View Integrated Monitoring and Analytics

For supported software information, click here.

The View tab provides a combination of monitoring and analytics in Concerto. Live and historical data are available at a single location and the information that you can view depends on your role and the tenant license. View displays dashboards for Versa secure private access (VSPA), security, and secure SD-WAN services.

This article describes:

- The statistics for VSPA users for a tenant, site-to-site tunnel, and route details
- Summary of security actions and threats, internet protection statistics, and private application protection statistics
- Realtime statistics of secure SD-WAN devices
- How to use monitoring tools to run ping, traceroute, and speed test

View Secure Access Information

Concerto collects various statistics about a tenant's VSPA users that you can display from the View tab. For each tenant, the Secure Access tab displays information about the following:

- Overview—Successful, failed login attempts, active users, and dashboards for statistics.
- Users—Displays the statistics of the VSPA client users based on usage, events, and registry.
- Digital Experience—(For Releases 12.1.1 and later.) Displays information about the end-to-end network and application experience for each user device.
- Site to Site Tunnels—Displays the tunnels that are up and down, tunnel status, top tunnels by bandwidth.
- Routes—Displays route details such as destination, state, protocol, and RPM.
- Logs—Displays events, policies, and charts for authentication log, as well as for endpoint information.

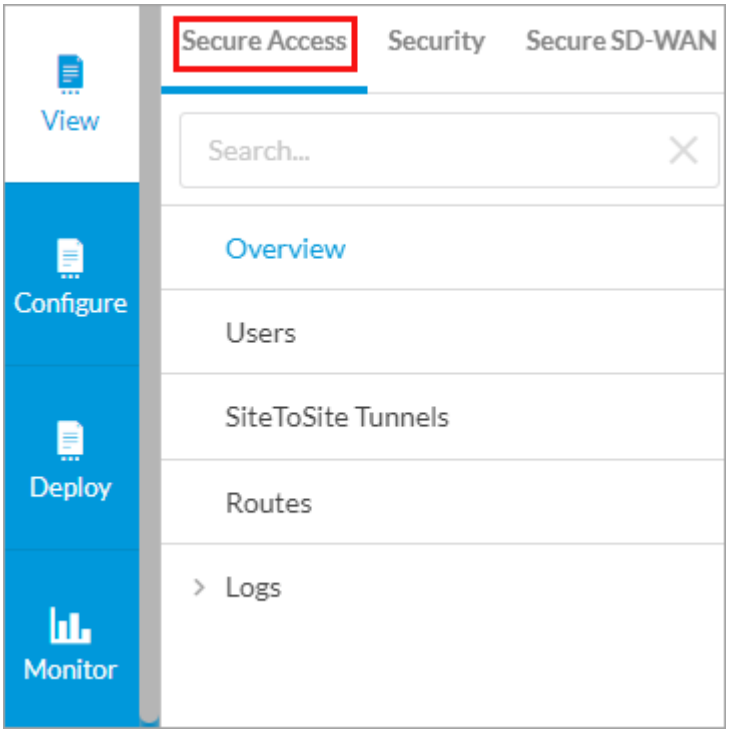
VSPA Overview Tab

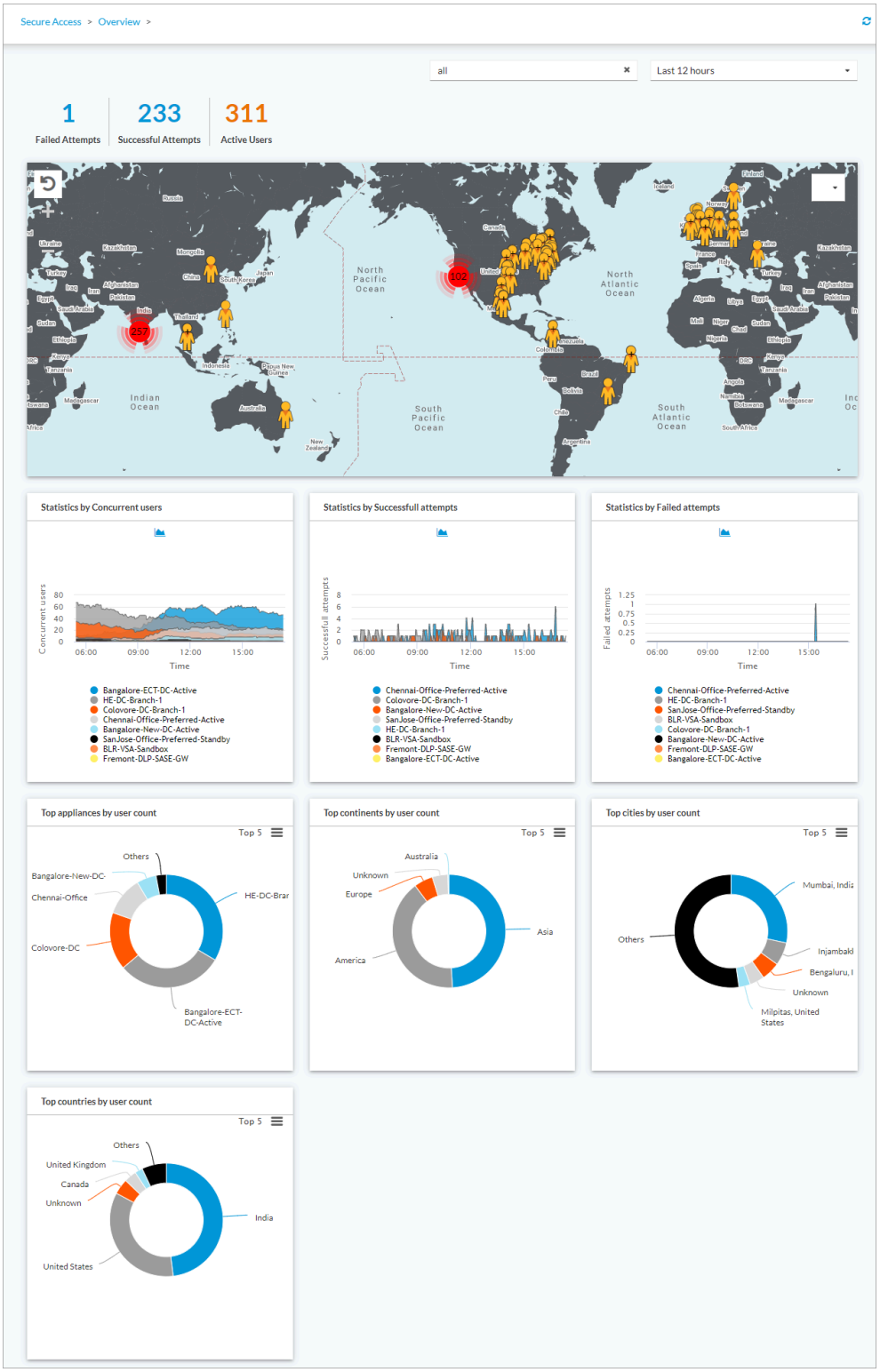
The VSPA Overview tab displays the following:

- Failed and successful attempts
- Number of active users
- Statistics for users and attempts

To display VSPA overview information:

1. Select View in the left navigation pane. The Secure Access > Overview page displays by default.

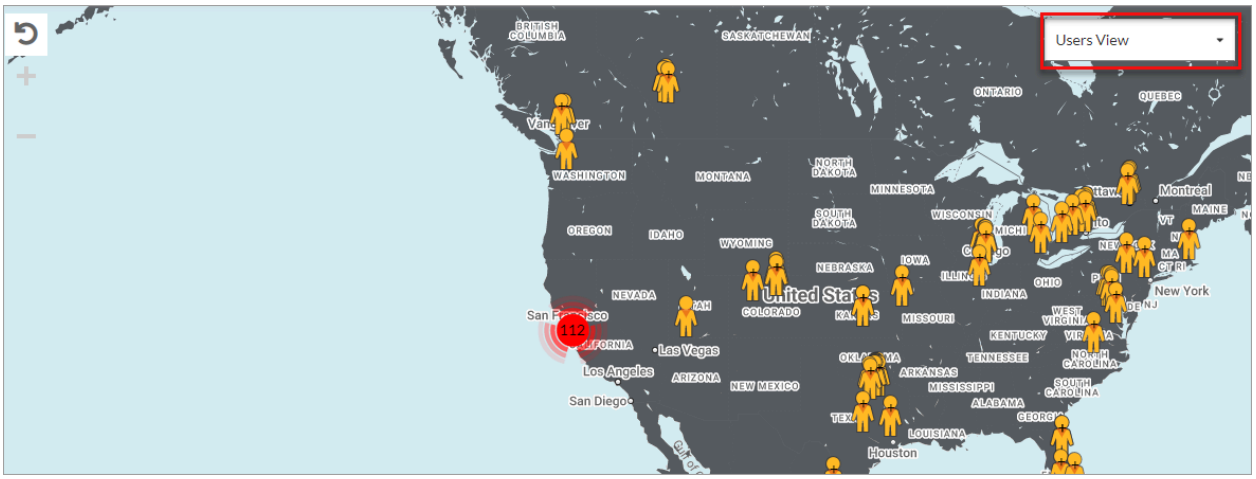




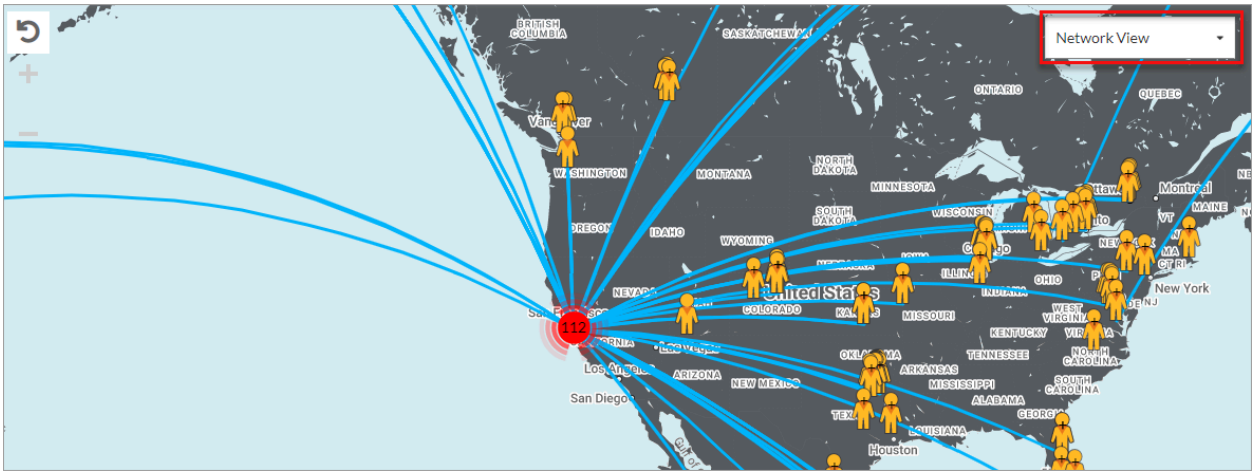
2. In the horizontal menu bar, select the device and select the time interval for which to display information:
   - Last 5 minutes
   - Last 15 minutes

- Last 30 minutes
- Last hour
- Last 12 hours
- Last day
- Last 7 days
- Last month
- Custom range

3. To display maps with VSPA information about a tenant's users, select Users View (default).



4. Click a  User icon to display the following information about the user:
   - User—Email address of the user
   - Appliance—Appliance name of the user
   - IP—User's WAN IP address
5. Click Network View to display the geographical location of active users during the specified time range.



Updated: Wed, 23 Oct 2024 08:54:28 GMT

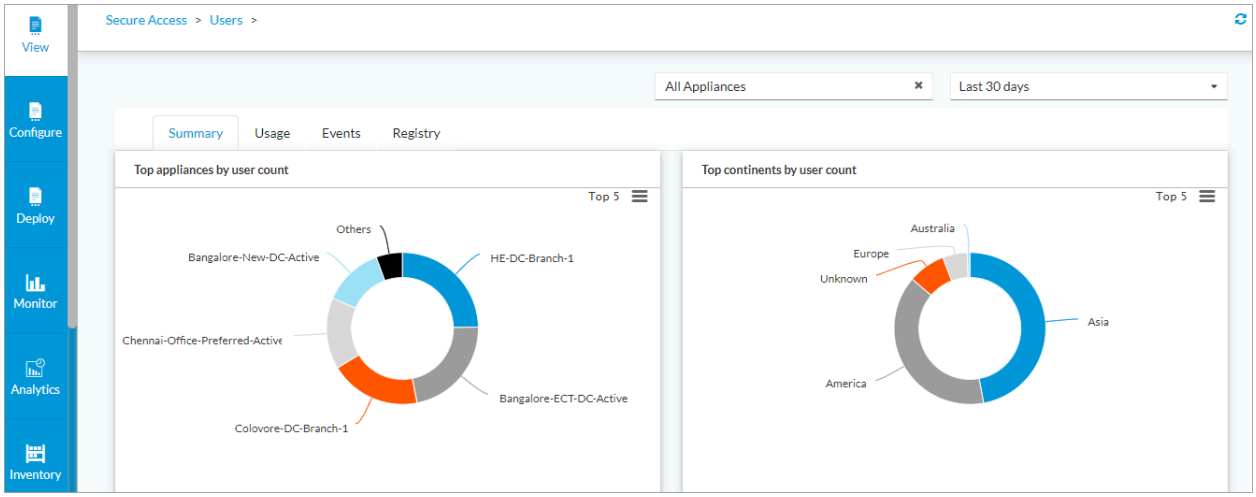
6. For more information about the user displaying a tenant's VSPA features, see Users View below.

Users View

Users view shows statistics about a tenant's VSPA users, including summary, usage, events, and registry.

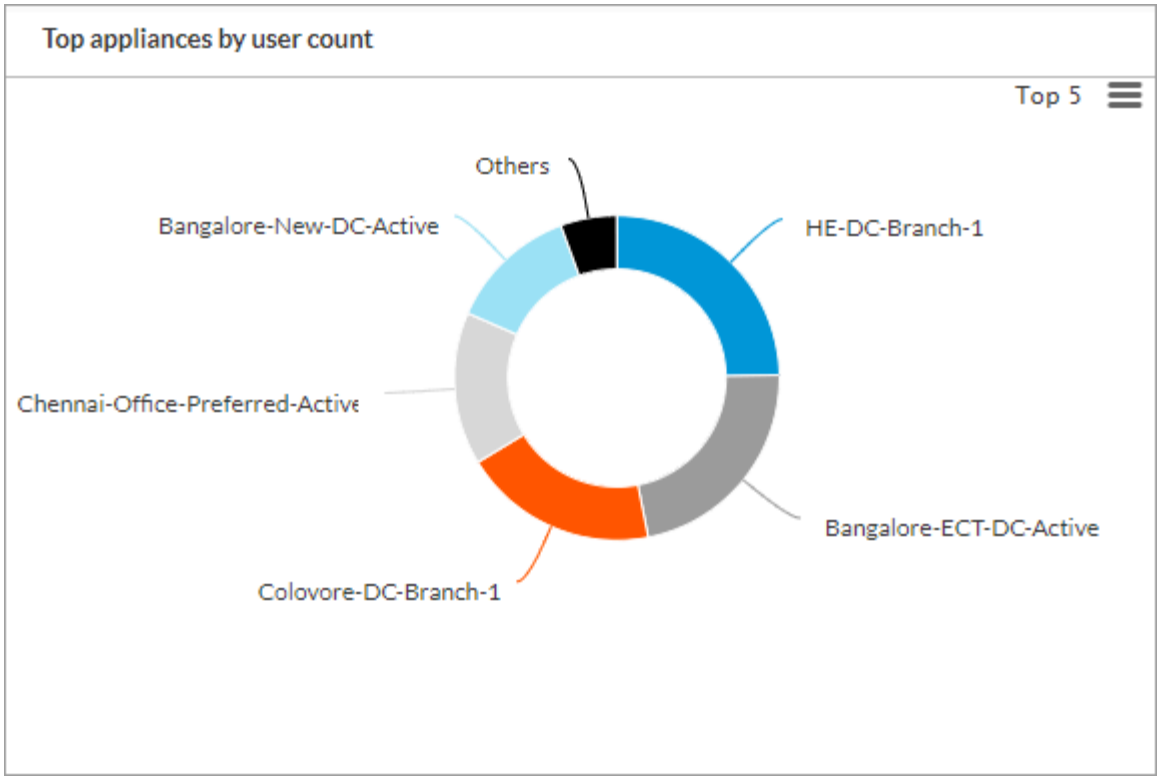
To display VSPA information about a tenant's users:

1. Select View in the left navigation pane.
2. Select Secure Access > Users. The dashboard has the following tabs:
   - Summary
   - Usage
   - Events
   - Registry

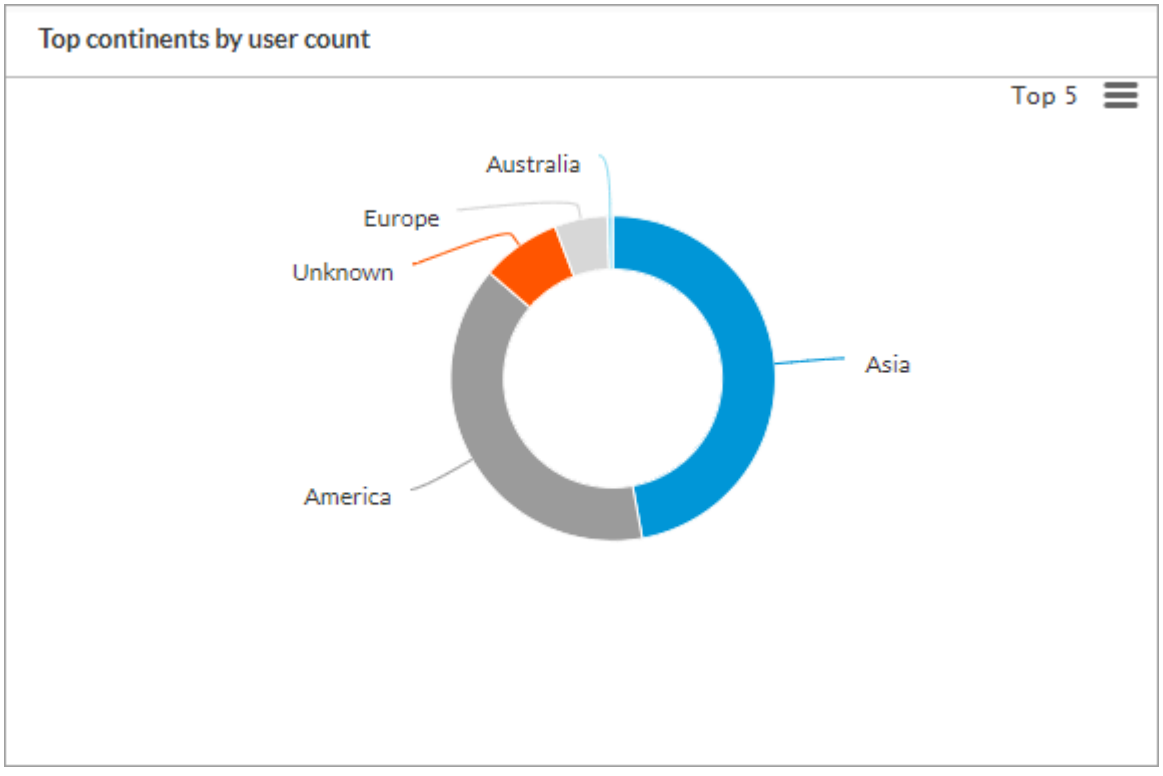


3. Select the Summary tab to view a summary of user analytics statistics by user count for top devices, continents, countries, and cities. The Summary tab displays the following panes:
   - Top devices by user count

