customize how future reports are generated.

Use these steps to edit an existing report to modify its configuration parameters and customize how future reports are generated.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **...** adjacent to the corresponding report name and choose **Edit**.
4. In the **Executive Summary Report** pane, review and edit the configured parameters of the report.
5. Click **Update Report**.

After you edit and update the report configuration, any future report generations reflect the new configuration.

Rerun a report

Configure a report to run again when it is in scheduled, completed, or failed state.

Rerun reports that need to be executed again for updated data or to resolve previous failures.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **...** adjacent to the corresponding report name and choose **Run Now**.

Cancel a scheduled report

Configure the cancellation of a scheduled report that is currently in the scheduled state.

This task allows you to cancel a report that has been scheduled but not yet executed.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **...** adjacent to the corresponding report name and choose **Cancel**.

The scheduled report is cancelled and removed from the scheduled reports list.

Delete a report

Configure report management by deleting scheduled, completed, or failed reports from the system.

Delete reports that are no longer needed to maintain an organized report list and free up system resources.

The delete option is available when a report is in the scheduled, completed, or failed state.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports**.
2. Click **My Reports**.
3. Click **...** adjacent to the corresponding report name and choose **Delete**.

The selected report is removed from the system.

Generate CPU, memory, energy report

Lists the fields and options available when generating CPU, memory, and energy reports.

Use this table to understand the configuration fields and scheduling options when generating CPU, memory, and energy reports.

Field	Description
Report Name	Enter a name for the report.
Sites	Choose the sites for which you want to generate the report.
File Type	Choose a file type in which to render the report.
Time Range	Choose the time range for which you want to generate the report. Default: 7 days
Schedule	Choose one of the schedule options. • **Run Now**: Run the report immediately. • **Run Later (One-Time)**: To run the report once, enter the start date and start time. • **Run Recurring**: To run the report periodically, enter the start date and start time, and choose a frequency from the **Repeats** drop-down list.
Delivery	• **Email Report**: Send the report via email. • **Email**: Enter up to five email addresses.

Generate energy management report

Explains how to generate and access the energy management report.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports** > **Reports**.
2. Click **Report Templates**.
3. In the **Report Templates** page, choose a **Energy management report** card and click **Generate**.

The Energy management report window appears.

4. In the Energy management window, enter the name of the report in the **Report name** field.
5. Choose sites from the **Sites** drop-down list.
6. Choose the **File type**.
   - **CSV**
   - **PDF**
7. Choose the **Time range**.
8. Choose the **Schedule**.
   - **Run now**
   - **Run later (one-time)**
   - **Run recurring**
9. (Optional) Choose the **Delivery method**.

   You can enter up to 5 email addresses in the **Email** field.

A new energy management report is created in the specified format and are available in the **My reports** tab. Reports are also delivered to the email addresses mentioned.

Generate upgrade pre-check report

Provides steps to generate an upgrade pre-check report.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Reports** > **Reports**.
2. Click **Report Templates**.
3. In the **Report Templates** page, choose a **Upgrade Pre-check report** card and click **Generate**.

   The Upgrade Pre-check report window appears.
4. In the Upgrade Pre-check report window, enter the name of the report in the **Report name** field.

   Note

   To ensure the current device versions are compatible with the desired upgrade version for custom selection, ensure to check the compatibility matrix for the desired upgrade version SD-WAN compatibility matrix.
5. In the **Recommended image** pane, to onboard Cisco Services, click **Register now** after reading the End User License Agreement OR select the **Custom** option and choose the image from the **Select and image** drop-down list.
6. (Optional) Click **Add New Image** to add new image.
7. Choose the **File type**.
   - **CSV**
   - **PDF**

8. (Optional) To enable email delivery, configure email settings in the **Settings** page.

