Cisco vManage Monitor Overview

Table 1: Feature History

Feature Name	Release Information	Description
Enhanced Cisco vManage User Interface for a Consolidated Monitoring View	Cisco vManage Release 20.7.1	This feature introduces the enhanced user interface of Cisco vManage. 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 SD-WAN overlay network. It provides an entry point for all Cisco vManage 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 vManage 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 vManage	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 vManage	Cisco vManage Release 20.10.1	The time filter option added to the **Monitor Overview** and **Monitor Security** dashboards in Cisco vManage enables you to filter the dashboard data for a specified time range.

The following dashlets are available on the **Monitor** > **Overview** dashboard in Cisco vManage. (In Cisco vManage Release 20.6.x and earlier releases, these dashlets are part of **Dashboard** > **Main Dashboard**.)

- **WAN Edge Health**
- **Site BFD Connectivity**
- **Transport Interface Distribution**

- **WAN Edge Inventory**
- **Transport Health**
- **Top Applications**
- **Application-Aware Routing**

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 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 vManage again.
- When you navigate from another window to the **Monitor Overview** dashboard.
- When you upgrade Cisco vManage from an earlier release to a new release.

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 vManage 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**.

Delete a Dashlet

1. From the Cisco vManage 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 vManage 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 vManage 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 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.

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 vManage 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.

View Controller and Device Information

The **Controllers** and **WAN Edges** areas of the menu bar, which runs across the top of the **Monitor** > **Overview** page, display the total number of Cisco vSmart Controllers, Cisco vBond Orchestrators, and Cisco vManage 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 Cisco vManage Release 20.6.x and earlier releases, Cisco vManage has the following behavior:

- The **Controllers** 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 vManage Status

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

1. From the Cisco vManage 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**.

   For a Cisco vManage controller, the health status indicates the following:

   - **Good**: Cisco vManage is using less than 75% of available memory, and less than 75% of CPU resources.
   - **Fair**: Cisco vManage is using between 75% and 90% of total memory or CPU.
   - **Poor**: Cisco vManage is using more than 90% of total memory or CPU.

2. Click a Cisco vManage 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 vManage controller is using more than 90% of total memory or CPU, its performance may be degraded. If you cannot log in to Cisco vManage, contact Cisco TAC for assistance.

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.x and earlier releases, Cisco vManage 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.x and earlier releases, Cisco vManage 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.x and earlier releases, Cisco vManage 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.x and earlier releases.

The **Control Status** pane displays whether Cisco vSmart and WAN Edge devices are connected to the required number of Cisco vSmart Controllers. Each Cisco vSmart Controller must connect to all other Cisco vSmart Controllers in the network. Each WAN Edge router must connect to the configured maximum number of Cisco vSmart 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 vSmart Controller.
- **Partial**: Total number of devices with some, but not all, operational control plane connections to Cisco vSmart Controllers.
- **Down**: Total number of devices with no control plane connection to a Cisco vSmart Controller.

Note The **Control Status** pane depends upon both Cisco vManage control connection and vSmart 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.x and earlier releases, Cisco vManage 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 donut 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 SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer,calleda 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.x and earlier releases, Cisco vManage 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. 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.x and earlier releases, Cisco vManage 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 the vManage 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 vManage.

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.x and earlier releases, Cisco vManage 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 75% of total memory or total CPU is classified as good.
- **Fair**: Number of routers with memory, hardware, or CPU in fair state. Using between 75% and 90% of total memory or total CPU is classified as in a fair state.
- **Poor**: Number of routers with memory, hardware, or CPU in poor state. Using more than 90% of total memory or total CPU is classified as in a poor state.

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.x and earlier releases, Cisco vManage 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 hardware node is classified as normal if it uses 70% of total memory or total CPU instead of 75%. Similarly, it is classified as in a warning state if it uses between 75% and 90% of total memory or total CPU instead of the range of 70%-90%.
- A pop-up window opens instead of a sidebar when you click the data.
- The Device Dashboard or Device Details view is part of he **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.x and earlier releases, Cisco vManage 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 vManage **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.x 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.x 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.x and earlier releases, Cisco vManage 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 vManage 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.x and earlier releases, Cisco vManage 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 vManage 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 vManage **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.x 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 vManage server, in the **Administration** > **Settings**, the Cisco vManage **Monitor** > **Overview** page displays a maintenance window alert notification two days before the start of the window.

Note In Cisco vManage Release 20.6.x 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). The application bandwidth usage information is displayed 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.

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**.

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

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.

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 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.

You can view information for all sites by clicking the **All Sites** button on the top of the page, and clicking the radio button next to **All Sites**. You can view information for a single site by clicking the **All Sites** button on the top of the page, and clicking the radio button next to **Single Site**. Click the radio button next to the site to enter the single site view.

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. The dashlet also displays bandwidth usage information for each site. 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.
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. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

Security

The following panes are available on the **Monitor** > **Security** page in Cisco vManage:

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

- **Firewall Enforcement**
- **Top Signature Hits**
- **URL Filtering**
- **Advanced Malware Protection**

View Firewall Enforcement Pane

From the Cisco vManage menu, choose **Monitor** > **Security**. The **Firewall Enforcement** pane displays the number of sessions that were inspected or dropped over the specified time period.

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.

Click **Inspected** to see the number of inspected data sessions.

Click **Dropped** to see the number of dropped packets.

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

Click **View Details** to open the **Firewall Enforcement** sidebar. It displays a more detailed view of the same information. To display the information in tabular format, click **Details**. You can change the time period to view details for the specified duration.

Note In Cisco vManage Release 20.6.x and earlier releases, Cisco vManage 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 Top Signature Hits Pane

From the Cisco vManage menu, choose **Monitor** > **Security**. The **Top Signature Hits** pane displays the Intrusion Prevention System (IPS) signature violations by severity or by count over the specified time period. IPS uses Cisco Talos signatures for monitoring network traffic.

Click **By Severity** to filter signature violations by severity.

Click **By Count** to filter signature violations by count.

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

Click **View Details** to open the **Top Signature Hits** sidebar. It displays a more detailed view of the same information. To display the information in tabular format, click **Details**. You can change the time period to view the information for the specified duration.

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

- The **Top Signature Hits** 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 **Top Signature Hits** pop-up window.

View URL Filtering Pane

From the Cisco vManage menu, select **Monitor** > **Security**. The **URL Filtering** pane displays the number and types of URLs that were blocked or allowed over the specified time period.

Click **Blocked** to see the list of blocked websites.

Click **Allowed** to see the list of allowed websites.

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

Click **View Details** to open the **URL Filtering** sidebar. It displays a more detailed view of the same information. To display the information in tabular format, click **Details**. You can change the time period to view the information for the specified duration.

Note In Cisco vManage Release 20.6.x and earlier releases, Cisco vManage 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 Pane

From the Cisco vManage menu, choose **Monitor** > **Security**. 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.

Click **File Reputation** to see the number of malicious files detected by AMP over the selected time internal.

Click **File Analysis** to see the number of unknown files uploaded to Cisco AMP Threat Grid over the selected time interval.

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

Click **View Details** to open the **Advanced Malware Protection** sidebar. It displays a more detailed view of the same information. To display the information in tabular format, click **Details**. You can change the time period to view the information for the specified duration.

Note In Cisco vManage Release 20.6.x and earlier releases, Cisco vManage 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.

Multicloud

The following panes are available on the **Monitor** > **Multicloud** page in Cisco vManage:

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

- **Amazon Web Service**
- **Google Cloud Platform**
- **Microsoft Azure**
- **Megaport**

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