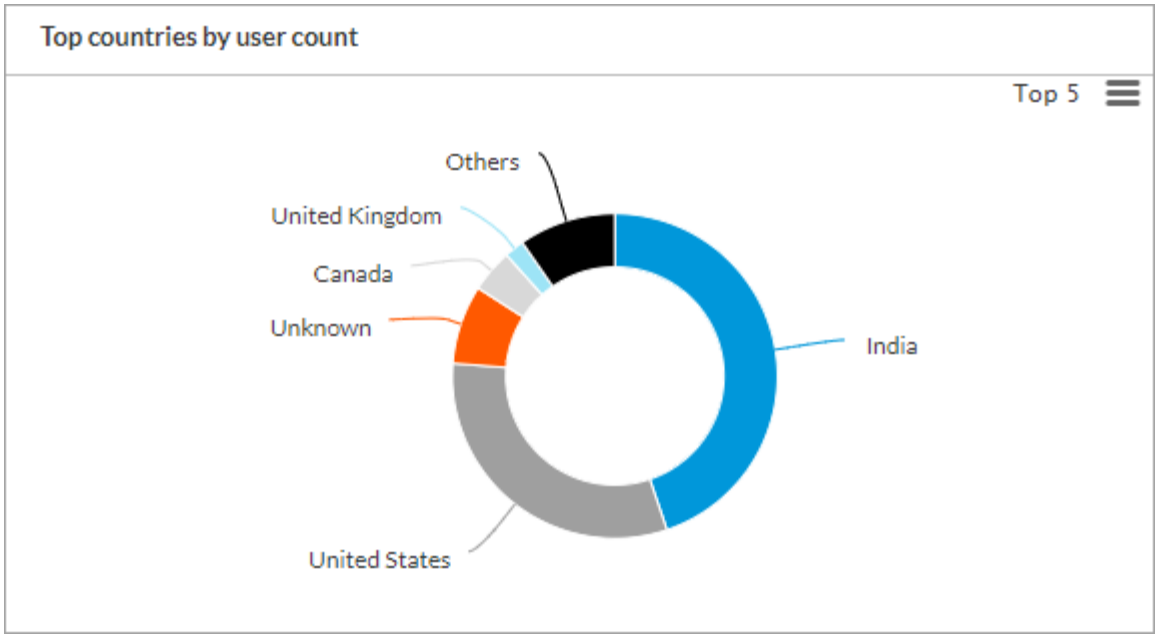
Updated: Wed, 23 Oct 2024 08:54:28 GMT



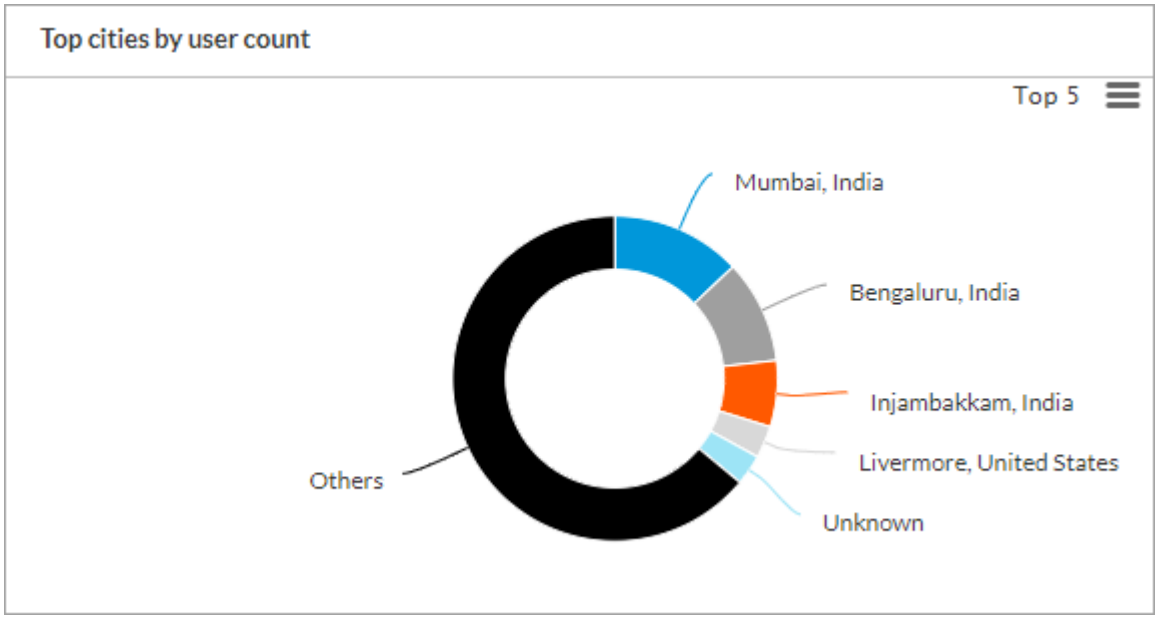
- Top continents by user count



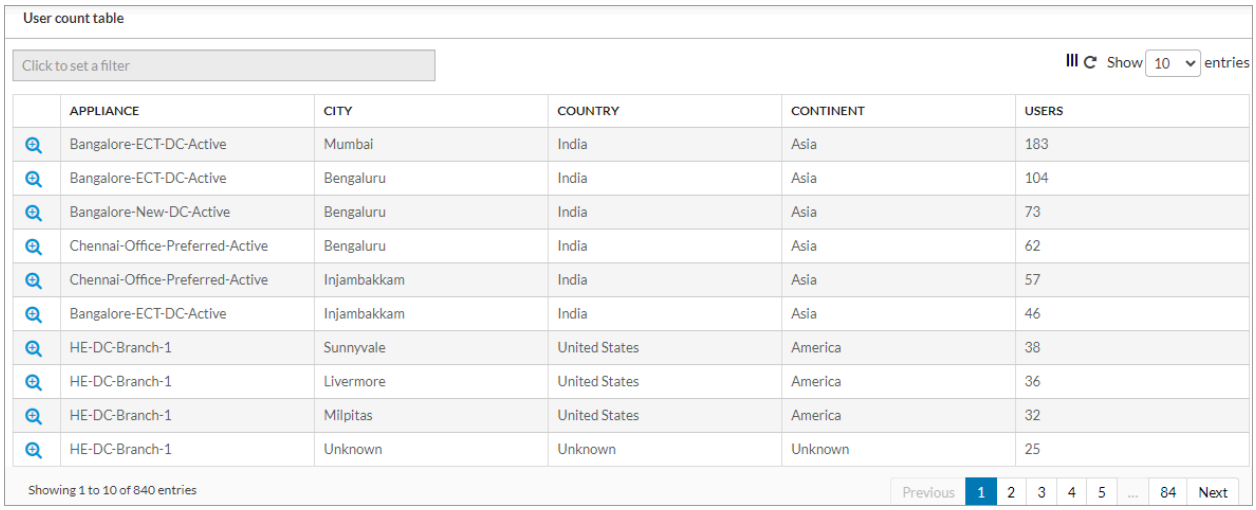
- Top countries by user count



- Top cities by user count



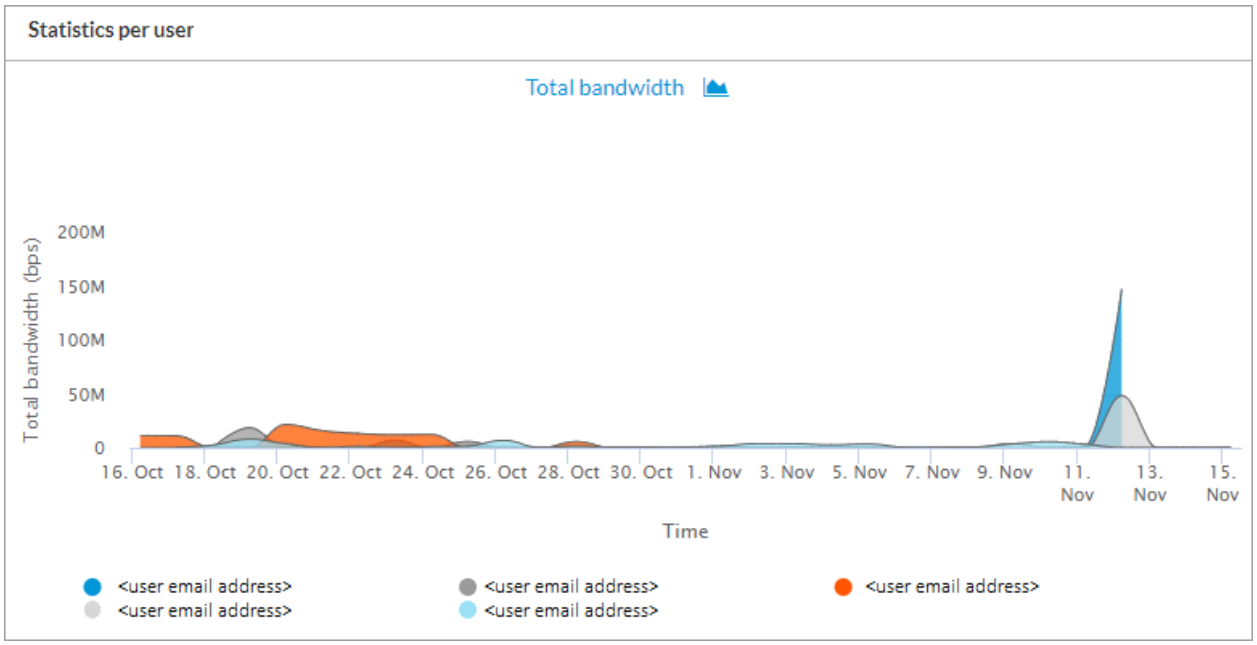
- User count table



Click the Zoom icon to view user statistics for each device.

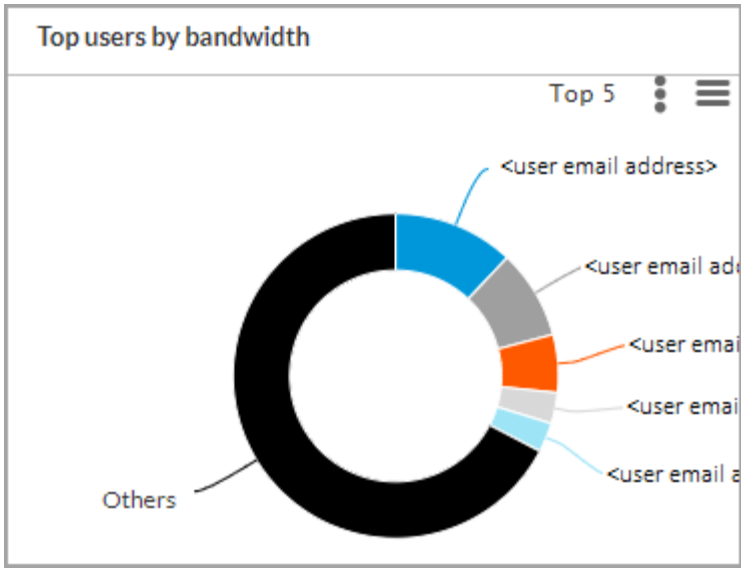
4. Select the Usage tab to view analytics statistics per user and top users. The Usage tab displays the following panes:

   - Statistics per user



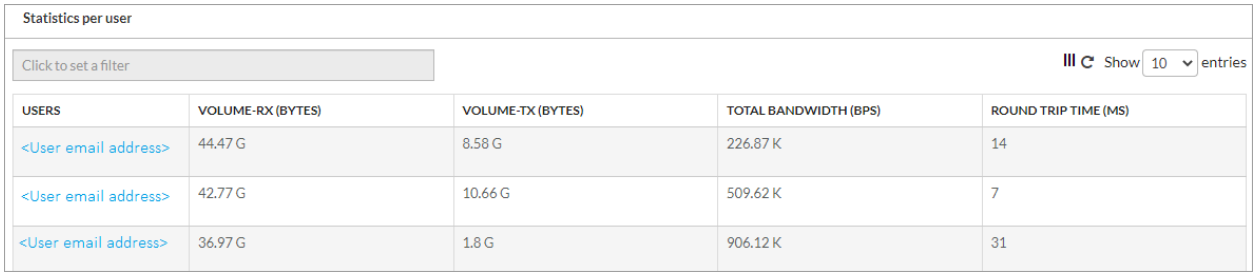
To change the graphical representation of data, click the Chart Menu icon to select the current graphical data representation. The format can be Column, Bar, Stacked Bar, Area, Line, or Scattered Chart.