21 Configuration consistency across Cisco Catalyst SD-WAN Controllers

Topics:

- Feature history of configuration consistency across Cisco Catalyst SD-WAN Controllers
- Configuration consistency across Cisco Catalyst SD-WAN Controllers
- Multi-stage approach for configuration consistency across Cisco Catalyst SD-WAN Controllers
- Prerequisites for configuration consistency across Cisco Catalyst SD-WAN Controllers
- Restrictions for configuration consistency across Cisco Catalyst SD-WAN Controllers
- Warning messages for offline Cisco SD-WAN Controllers
- Verify consistent configuration across Cisco Catalyst SD-WAN Controllers

Feature history of configuration consistency across Cisco Catalyst SD-WAN Controllers

Development of the configuration consistency feature, by release.

Development of the configuration consistency feature, by release.

Feature name	Release information	Description
Configuration Consistency across Cisco SD-WAN Controllers	Cisco Catalyst SD-WAN Control Components Release 20.18.1	This process maintains configuration consistency across Cisco SD-WAN Controllers through three stages: • Validate: Cisco SD-WAN Manager validates the configuration. • Apply: Cisco SD-WAN Manager applies the configuration. • Rollback (optional): Cisco SD-WAN Manager reverts the changes if the application fails. This approach prevents configuration inconsistencies across Controllers.

Configuration consistency across Cisco Catalyst SD-WAN Controllers

Explains how configuration consistency is maintained across Cisco SD-WAN Controllers in both single-tenant and multitenant deployments.

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

Configuration consistency across Cisco SD-WAN Controllers is a mechanism that:

- maintains consistent configurations across all Cisco SD-WAN Controllers in a single-tenant cluster.
- maintains consistent configurations across the Cisco SD-WAN Controllers that belong to a tenant in a multitenant deployment.
- uses a multi-stage approach to validate and apply configuration changes.
- rolls back changes when failures occur to prevent configuration inconsistencies.

This process applies to Cisco SD-WAN Controllers in both single-tenant and multitenant deployments.

Multi-stage approach for configuration consistency across Cisco Catalyst SD-WAN Controllers

Describes how Cisco SD-WAN Manager validates and applies configuration changes across Controllers and rolls back changes when application fails.

This approach ensures uniformity in configuration across Cisco SD-WAN Controllers in a network.

Summary

The multi-stage approach consists of two primary stages: validation and application. If the application fails, Cisco SD-WAN Manager optionally rolls back the configuration changes to prevent partial configuration.

Workflow

The multi-stage approach includes these stages:

The multi-stage approach involves these stages:

1. Stage 1: Validate Configuration - Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to perform various validation checks on the configuration.
   - Resource validation
   - Syntax validation
   - Semantic validation

   During this stage, Cisco SD-WAN Controllers send periodic interim ACKs back to Cisco SD-WAN Manager to keep communication active and display ongoing status through task logs.
2. Stage 2: Apply Configuration - Upon successful completion of Stage 1, Cisco SD-WAN Manager instructs all Cisco SD-WAN Controllers to apply the configuration.

   The Cisco SD-WAN Controllers perform another resource validation check before committing the configuration. The rolling timeout period of 25 minutes starts after Cisco SD-WAN Manager receives the last successful interim ACK from any Cisco SD-WAN Controller.
3. Stage 3: Rollback Configuration (Optional) - Cisco SD-WAN Manager initiates this stage only when Stage 2 fails.

   This stage involves rolling back configuration changes on all Cisco SD-WAN Controllers if one or more controllers are unable to accept or apply the configuration. Cisco SD-WAN Manager rolls back the configuration changes on all devices to which they were successfully deployed .

   If a timeout occurs, Cisco SD-WAN Manager terminates applying configuration changes to all the Cisco SD-WAN Controllers in the network and initiates a rollback.

   Rollback prevents partial implementation of configurations and ensures uniformity in configuration across Cisco SD-WAN Controllers in a network.

Prerequisites for configuration consistency across Cisco Catalyst SD-WAN Controllers

Outlines the minimum supported version and device requirements for configuration consistency process across Cisco Catalyst SD-WAN Controllers.

Ensure that all devices operate on Cisco SD-WAN Controller version 20.17.1 and Cisco Catalyst SD-WAN Manager Release 20.18.1 to support the configuration consistency process.

