

Cisco SD-WAN Manager Monitor Overview

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.
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.

Feature Name	Release Information	Description
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.
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.

Feature Name	Release Information	Description
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.
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.

Feature Name	Release Information	Description
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.

The following dashlets are available by default on the **Monitor** > **Overview** dashboard in Cisco SD-WAN Manager. (In Cisco vManage Release 20.6.1 and earlier releases, these dashlets are part of **Dashboard** > **Main Dashboard**.)

- **Site Health**
- **Tunnel Health**
- **WAN Edge Health**
- **Application Health**
- **Top Applications**
- **WAN Edge Management**

- Information About Customizing the Monitor Overview Dashboard, on page 5
- Restrictions for Customizing the Monitor Overview Dashboard, on page 6
- Customize the Monitor Overview Dashboard, on page 6
- Filter the Dashboard Data, on page 8
- Monitor Cellular Devices, on page 9
- View Controller and Device Information, on page 11
- View Cisco SD-WAN Manager Status, on page 11
- View EoX Status, on page 12
- View Certificate Status Pane, on page 13
- View Licensing Pane, on page 13
- View Reboot Pane, on page 14

• View Control Status Pane, on page 14
• View BFD Connectivity Pane, on page 15
• View Transport Interface Distribution Pane, on page 16
• View WAN Edge Inventory Pane, on page 17
• View WAN Edge Health Pane, on page 18
• View Transport Health Pane, on page 19
• View Top Applications Pane, on page 20
• View Application-Aware Routing Pane, on page 22
• View Web Server Certificate Expiration Date Notification, on page 22
• View Maintenance Windows Alert Notification, on page 23
• View Application Health Dashlet, on page 23
• View Tunnel Health Dashlet, on page 24
• View Top Alarms Dashlet, on page 24
• View temperature and energy usage dashlet, on page 25
• View underlay alarms dashlet, on page 26
• View data plane drops dashlet, on page 26
• View WAN Edge Health Dashlet, on page 27
• View WAN Edge Management Dashlet, on page 28
• View Site Health Dashlet, on page 28
• Security, on page 32
• Multicloud, on page 41
• Explore, on page 44
• Energy management, on page 45
• Advisories, on page 46
• Converged Dashboard for SD-WAN Analytics and SD-WAN Manager, on page 48

Information About Customizing the Monitor Overview Dashboard

Minimum release: Cisco vManage Release 20.9.1

By default, the **Monitor Overview** dashboard displays all the available dashlets that help you monitor the different components and services of a Cisco Catalyst SD-WAN overlay network. The customizable dashboard feature enables you to do the following:

- Add dashlets
- Delete dashlets
- Rearrange dashlets
- Restore default settings

The customized dashboard settings are saved in a database. These settings are retrieved in the following 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.

Note We recommend that you use Google Chrome browser to access Cisco SD-WAN Manager. However, Firefox browser is also supported.

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

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

Benefits of Customizing the Monitor Overview Dashboard

- 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

Minimum release: Cisco vManage Release 20.9.1

- 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

Minimum release: Cisco vManage Release 20.9.1

Add a Dashlet

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**.

Note 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**.

You can customize the following dashlets:

- **Transport Health**
- **Site BFD Connectivity**
- **Transport Interface Distribution**
- **WAN Edge Inventory**
- **Application-Aware Routing**
- **Remote Access Sessions**
- **Remote Access Headends**

Note The remote access sessions and remote access headends dashlets are available from Cisco Catalyst SD-WAN Manager Release 20.14.1 and later releases.

Delete a Dashlet

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

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**.

Restore Default Settings

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 the Dashboard Data

Minimum release: Cisco vManage Release 20.10.1

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 the following 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.

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

To filter the data, do the following:

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.

   The dashlets display the data based on the chosen time.

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.

Monitor Cellular Devices

View Cellular Device Count

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

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. Active devices are those with the cellular link in use, while standby devices are those with the cellular link not in use. The data on the dashlet changes based on the selected filter.

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.

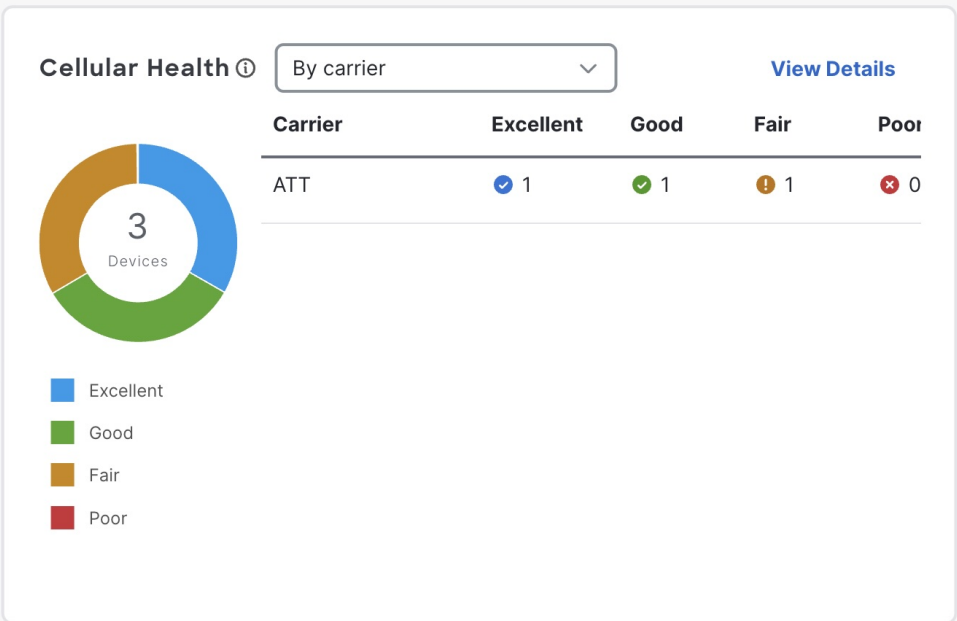
View Cellular Health Dashlet

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

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 Controller and Device Information



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

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 has the following behavior:

- 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 Cisco SD-WAN Manager Status

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.

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, the following 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**.

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

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.

View EoX Status

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.

Procedure

Step 1 From Cisco SD-WAN Manager, click **Monitor** > **Devices**.

Step 2 Under **EoX Status**, you can view end-of-life and end-of-support announcements for Cisco products.

View Certificate Status Pane

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.



Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following 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 Licensing Pane

The **Licensing** pane displays the total number of devices configured and the number of devices licensed. Click the **Licensing** pane to open the **Monitor** > **Devices** > **Licensing** page, which displays the following information of a device:

- 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

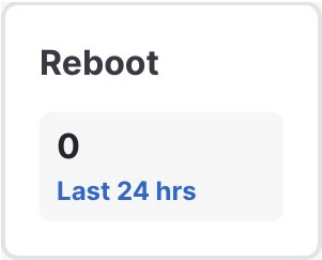


Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- 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 Reboot Pane



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. Whewn 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.

Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following 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 Control Status Pane

The **Control Status** pane is available only in Cisco vManage Release 20.7.1 and earlier releases.

The **Control Status** pane displays whether Cisco SD-WAN Controller and WAN Edge devices are connected to the required number of Cisco SD-WAN Controllers. Each Cisco SD-WAN Controller must connect to all other Cisco SD-WAN Controllers in the network. Each WAN Edge router must connect to the configured maximum number of Cisco SD-WAN Controllers.

The **Control Status** pane shows three counts:

- **Up**: Total number of devices with the required number of operational control plane connections to a Cisco SD-WAN Controller.
- **Partial**: Total number of devices with some, but not all, operational control plane connections to Cisco SD-WAN Controllers.
- **Down**: Total number of devices with no control plane connection to a Cisco SD-WAN Controller.

Note The **Control Status** pane depends upon both Cisco SD-WAN Manager control connection and Cisco SD-WAN Controller control connection states.

Click the UP/Down/Partial data, and the **Monitor** > **Devices** page appears. For the desired device, click **...** to access Device Dashboard or Real Time view or to access the **Tools** > **SSH Terminal**.

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

- The **Control Status** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Up**, **Partial**, and **Down** statuses are titled **Control Up**, **Partial**, and **Control Down**, respectively.
- A status bar instead of a doughnut chart displays the data.
- A pop-up window opens instead of the **Monitor** > **Devices** page when you click the data.