   - Top users by bandwidth



To change the graphical representation of data, use the following icons in the pane:

- Click the Metrics Menu icon to select the view type. The view type can be one of the following:
  - Bandwidth
  - Volume received (RX)
  - Volume transmitted (TX)
  - Volume received and transmitted
  - Bandwidth received and transmitted
  - Round-trip time
- Statistics per user



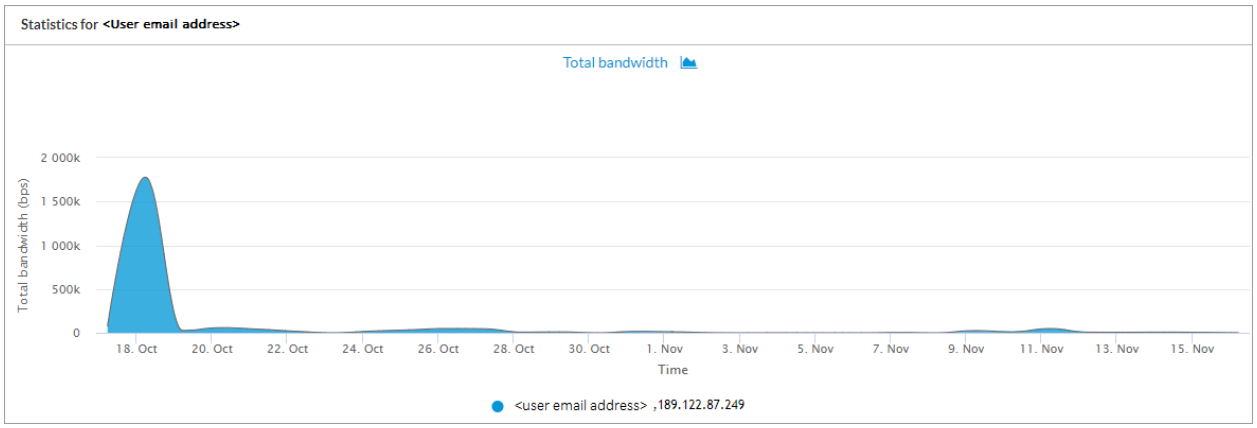
Field	Description
Users	Displays the username.
Volume-RX (Bytes)	Displays the amount of data received by the user, in bytes.
Volume-TX (Bytes)	Displays the amount of data transmitted by the user, in bytes.

Field	Description
Total Bandwidth (bps)	Displays the total bandwidth used by the user, in bits per second.
Round-Trip Time (ms)	Displays the round-trip time from the VSPA client to the gateway, in milliseconds.

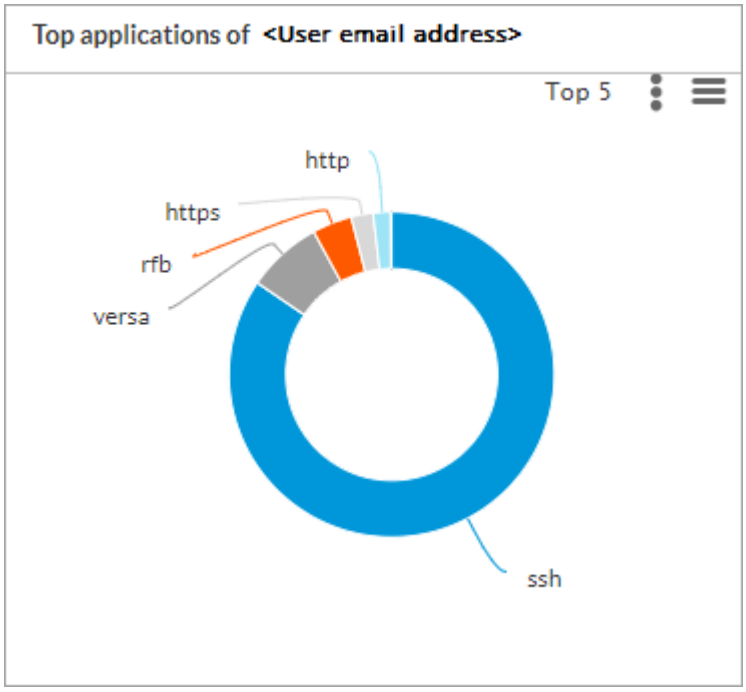
- Click Copy, CSV, or PDF to copy the search results or to save them in a PDF file or in a file in CSV format.

a. Drill down on a specific user to display a user's statistics by bandwidth, applications, business tags, and categories. The drill-down displays the following panes:

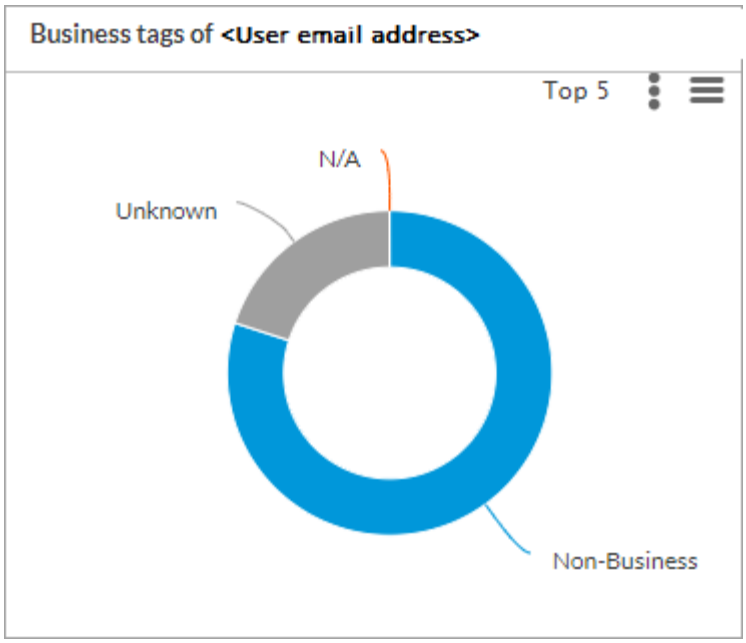
- User statistics by total bandwidth



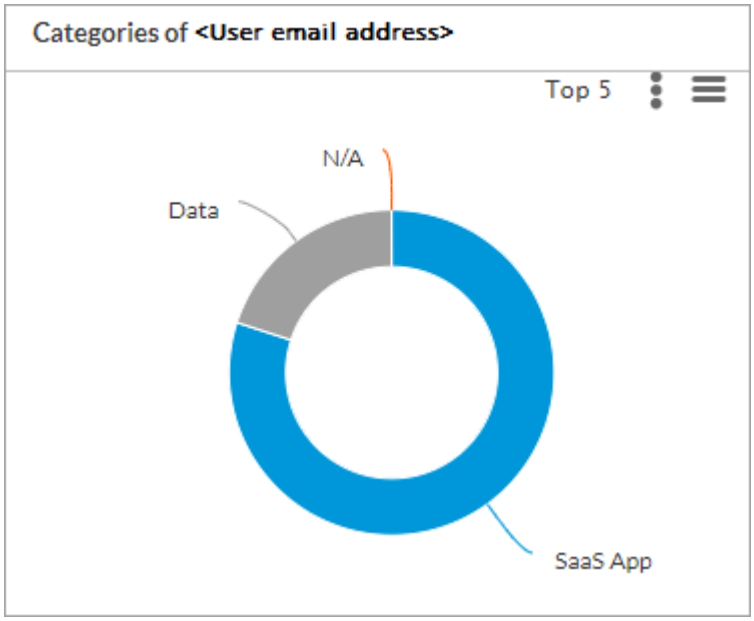
- User's top applications



- User's business tags



- User's data categories



- User-specific statistics

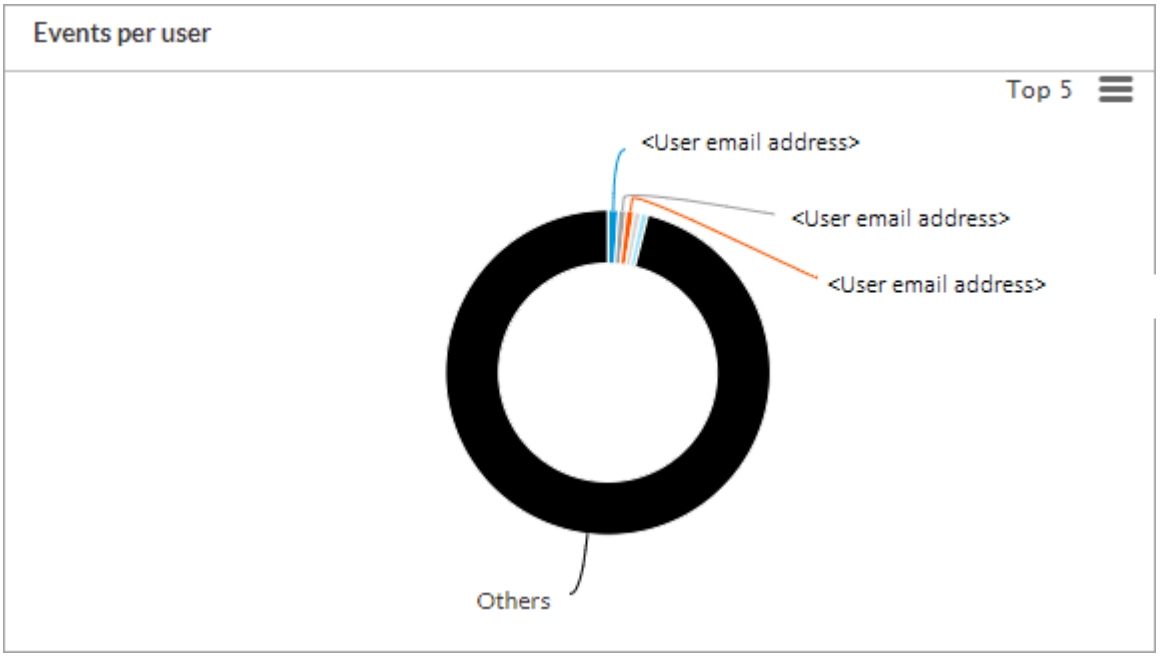
Statistics for **<User email address>**

Show 10 entries

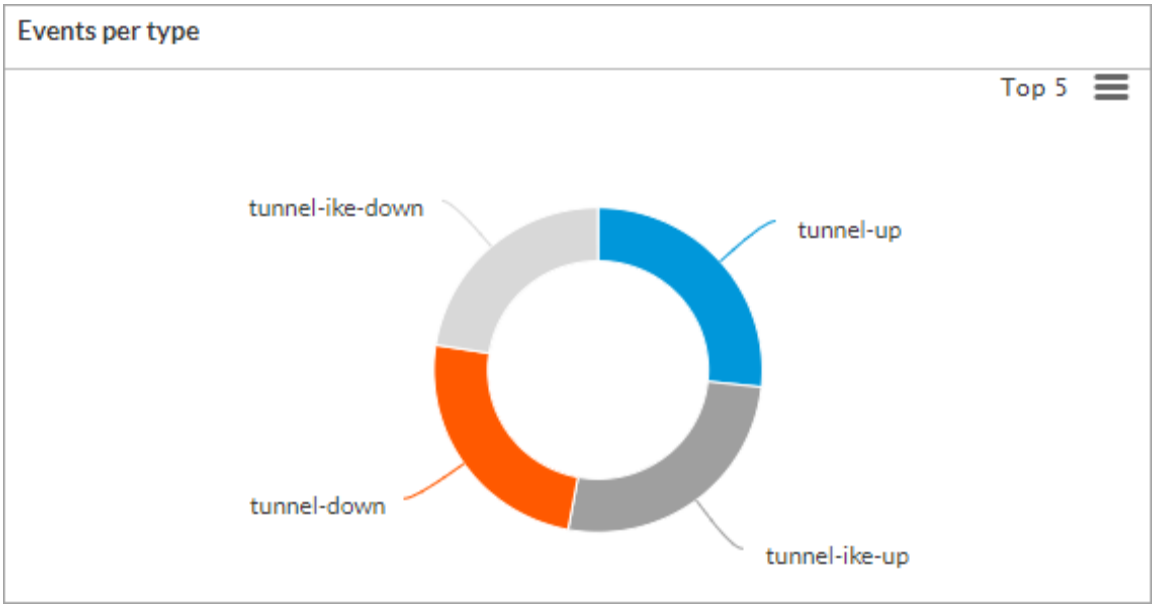
USERS	LATITUDE, LONGITUDE	CITY	COUNTRY	IP	ISP	VOLU
<User email address>	-22.9581,-43.1930	Rio de Janeiro	Brazil	189.122.87.249	Claro NXT Telecomunicacoes Ltda	12.9
<User email address>	-22.9570,-43.1930	Rio de Janeiro	Brazil	189.122.87.249	Claro NXT Telecomunicacoes Ltda	70.8

b. Select the Events tab to view the events per user, type, and authentication failures. The common reasons for authentication failures are invalid username or password, OTP mismatch, cipher mismatch, and server tunnel IP address exhaustion. The Events tab displays the following panes:

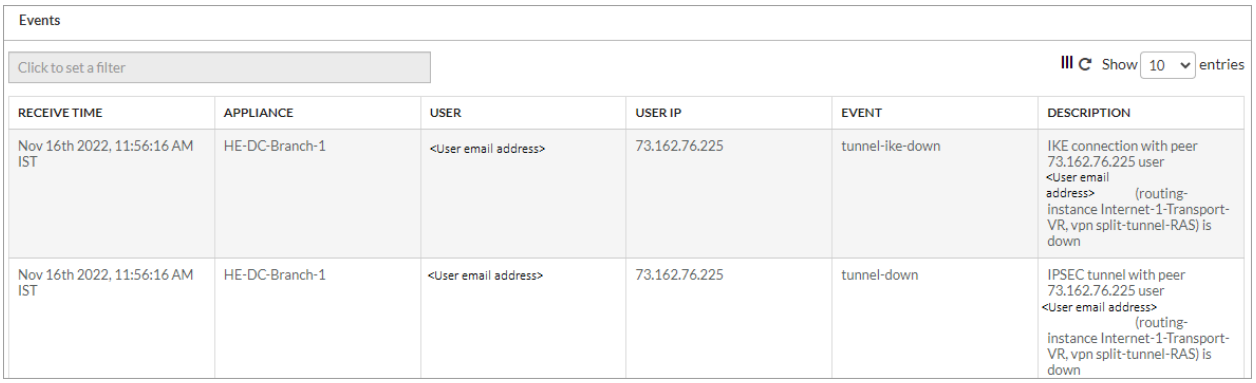
- Events per user



- Events per type



- Events, including reasons for authentication failures.