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

Restrictions for configuration consistency across Cisco Catalyst SD-WAN Controllers

Outlines restrictions for maintaining configuration consistency across Cisco SD-WAN Controllers with minimum supported version requirements and multi-stage deployment considerations.

These are the restrictions for maintaining configuration consistency across Cisco SD-WAN Controllers:

- Cisco Catalyst SD-WAN Manager Release 20.18.1 supports the multi-stage approach for maintaining configuration consistency only for Cisco SD-WAN Controller version 20.18.1 and later. Cisco Catalyst SD-WAN Manager Release 20.18.1 does not support the multi-stage approach for Cisco SD-WAN Controller 20.16.1 and below. For Cisco

SD-WAN Controller versions prior to 20.16.1, Cisco SD-WAN Manager implements configuration changes through the older one-step configuration deployment method.

- The Cisco SD-WAN Controllers older than version 20.18.1 do not support the multi-stage approach. During the validation before configuration deployment, if Cisco SD-WAN Manager detects an older version alongside Cisco SD-WAN Controllers running version 20.18.1 and later, it stops the configuration deployment.
- Although the process is designed to maintain configuration consistency across Cisco SD-WAN Controllers, this process may occasionally be unsuccessful. If Cisco SD-WAN Manager fails to apply configuration changes and configuration rollback does not restore consistency, you may have to manually fix the validation issues.

Warning messages for offline Cisco SD-WAN Controllers

Lists warning messages that appear during validation when Cisco SD-WAN Manager detects offline Cisco SD-WAN Controllers during configuration deployment.

When deploying a configuration on Cisco SD-WAN Controllers, Cisco SD-WAN Manager displays a warning message during validation if it detects one or more offline Cisco SD-WAN Controllers.

This message includes details of the validation issues. It appears during the validation stage in these procedures:

- When you activate a centralized policy.
- When you deploy a topology group to the Cisco SD-WAN Control Components.
- After you push the configuration to the devices.
- When you save an application-aware policy in the Cisco SD-WAN Controllers.

Verify consistent configuration across Cisco Catalyst SD-WAN Controllers

Provides commands to verify configuration consistency across Cisco Catalyst SD-WAN Controller controllers.

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

Use these commands to verify the configuration consistency across Cisco Catalyst SD-WAN Controller.

View Configuration Transaction Status

Use the **show config-pull transactions detail** command to view the details and current status of a configuration transaction.

Example:

```
Device# show config-pull transactions detail
config-pull transactions 1
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497

 tenant     default
 start-time 2025-01-26T03:49:15
 activity 2025-01-26T03:49:20.124
  type    validate-in-progress
  message "Time elapsed: 5 secs"
 activity 2025-01-26T03:49:24.302
  type    validate-in-progress
  message "Time elapsed: 9 secs"
 activity 2025-01-26T03:49:32.461
  type    validate-in-progress
  message "Time elapsed: 17 secs"
```

```
 activity 2025-01-26T03:49:36.626
  type    validate-success
  message "Config validation success"
 activity 2025-01-26T03:49:41.752
  type    apply-in-progress
  message "Time elapsed: 4 secs"
 activity 2025-01-26T03:49:45.917
  type    apply-in-progress
  message "Time elapsed: 8 secs"
 activity 2025-01-26T03:49:54.094
  type    apply-in-progress
  message "Time elapsed: 17 secs"
 activity 2025-01-26T03:50:10.332
  type    apply-in-progress
  message "Time elapsed: 33 secs"
 activity 2025-01-26T03:50:18.521
  type    apply-success
  message "OMP readiness check progress 100%"
```

The output displays transaction details, including the transaction ID, tenant, activity timestamps, and validation and application status.

View Configuration Transaction History

Use the **show config-pull history detail** command to view the history of configuration validation and application.