View BFD Connectivity Pane

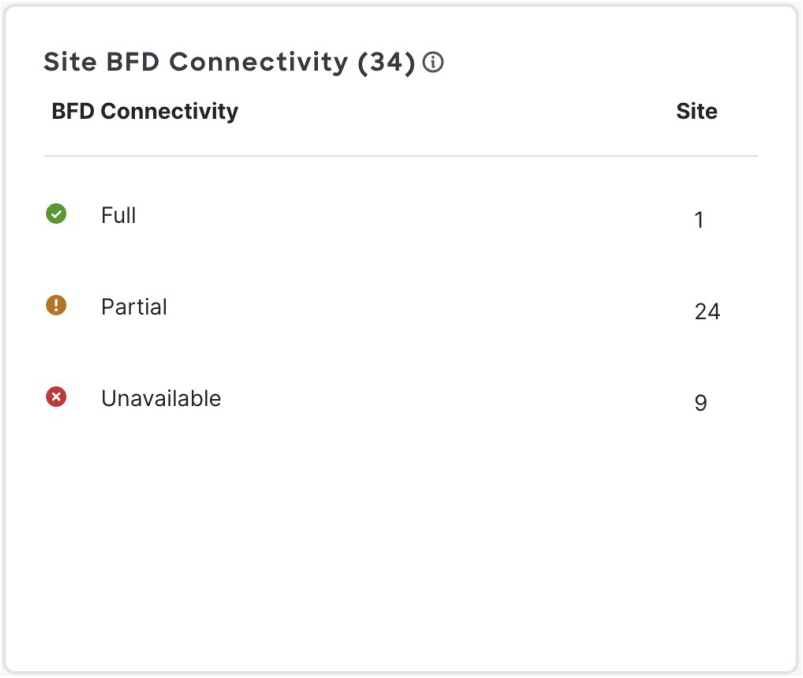
A site is a specific physical location within the Cisco Catalyst SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each device at a site is identified by the same site ID.

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**.



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

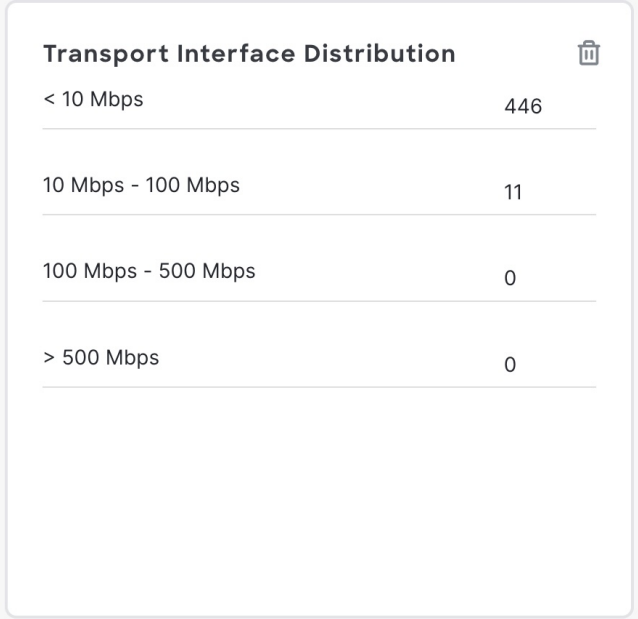
- The **Site BFD Connectivity** pane is titled **Site Health**. The **Site Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Full**, **Partial**, and **Unavailable** statuses are titled **Full WAN Connectivity**, **Partial WAN Connectivity**, and **No WAN Connectivity**, respectively.
- A pop-up window opens instead of a sidebar when you click the data.
- The Device Dashboard or Real Time view is part of the **Monitor** > **Network** page.

View Transport Interface Distribution Pane

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces.

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.

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

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

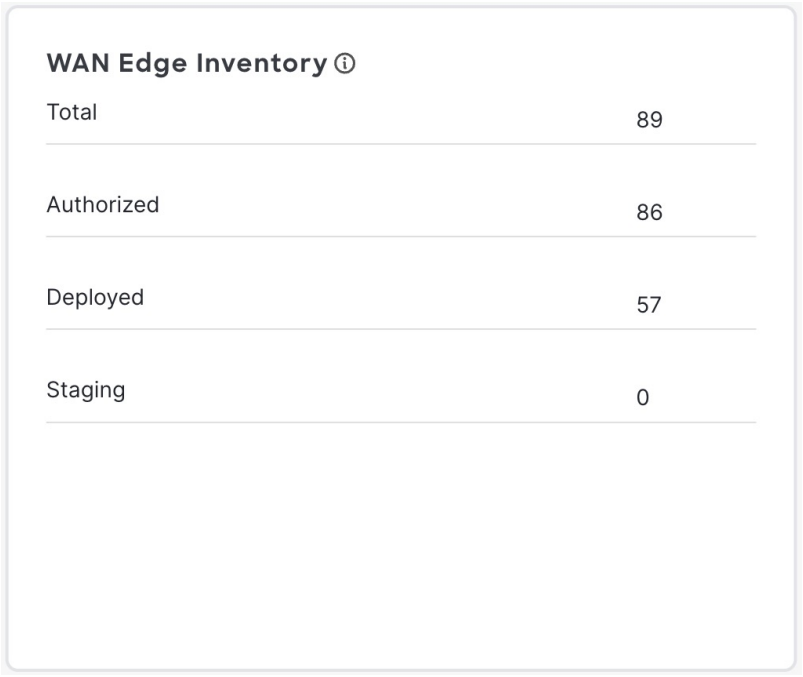
View WAN Edge Inventory Pane

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.



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

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

View WAN Edge Health Pane

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.

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.

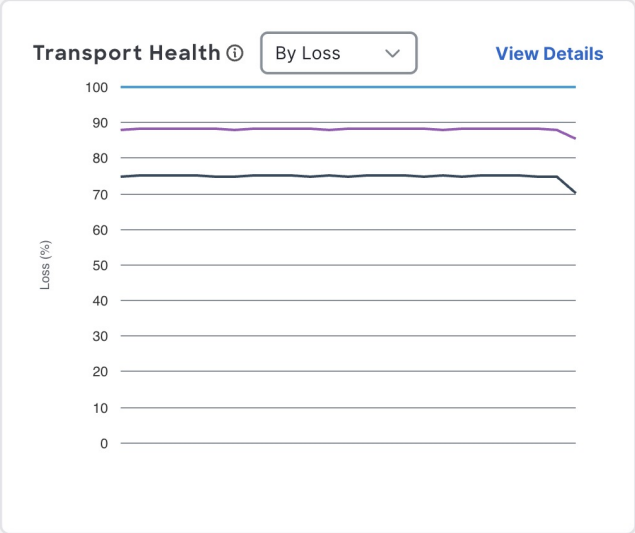
Note In Cisco vManage Release 20.6.1 and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **WAN Edge Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- The **Good**, **Fair**, and **Poor** statuses are titled **Normal**, **Warning**, and **Error**, respectively.
- A pop-up window opens instead of a sidebar when you click the data.
- The Device Dashboard or Device Details view is part of the **Monitor** > **Network** page.

View 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).

- From the **Type** drop-down list, select loss, latency, or jitter.
- Click the **Time** drop-down list to select a time period for which to display data.
- Click **View Details**, and the sidebar displays the information in tabular format. You can change the displayed type and time period as described above.



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

- The **Transport Health** pane is part of the **Dashboard** > **Main Dashboard** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Transport Health** pop-up window.

View Top Applications Pane

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 In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

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.

To list top applications in a sidebar:

1. Click **View Details** to open the **Top Applications** sidebar. It displays a more detailed view of the same information.
2. 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.

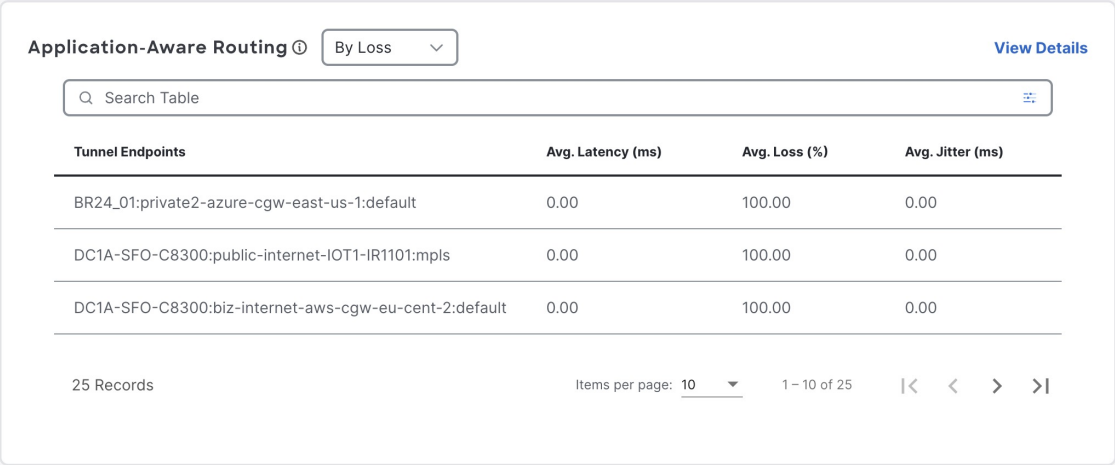
3. Click **SSL Proxy**, from the **View by Policy Actions** drop-down list, select the policy action. All Policy Action, Encrypted, Un-Encrypted, Decrypted view are supported. From the **VPN** drop-down list, select the desired VPN, and then click **Search**. The **Hour** option displays statistics for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

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

- The **Top Applications** pane is part of the **Dashboard** > **Main Dashboard** page.
- A filter icon instead of a drop-down list lists the VPN options and indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Top Applications** pop-up window.

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.

View 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.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down for specifying a custom time period.

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.

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

- The **Application-Aware Routing** pane is part of the **Dashboard** > **Main Dashboard** page.
- An expand icon instead of the **View Details** button opens the **Application-Aware Routing** pop-up window.

View Web Server Certificate Expiration Date Notification

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.

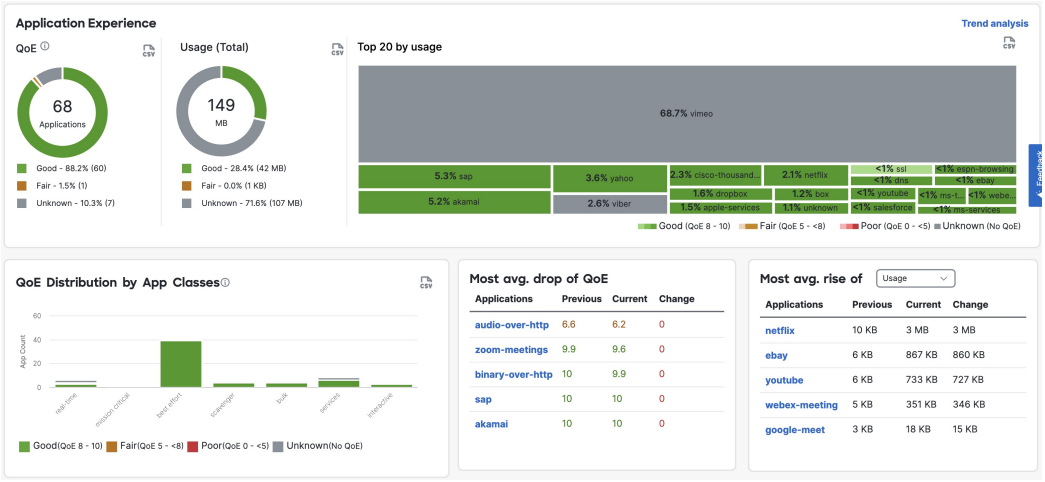
Note In Cisco vManage Release 20.6.1 and earlier releases, the **Dashboard** > **Main Dashboard** page displays the certificate expiry notification.

View Maintenance Windows Alert Notification

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.

Note In Cisco vManage Release 20.6.1 and earlier releases, the **Dashboard** > **Main Dashboard** page displays the maintenance window alert notification.

View Application Health Dashlet



Minimum supported release: Cisco vManage Release 20.10.1

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**.

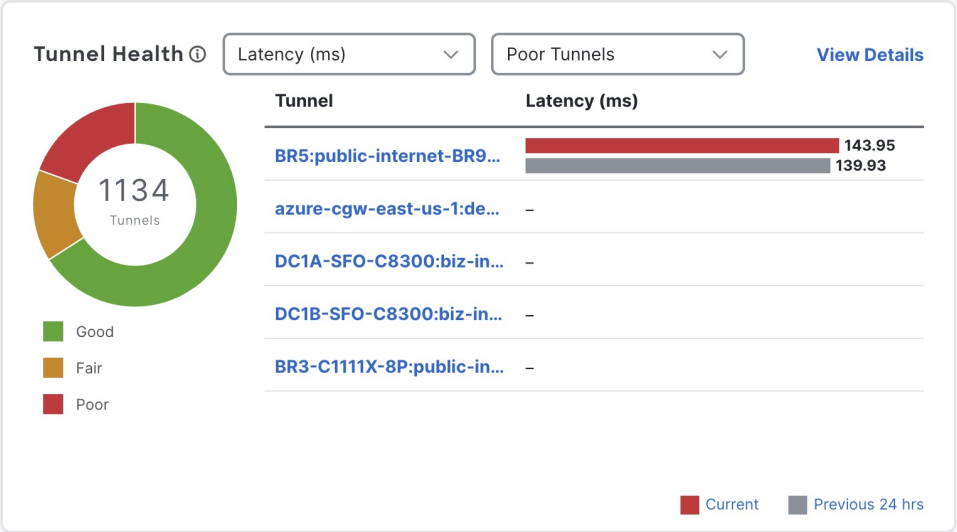
Click **View Details** to open the **Monitor > Applications** window.

View Tunnel Health Dashlet

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 the following 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

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.

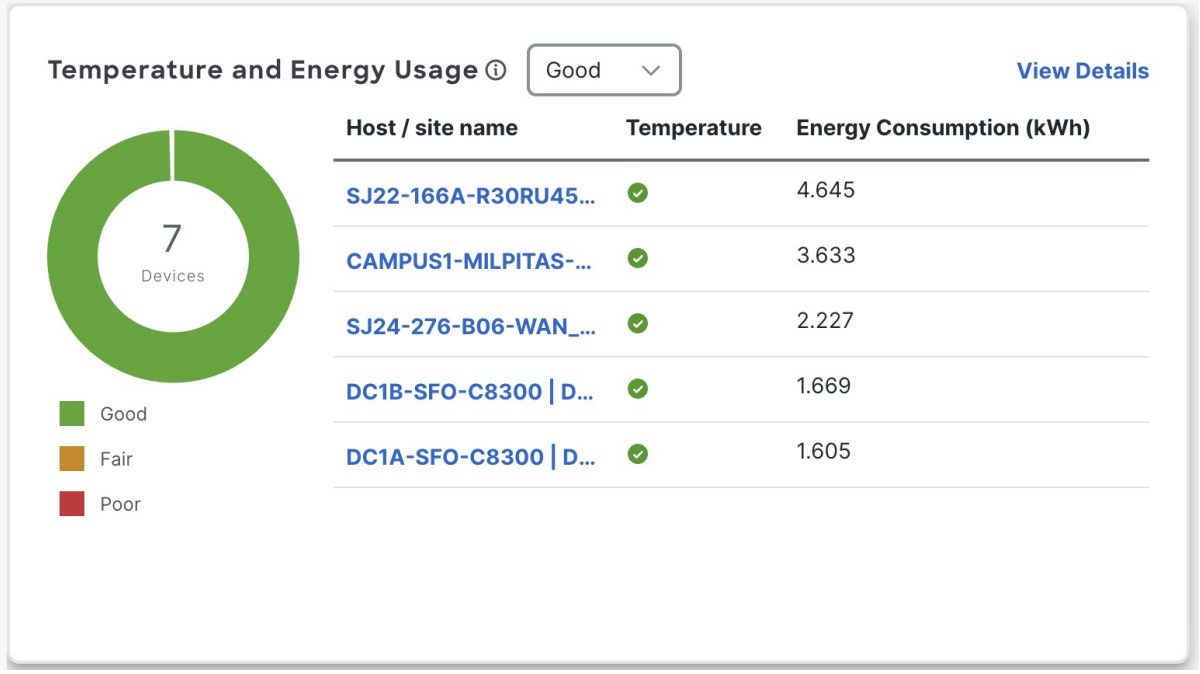
View temperature and energy usage dashlet

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.

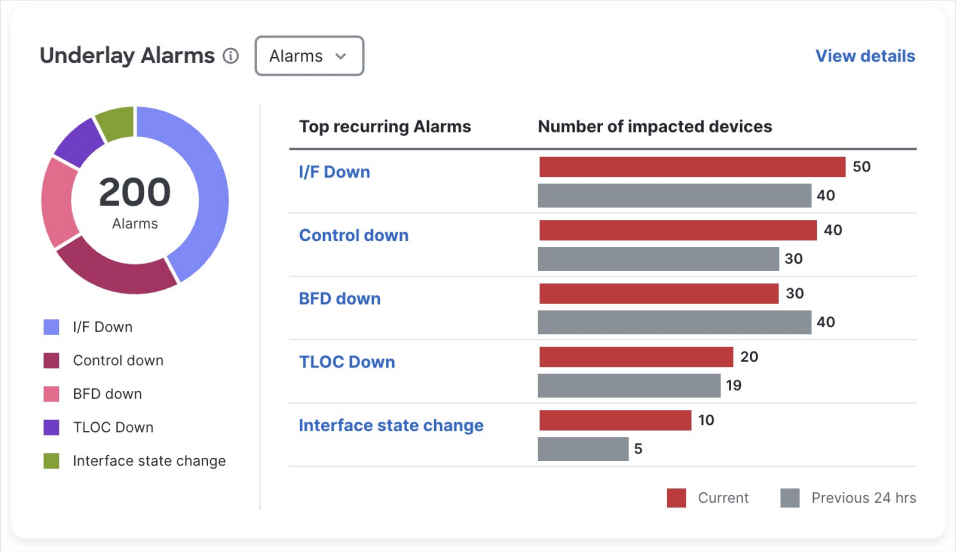


The health status is categorized as Good, Fair, or Poor based on predefined temperature thresholds:

- 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



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.