Example:

```
Device# show config-pull history detail
config-pull history 1
 start-time 2025-01-26T03:49:15
 tenant     default
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497

 stage      validate
 duration   21
 result     success
config-pull history 2
 start-time 2025-01-26T03:49:37
 tenant     default
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497

 stage      apply
 duration   41
 result     success
```

The output displays the validation and application stages, their duration, and the result of each stage.

22 Packet Capture

Topics:

- Feature history of packet capture
- Bidirectional packet capture
- Configuring packet capture

Feature history of packet capture

Lists the development milestones and release information for packet capture, including feature description.

This table describes the developments of this feature, by release.

Table 38: Feature history

Feature name	Release information	Description
Embedded packet capture	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This feature provides an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from a device.
	Cisco vManage Release 20.3.1	Administrators can analyze the captured packets locally or save and export them for offline analysis Cisco SD-WAN Manager. The captured packet information supports application analysis, security, and troubleshooting.
Embedded packet capture for Cisco vEdge Devices using CLI commands	Cisco SD-WAN Release 20.6.1	This feature provides an alternative method for capturing traffic data to troubleshoot connectivity issues between Cisco vEdge devices and Cisco SD-WAN Manager using CLI commands. Use these commands to capture and view traffic details: • `request stream capture` • `show packet-capture`
Bidirectional packet capture for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This feature enhances the embedded packet capture functionality to support bidirectional packet capture through Cisco SD-WAN Manager.
	Cisco vManage Release 20.7.1	You can now enable the **Bidirectional** option using Cisco SD-WAN Manager to capture bidirectional packets.
IPv6 support for bidirectional packet capture	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This feature allows you to capture IPv6 traffic bidirectionally to troubleshoot connectivity issues using a CLI template.

Bidirectional packet capture

Describes a network troubleshooting feature that captures traffic flowing through interfaces or control plane in single or both directions for analysis.

Bidirectional packet capture is a network troubleshooting feature that

- captures traffic flowing through an interface or control plane in a single direction or both directions
- enables analysis of packets locally or export of captured traffic for offline analysis, and

From Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, packet capture supports IPv6 traffic.

Configuring packet capture

Procedures, using different methods, for configuring packet capture.

Use one of these methods to configure packet capture.

- Configure packet capture using Cisco SD-WAN Manager
- Configure packet capture using CLI commands

Configure packet capture using Cisco SD-WAN Manager

Configure packet capture to capture control plane and data plane packets in real time and save these packets to a file available on edge devices.

In a Cisco SD-WAN Manager cluster, you can run a speed test and capture packets on any device in the cluster, regardless of which Cisco SD-WAN Manager node the device is connected to. Configure the data stream using one of the following options:

- Management IP address and VPN 512. (The Cisco CSR 1000v Series platform does not support a management IP address.)
- Transport IP address and VPN 0.

In a cluster environment, we recommend that you do not configure the data stream with the system IP address of a Cisco SD-WAN Manager node and VPN 0. This configuration limits speed tests and packet captures to the devices connected to the Cisco SD-WAN Manager node specified in the data stream.

Packet capture is not supported for a loopback interface.

Use these steps to configure packet capture using Cisco SD-WAN Manager:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. To choose a device, click the device name in the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Traffic** area, click **Packet Capture**.
5. From the VPN drop-down list, choose a VPN.
6. From the **Interface** drop-down list, choose an interface.

   Note

   From Cisco vManage Release 20.8.1, you can capture IPv6 packets for tracing and troubleshooting traffic. To do this, choose an IPv6 interface from the **Interface** drop-down list. (Prior to Cisco vManage Release 20.8.1, only IPv4 interface capture was supported.)
7. (Optional) Click **Traffic Filter** to filter the packets to capture based on values in their IP headers.

   Enter values for the following fields:

a. In the **Source IP** field, enter the source IP address of the packet.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

b. In the **Source Port** field, enter the source port number of the packet.

c. In the **Protocol** field, enter the protocol ID of the packet.

d. In the **Destination IP** field, enter the destination IP address of the packet.