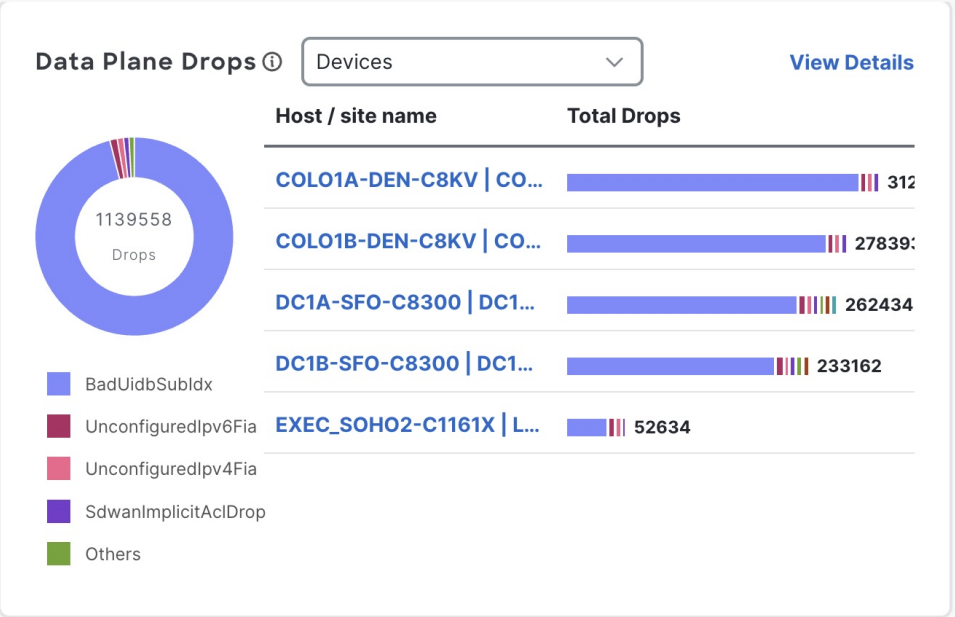
View data plane drops dashlet

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



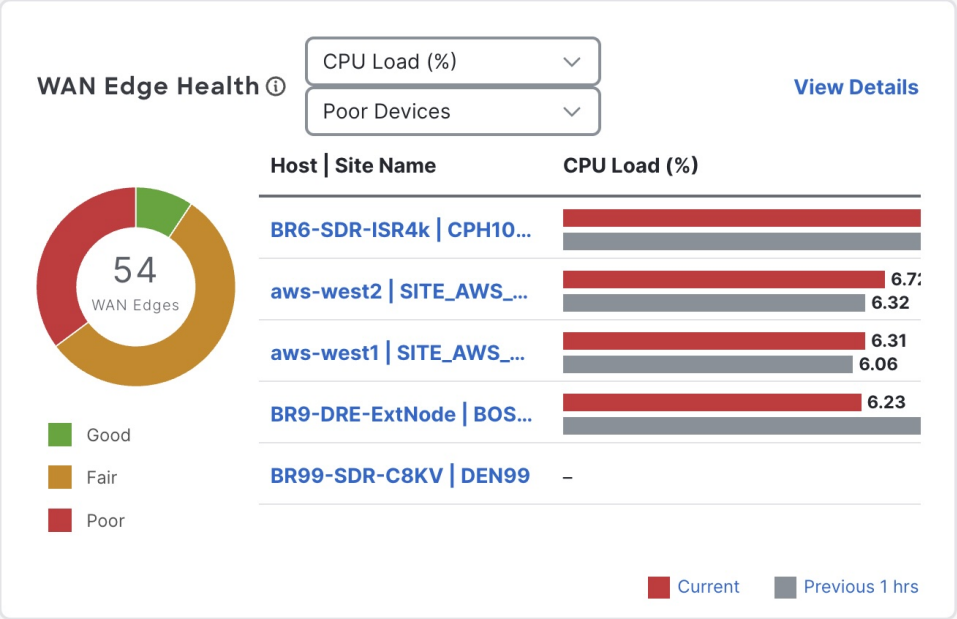
The dashlet displays historical data from device statistics. Only non-zero drop statistics are displayed. Click **View Details** to access more detailed data plane drop information.

View WAN Edge Health Dashlet

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

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**.

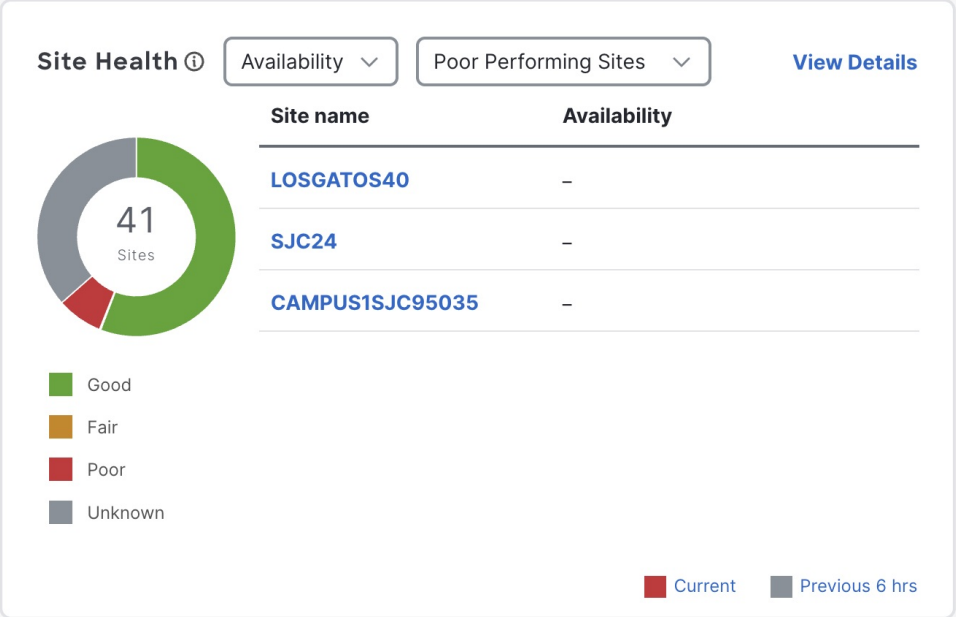
Click **View Details** to open the **Monitor > Devices** window to view the configured device details in table view.

View Site Health Dashlet

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.

Figure 6: Site Health Dashlet



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.

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

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 as follows:

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.

Health	Condition
Poor	Any one application, WAN edge device, or tunnel in poor state.

View Site Health in Heatmap View

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

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 renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

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

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

You can view all the WAN edge devices and sites for geographical regions worldwide. When you click an individual site, you can view the site details such as **Hostname**, **Site ID**, **Device Model**, **System IP**, **Health**, **Reachability**, and so on, in the side pane. When you click on the troubleshooting options available in the side pane, Cisco Catalyst SD-WAN Manager displays the relevant troubleshooting pages. Aggregated sites show the number of sites. The color of the aggregated site shows the site health.

To view the site topology of a specific site, click **Site Topology**. To view a specific site dashboard, click **Site Dashboard**. When you click **View Tunnels** available in the side pane, you can see the tunnels associated to a specific site. Click the tunnel line to view detailed tunnel information. Click the back button to go back from the tunnel view to the Global Network view.

You can filter the global topology view based on the health status of the sites using the **Good**, **Fair**, and **Poor** filter options.

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.

Time Interval, Search, and Network Hierarchy

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

Select the time from the drop-down list to select 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.

You can use the search option to filter the sites based on the configuration groups, policy groups, tags and so on, using the **Contains** and **Match** options.

You can filter the global topology view based on the health status of the sites and tunnels using the **Good**, **Fair**, and **Poor** filter options.

When you click the summary icon, the topology view of the site and tunnel health across geographical locations is displayed. You can view the site and tunnel health details by clicking the non-zero number in the topology view. If you click the eye icon, you can view the tunnel connection with aggregated tunnel health between the sites.

Click the arrow on the left to open the network hierarchy menu. Click an individual site from this menu, to view the following site details in the side pane:

- You can view the following 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.

- Network Wide Path Insight:

  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. Click **Create a trace** to start a new trace. 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**.

- Troubleshooting:

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

- Detailed Information:
  - To view the site topology of a specific site, click **Site Topology**.
  - To view a specific site dashboard, click **Site Dashboard**.
  - To view the tunnels associated to a specific site, click **View Tunnels**. Click a tunnel line to view detailed tunnel information.

Global Region View

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

If Multi-Region Fabric is enabled, click **Region** to display a topology diagram showing the access regions and the core region. The diagram indicates 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.

Security

The following dashlets and options are available on the **Monitor** > **Security** page in Cisco SD-WAN Manager:

Note In Cisco vManage Release 20.6.x and earlier releases, these options and dashlets are part of the **Dashboard** > **Security** page.

Table 2: 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

Dashlet Name	Version
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.

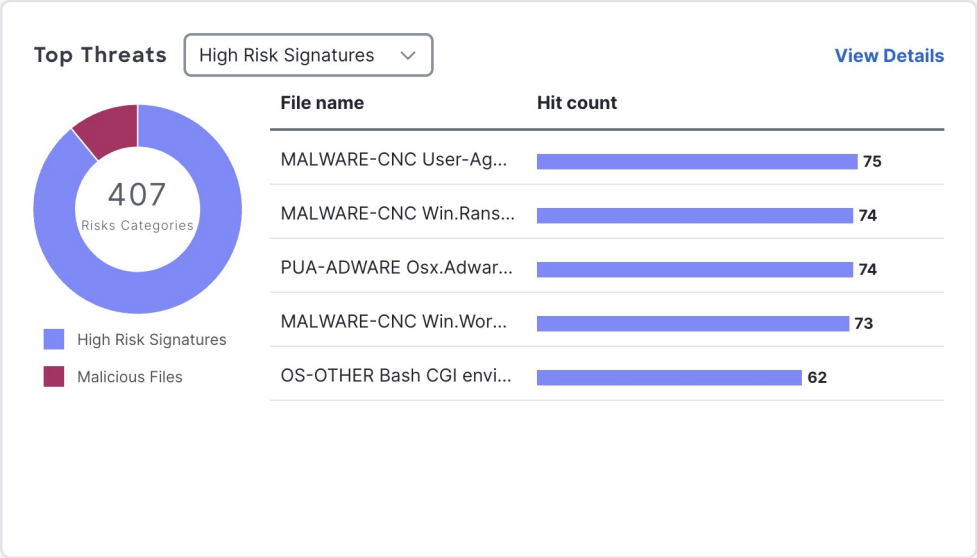
The **Actions** drop-down list in the security dashboard has the following options:

Table 3: Actions

Option	Description
Edit Security Dashboard	Choose this option to edit the security dashboard. You can perform the following 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.

Option	Description
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



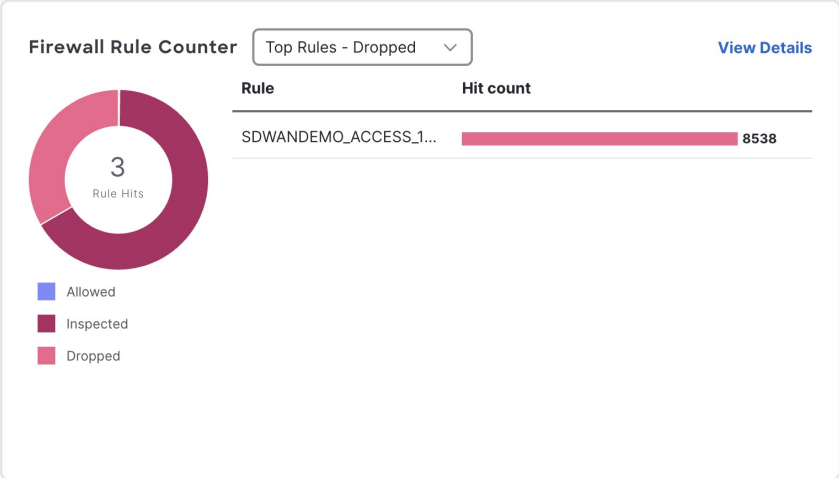
Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

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.

To view more information about the threats such as file name, type of event, device name, and more, click **View Details**. Click a device number in the **Devices Impacted** column to view the threat details at a device level.

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

View Firewall Rule Counter



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.

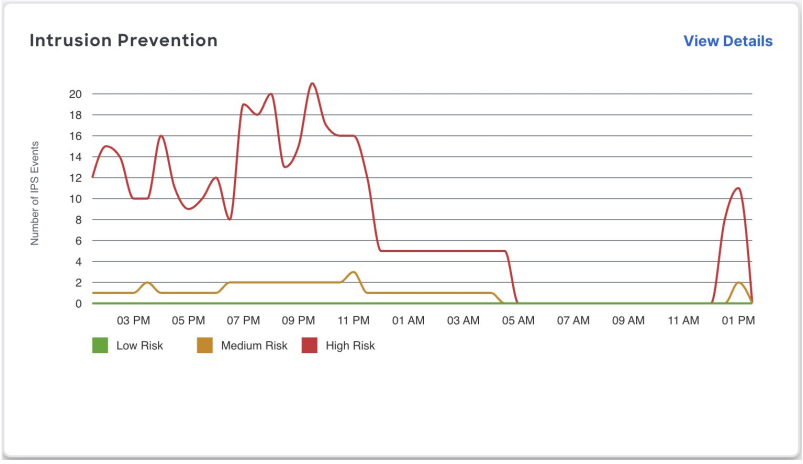
Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for data traffic inspection. Zone-based firewalls allow inspection of TCP, UDP, and ICMP data traffic. A zone can contain a group of one or more VPNs. Grouping VPNs into zones allows users to 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.

Note In Cisco vManage Release 20.6.x and earlier releases, Cisco SD-WAN Manager has the following behavior:

- The **FireWall Enforcement** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **FireWall Enforcement** pop-up window.

View Intrusion Prevention



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

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

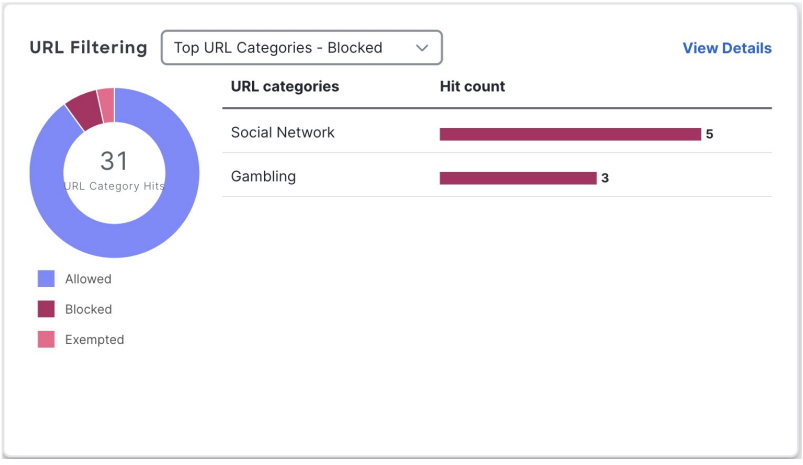
Click **View Details** to view to more details about a threat.

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.

Click a device number in the **Device Impacted** column to view more details about the threats at a device level.

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

View URL Filtering



The **URL Filtering** dashlet displays the categories of URLs that are allowed, blocked, or exempted from blocking.

Note 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.

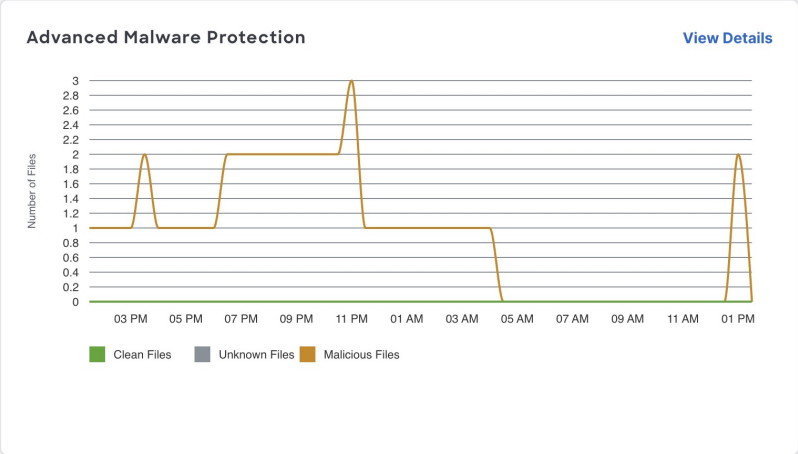
Choose an option in the **Top URL Categories** drop-down list to filter the URL categories and view information about a particular URL category.

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

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

- The **URL Filtering** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **URL Filtering** pop-up window.

View Advanced Malware Protection



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.

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.