   For releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 address. From Cisco Catalyst SD-WAN Manager Release 20.13.1, enter an IPv4 or IPv6 address.

e. In the **Destination Port** field, enter the destination port number of the packet.

8. For a Cisco IOS XE Catalyst SD-WAN device, to enable bidirectional packet capture, set the **Bidirectional** toggle button to **On**.

   Note

   The bidirectional packet capture functionality is available from Cisco vManage Release 20.7.1.

9. Click **Start**.

   The packet capture begins, and progress is displayed:

   a. Packet Capture in Progress: Packet capture stops after the file of collected packets reaches 5 MB, or when you click **Stop**.

   b. Preparing file to download: Cisco SD-WAN Manager creates a file in libpcap format (a .pcap file).

   c. File ready, click to download the file: Click the download icon to download the generated file.

Configure packet capture using CLI commands

Configure packet capture for IPv4 and IPv6 traffic using CLI commands to monitor network traffic through interfaces or control planes.

This task enables you to set up packet capture monitoring for both IPv4 and IPv6 traffic to analyze network communications and troubleshoot connectivity issues.

For more information about using CLI templates, see CLI Templates.

By default, CLI templates execute commands in global config mode.

Before you begin

Perform these steps and ensure that **Data Stream** is **Enabled** under **Administration** settings for the monitor packet capture CLI configurations to take effect.

1. From Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Data Stream**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.

3. Choose the **IP Address Type**. By default, **System** is selected. (**Transport** and **Management** types require additional **Hostname** and **VPN** settings.)
4. Click **Save**.

Procedure

1. Define a core filter for monitoring IPv4 packet capture.

```
monitor capture capture-name match ipv4 source-prefix/length
destination-prefix/length [bidirectional]
```

Example

Here is an example configuration to filter and capture IPv4 traffic:

```
monitor capture mycap match ipv4 198.51.100.0/24 host 198.51.100.1
```

Example

2. Configure a filter to monitor inbound, outbound, or bidirectional IPv6 traffic passing through an interface or the control plane.
   - Configure packet capture for an interface:

```
monitor capture capture_name  [interface interface-name interface-num {both | in
| out}] match ipv6 {{ipv6-source-prefix/length| host ipv6-src-addr| any}
{ipv6-destination-prefix/length| host ipv6-dest-addr| any}}
|protocol {<0-255>|tcp|udp}
{ipv6-source-prefix/length| host ipv6-src-addr| any} [{eq | lt| gt| neq |range
 port_number} port_number]
{ipv6-destination-prefix/length| host ipv6-dest-addr| any} [{eq | lt| gt| neq
 |range port_number} port_number]} [bidirectional]
```

   - Configure packet capture for the control plane:

```
monitor capture capture_name [control-plane {both | in | out}] match ipv6
{{ipv6-source-prefix/length| host ipv6-src-addr| any}
{ipv6-destination-prefix/length| host ipv6-dest-addr| any}}
|protocol {<0-255>|tcp|udp}
{ipv6-source-prefix/length| host ipv6-src-addr| any} [{eq | lt| gt| neq |range
 port_number} port_number]
{ipv6-destination-prefix/length| host ipv6-dest-addr| any} [{eq | lt| gt| neq
 |range port_number} port_number]} [bidirectional]
```

Examples showing how to configure to filter and capture IPv6 traffic:

```
monitor capture test interface GigabitEthernet 5 both match ipv6 protocol tcp
 host 2001:3c0:1::71 host 2001:380:1::71 bidirectional
monitor capture cap interface gig 2 in match ipv6 50::1/128 50::2/128
bidirectional
monitor capture cap interface gig 2 out match ipv6 50::1/128 50::2/128
bidirectional
monitor capture cap interface gig 2 both match ipv6 50::1/128 50::2/128
bidirectional
monitor capture cap control-plane in match ipv6 50::1/128 50::2/128
```

```
bidirectional
monitor capture cap control-plane out match ipv6 50::1/128 50::2/128
bidirectional
monitor capture cap control-plane both match ipv6 50::1/128 50::2/128
bidirectional
```