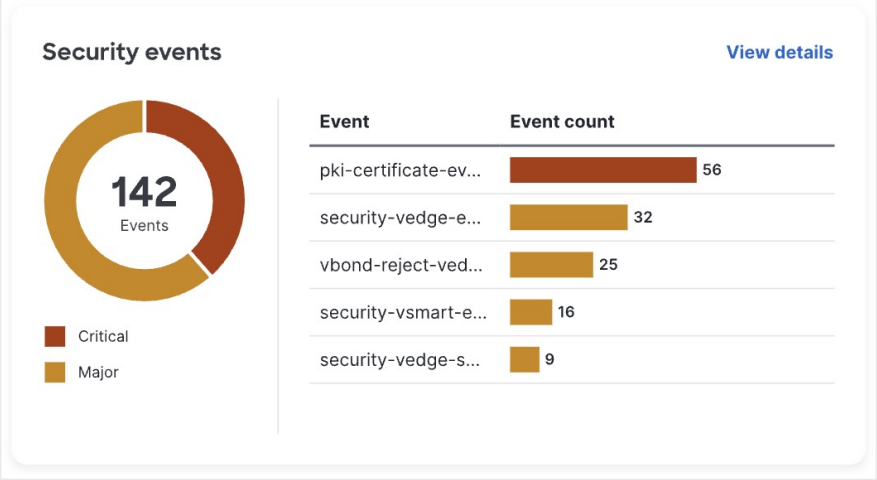
Click an entry in the **Last Occurrences** column to view additional information about the most recent event.

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

- The **Advanced Malware Protection** pane is part of the **Dashboard** > **Security** page.
- A filter icon instead of a drop-down list indicates the time period for which to display data.
- An expand icon instead of the **View Details** button opens the **Advanced Malware Protection** pop-up window.

View Security Events

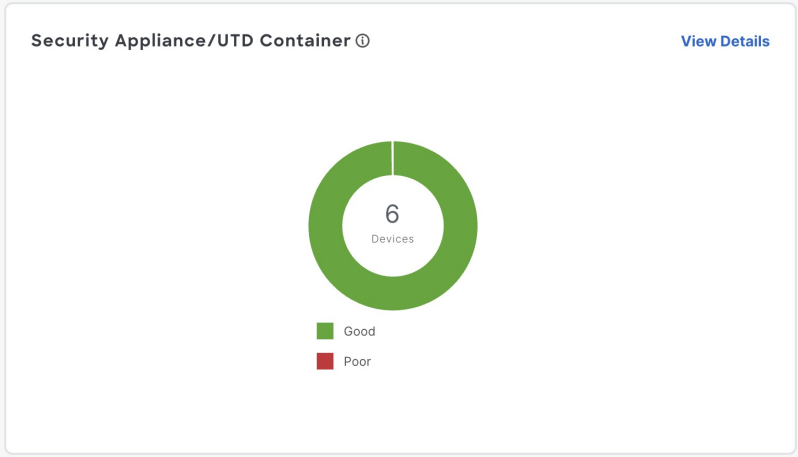


Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1.

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



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.

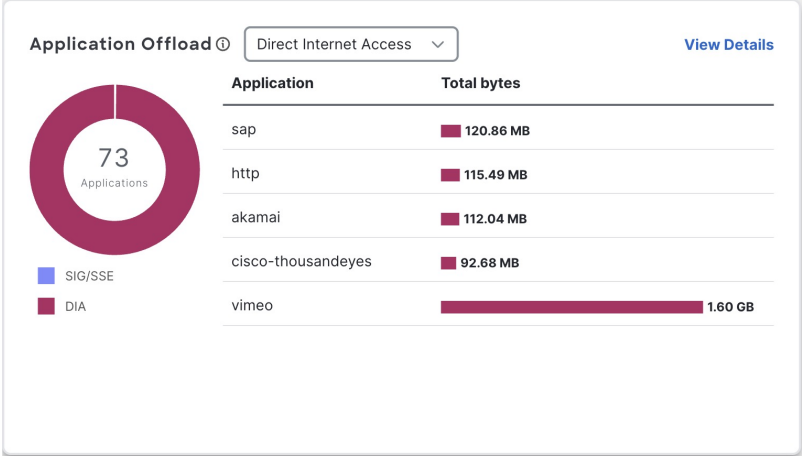
The dashlet provides an overview of various security components and monitors the following:

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

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.

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

View Application Offload



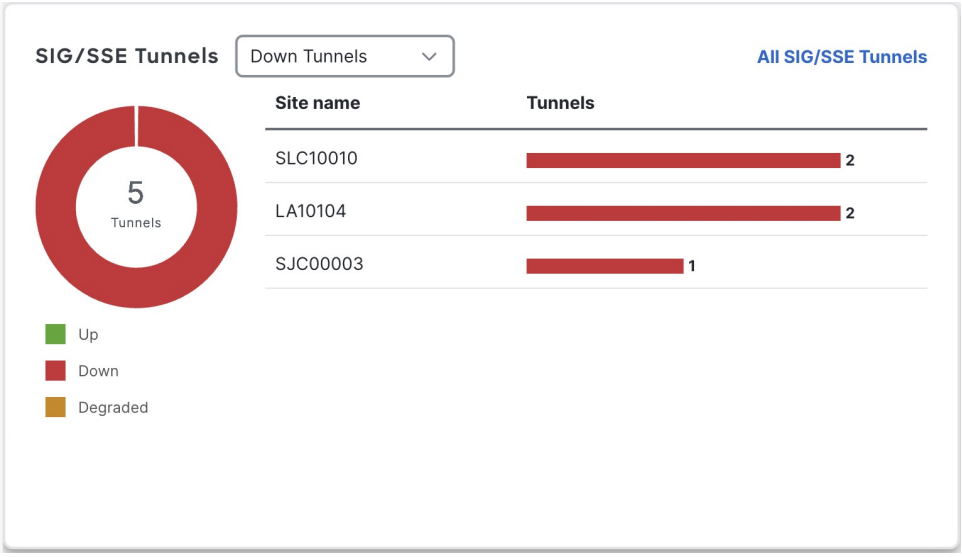
Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.14.1.

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 Tunnels



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.

View SecureX Ribbon



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

You use the **SecureX** ribbon to access the **SecureX** portal from the security dashboard.

The SecureX ribbon provides access to the applications you have configured in the SecureX portal. To access the SecureX portal, log in with your registered user credentials.

When you click **Show SecureX Ribbon** for the first time, the **SecureX Setup** dialog box is displayed. Perform the following steps to view the **SecureX** ribbon in the security dashboard:

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.

On successful authentication with SecureX, the **SecureX** ribbon is displayed in Cisco SD-WAN Manager.

Troubleshooting

Cannot See Data

Problem

Cannot see the data in the Security dashboard.

Possible Causes

It takes up to one hour for the Security dashboard to display traffic data.

Solution

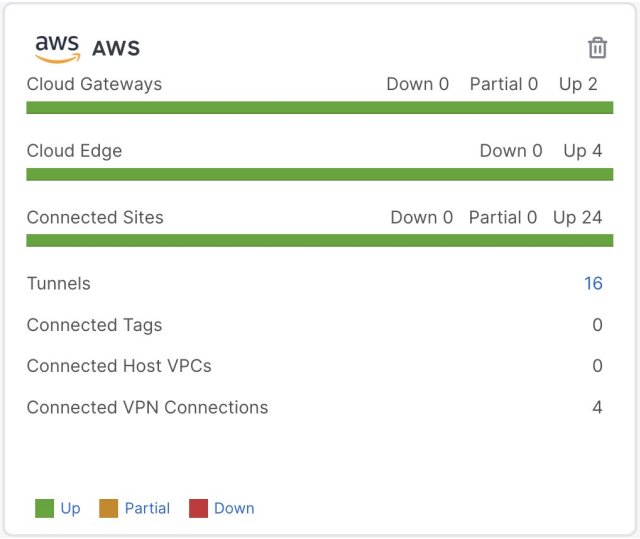
Choose a different time (1, 3, 6, or 24 hours) from the drop-down list.

Multicloud

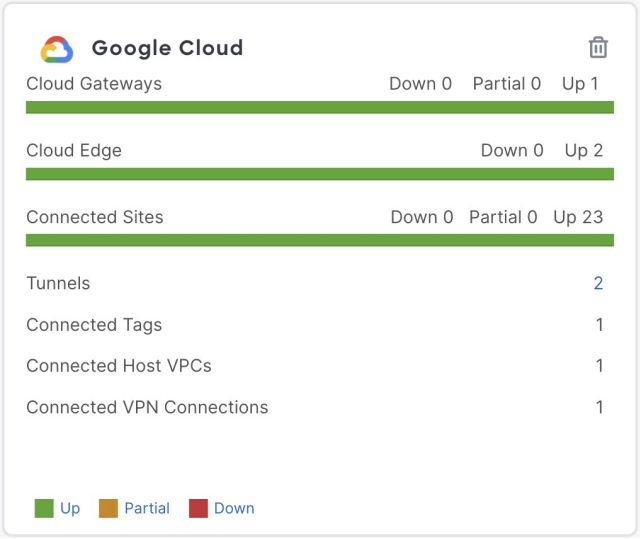
The following panes are available on the **Monitor** > **Multicloud** page in Cisco SD-WAN Manager:

Note In Cisco vManage Release 20.6.1 and earlier releases, these panes are part of the **Dashboard** > **Multicloud** page.

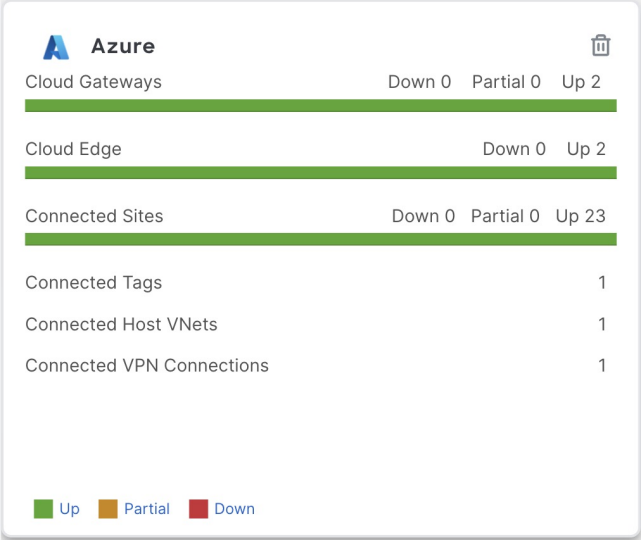
- **Amazon Web Service**



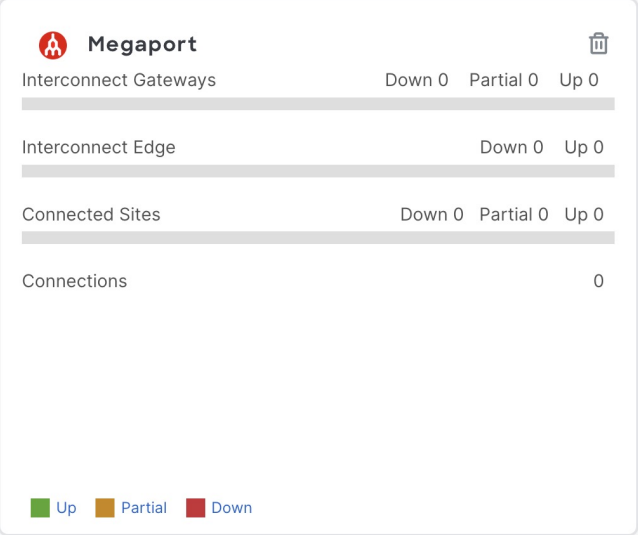
- **Google Cloud Platform**



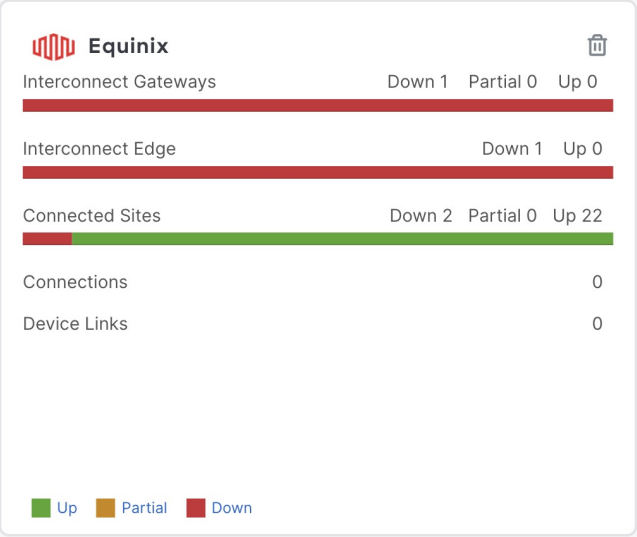
- **Microsoft Azure**



- **Megaport**



- **Equinix**



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

Explore

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

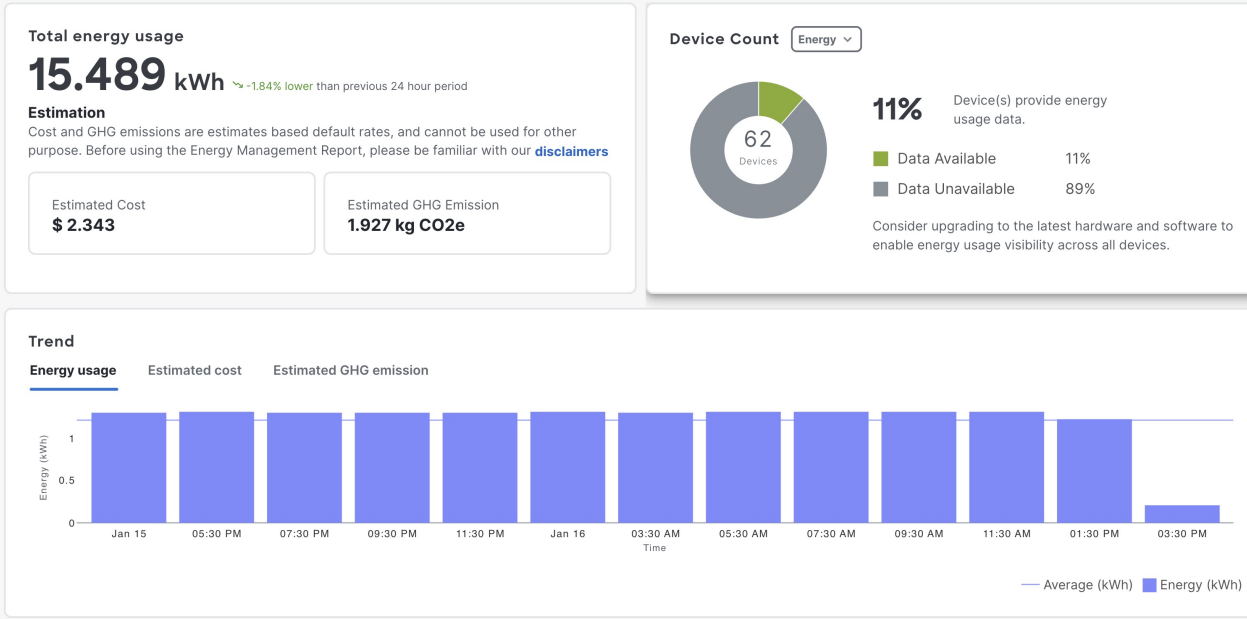
The **Explore** menu option opens a page presenting four job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. Based on the job role that you choose, the Explore page displays relevant Cisco Catalyst SD-WAN features, along with other Cisco resources such as developer guides, APIs, Cisco DNA Center,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

To view the Explore menu, perform the following steps:

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

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

Energy management



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.

Table 4:

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.

Supported Platforms for Energy Management

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

Advisories

The Cisco Catalyst SD-WAN Advisories feature is a solution that:

- Displays known security vulnerabilities, including potential known vulnerabilities on a Cisco secure WAN device, managed by the Cisco SD-WAN Manager.
- Displays field notices for non-security issues.
- Displays high and critical advisories, and field notices.

Flexible reporting

You can download security advisory data in CSV formats from Cisco SD-WAN Manager to analyze and manage network vulnerabilities. You can download this data for individual devices or the entire network.

Benefits of Advisories

- **Centralized visibility:**

  Provides a centralized dashboard to view security advisories across the entire Cisco SD-WAN network.

- **Actionable insights:**

  Provides recommended corrective actions to mitigate identified security risks.

Prerequisites for Advisories

- Enable cloud services from the **Admin** > **Settings** page using Cisco Smart Accountor Virtual Account credentials.
- For on-prem Cisco SD-WAN Managers, ensure the firewall is configured to allow access to the following URLs:
  - **SSP**: ssp.sdwan.cisco.com
  - **Okta**: id.cisco.com
  - **CX**: api-cx.cisco.com

View Security Advisory

To view and manage security advisories in Cisco SD-WAN Manager, follow these steps:

The following settings are enabled by default:

- Advisory collection: Enabled when you activate Cloud Services.
- Interval scan: Enabled
- Scan frequency: Set to once a week
- Advanced scan: Enabled and operates based on the device configuration.

Procedure

Step 1 From the Cisco SD-WAN Manager, choose **Monitor** > **Advisories**.

Step 2 Select **Security Advisory**.

Step 3 Select **Devices** or **Advisories** to view relevant security information.

- **Devices:** Lists all devices in your network and clearly indicates which devices have associated security risks.
- **Advisories:** Lists all active security advisories relevant to the network. Advisories can be either **Active**, requiring attention, or **Acknowledge**, indicating that action is being taken**.**

  To move an advisory to the acknowledged state, select the advisory and click **Acknowledge**.

Perform a scan in Advisories

Follow these steps to perform a scan to identify vulnerabilities, ensure compliance, and view actionable risk mitigation insights..

Procedure

Step 1 From Cisco SD-WAN Manager, select **Monitor** > **Advisories**

Step 2 Select **Security Advisory** > **More actions**.

Step 3 Choose **Scan now** from the drop down list to immediately check your network for vulnerabilities.

- **Affected**: Identifies devices known to be vulnerable based on Cisco SD-WAN Manager's analysis.
- **Potentially Affected**:Indicates a possible vulnerability and requires a detailed device analysis to confirm any vulnerabilities.

Note

After you add a new control component, run an on-demand advisory scan or wait for the next scheduled scan to update the Advisories inventory before performing Shield management operations.

View Field Notices

View Field Notices to stay informed about significant product-related issues, that may require upgrades, workarounds, or other actions.

Procedure

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

Step 2 Select **Field Notices**.

Converged Dashboard for SD-WAN Analytics and SD-WAN Manager

Information About 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 as follows:

- 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

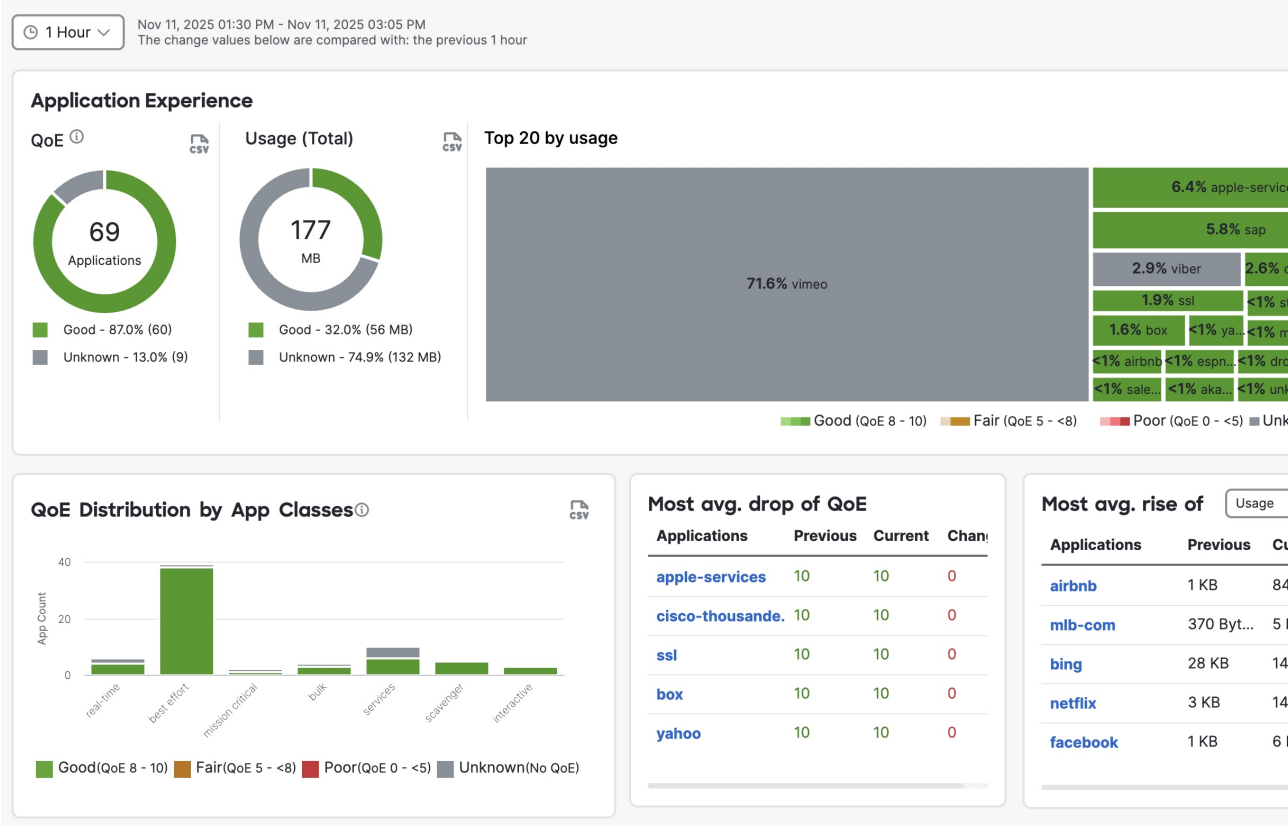
The **Applications** dashboard displays information on how different applications are performing across an overlay for all sites, and for a single site. The **Applications** dashboard gives an overview of Application performance for all applications across an overlay and across all sites, and compares 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

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.

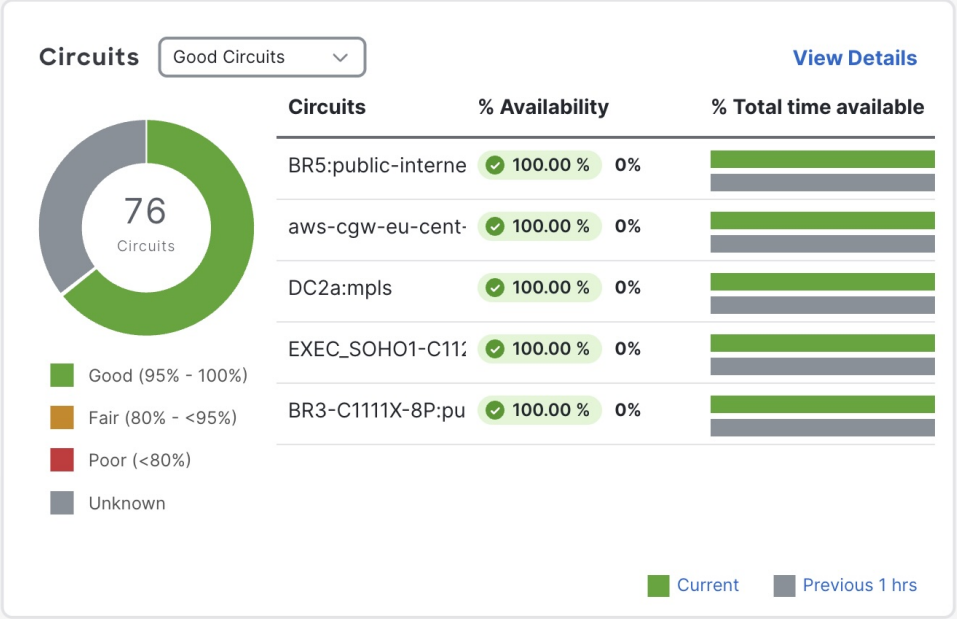
For more information about Sites analytics, see Site Dashboard in Cisco SD-WAN Analytics.

Circuits Dashboard

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:

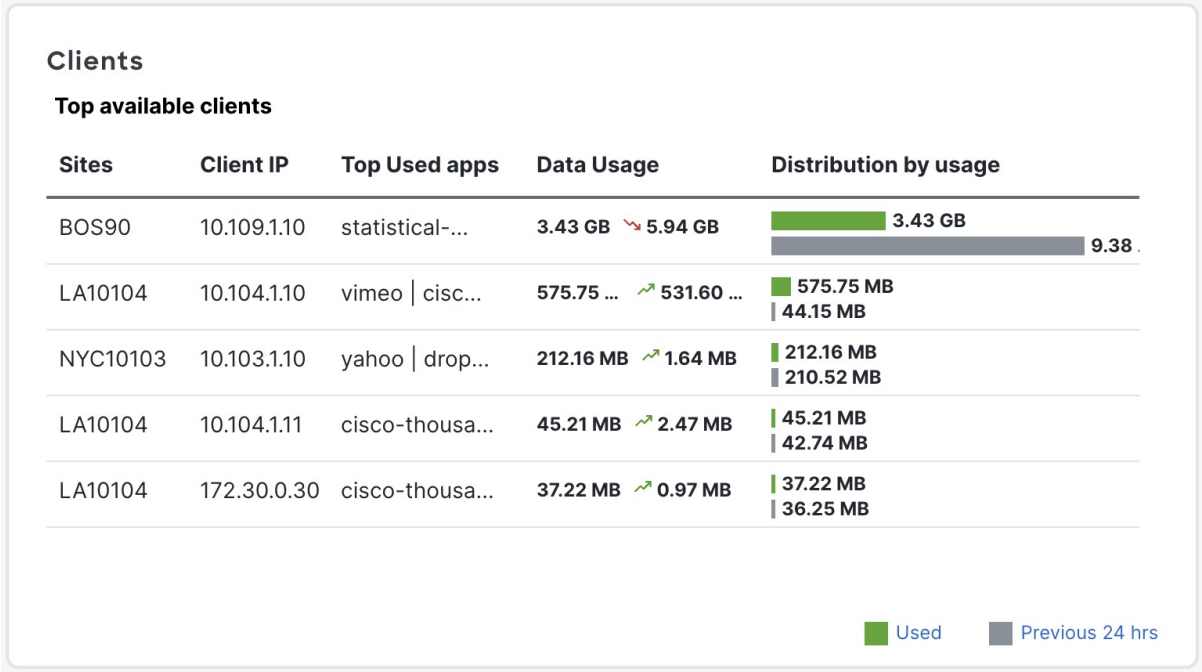
Figure 8: Circuits



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

Client Dashlet

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 6.