Events

Click to set a filter

Show 10 entries

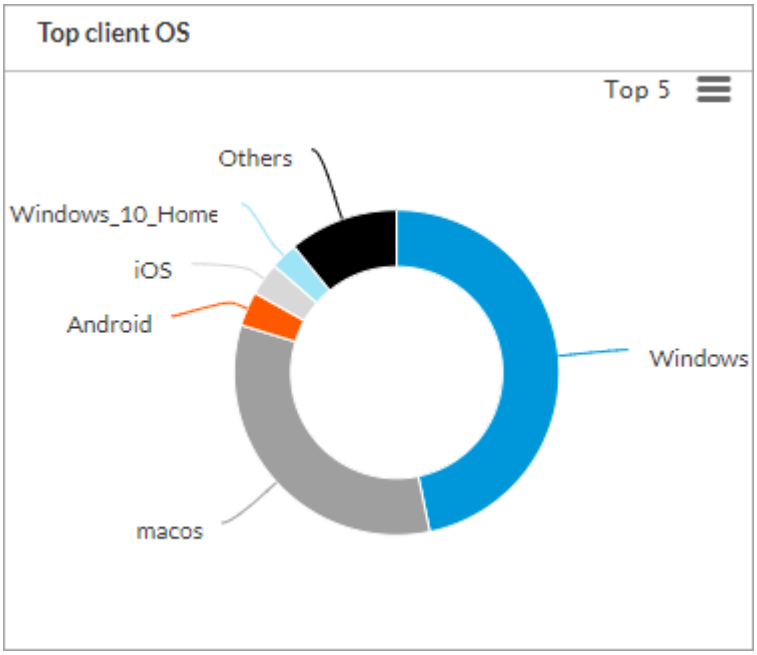
RECEIVE TIME	APPLIANCE	USER	USER IP	EVENT	DESCRIPTION
Nov 16th 2022, 11:56:16 AM IST	HE-DC-Branch-1	<User email address>	73.162.76.225	tunnel-ike-down	IKE connection with peer 73.162.76.225 user <User email address> (routing-instance Internet-1-Transport-VR, vpn split-tunnel-RAS) is down
Nov 16th 2022, 11:56:16 AM IST	HE-DC-Branch-1	<User email address>	73.162.76.225	tunnel-down	IPSEC tunnel with peer 73.162.76.225 user <User email address> (routing-instance Internet-1-Transport-VR, vpn split-tunnel-RAS) is down

Field	Description
Receive Time	Displays the time when the event occurred on the device.
Appliance	Displays the name of the device on which the event occurred.
User	Displays the username.
User IP	Displays the user's IP address.
Event	Displays the event type.
Description	Displays the event description.

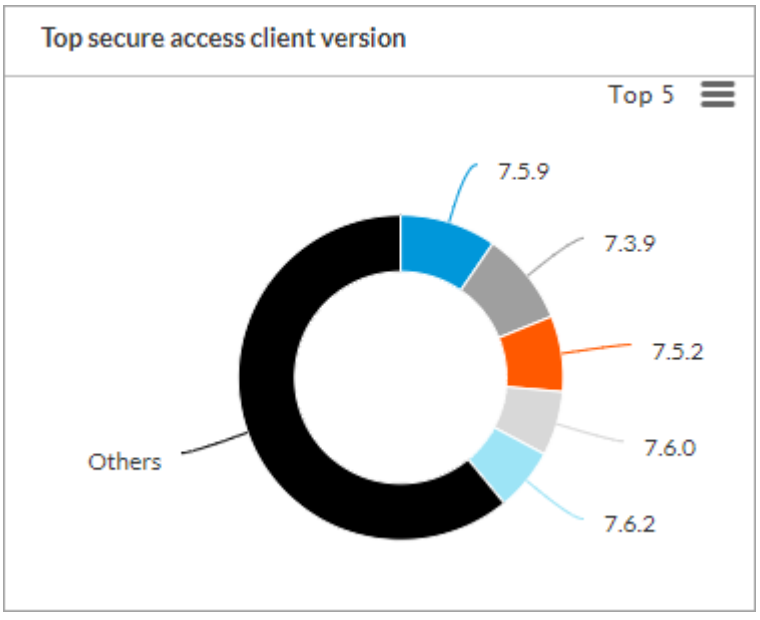
c. Select the Registry tab to view metrics about the top VSPA client operating systems (OSs), top VSPA client versions, VSPA gateways or VOS devices (appliances), and registration details. The Registry tab displays the

following panes:

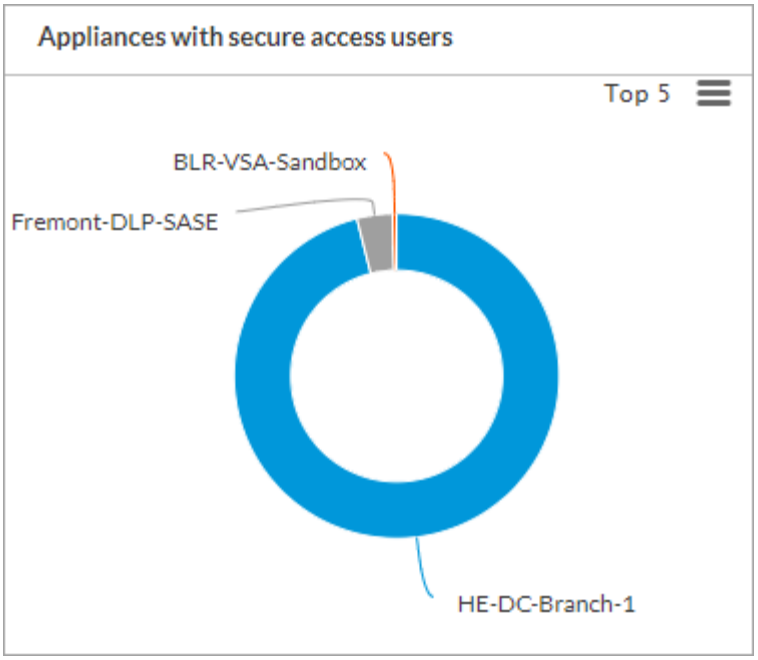
- Top client operating systems



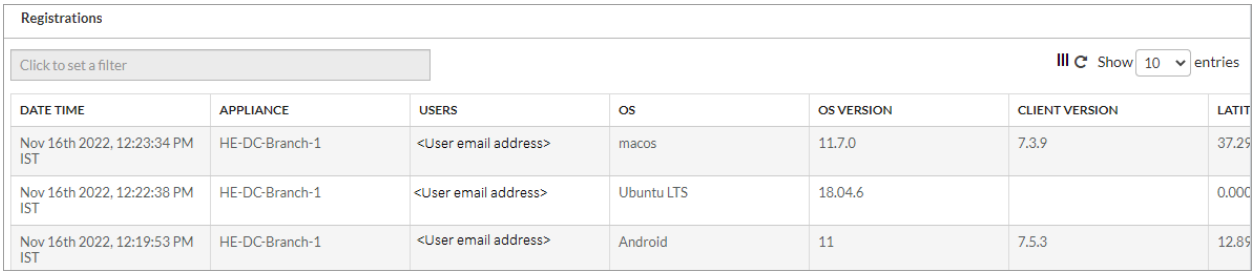
- Top secure access client versions



- VOS devices with secure access users



- Registration metrics



Field	Description
Date, Time	Displays the date and time of the registration.
Appliance	Displays the remote access gateway device name.
Users	Displays the username.
OS	Displays the OS running on the device on which the VSPA client is installed.
OS Version	Displays the OS version.
Client Version	Displays the VSPA client version.
Latitude, Longitude	Displays the latitude and longitude of the VSPA client.

Digital Experience Monitoring

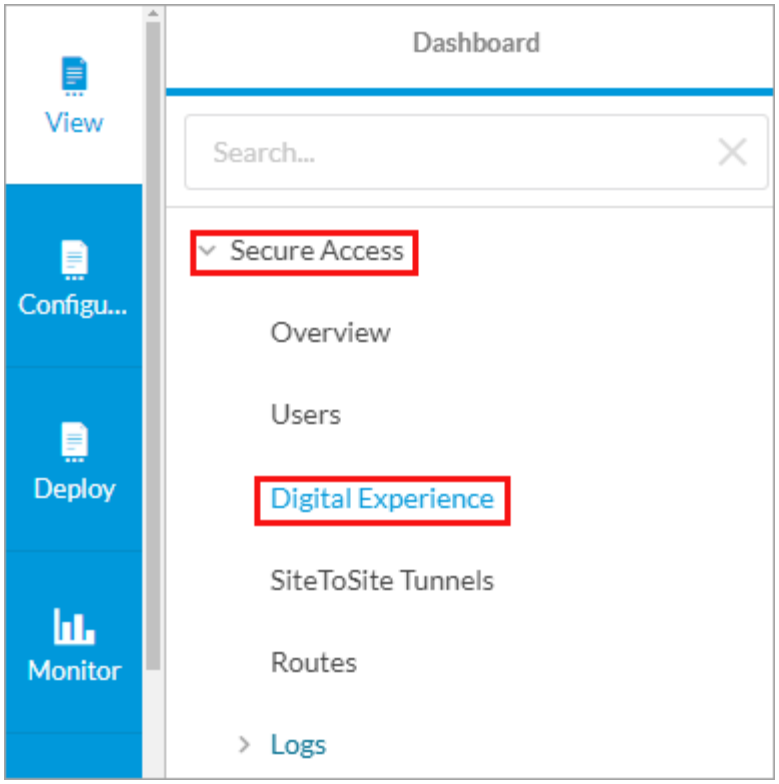
You can enable Digital Experience Monitoring (DEM) on remote secure access client devices to periodically monitor end-to-end network and application performance for the devices. When DEM is enabled on a device, secure access clients collect the following metrics for a user device:

- Device memory, CPU, disk utilization, and battery life
- WiFi signal strength, and transmit and receive bandwidth per SSID
- Local network segment metrics such as delay, jitter, and packet loss
- Internet segment metrics such as delay, jitter, and loss, both end to end and for each hop level
- Application metrics, including DNS lookup time, TCP and SSL connect times, HTTP latency, time to first and last byte, delay, jitter, and packet loss to application server.

The Secure Access Service Edge (SASE) client sends these metrics to Versa Analytics, which uses them to derive an experience rank value that ranges from 1 through 100. A value of 1 represents the best experience for the user's device and applications and a value of 100 represents the worst experience. Versa Analytics also provides in-depth information about the experience at the tenant, gateway, device, and application levels.

The Secure Access Digital Experience dashboard displays information about the end-to-end network and application experience for each user device.

To view the Secure Access Digital Experience dashboard, select View > Secure Access > Digital Experience.

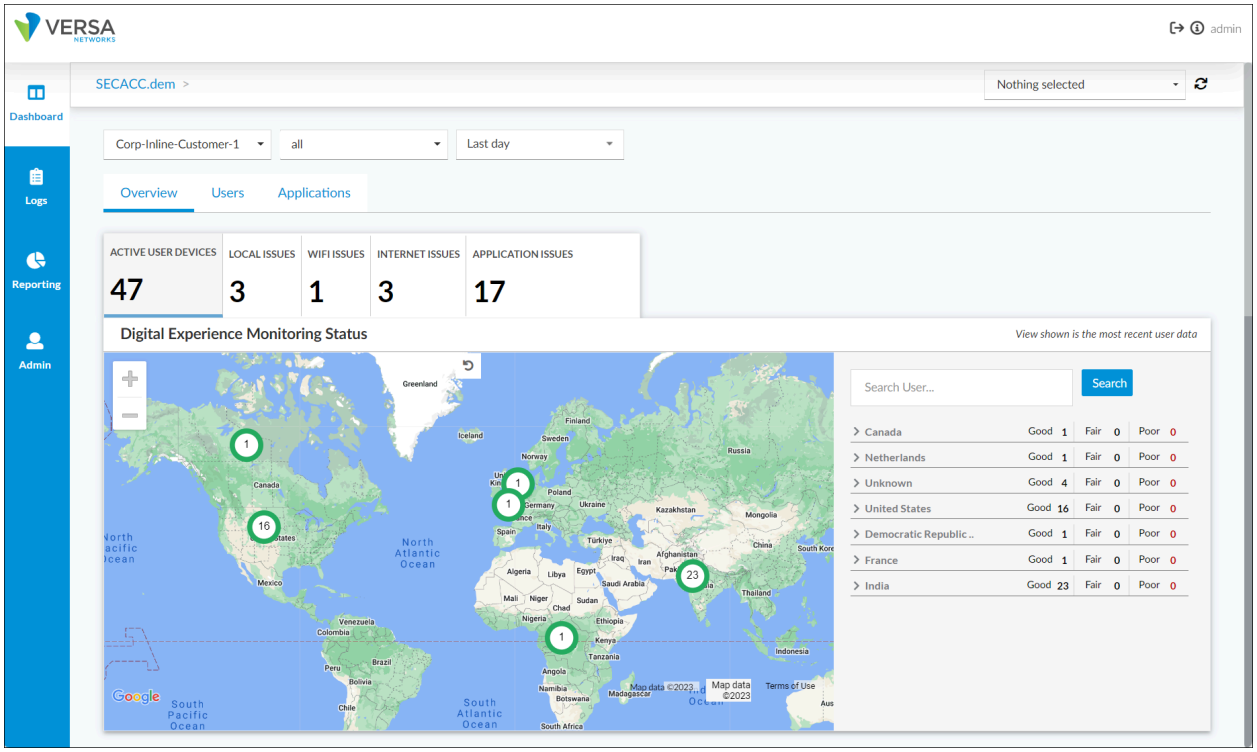


The Secure Access Digital Experience dashboard displays the following tabs in the horizontal menu bar:

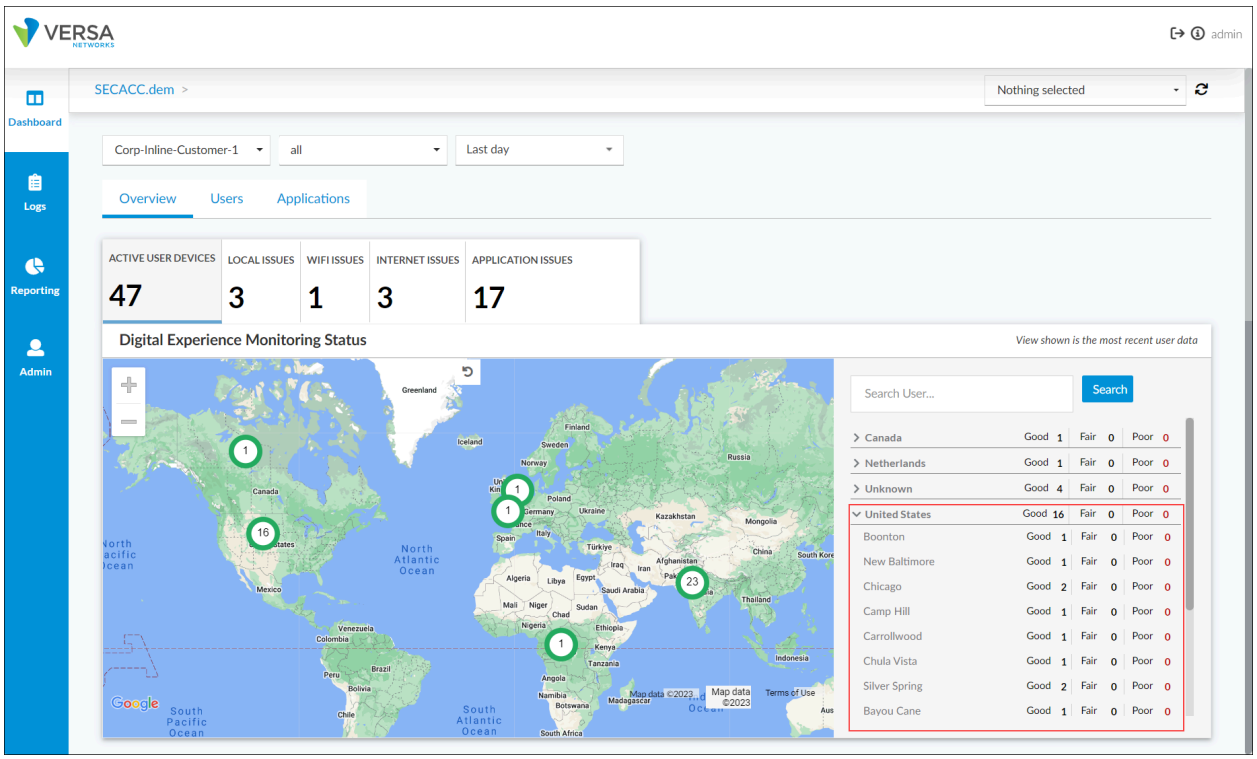
- Overview
- Users
- Applications

Overview Tab

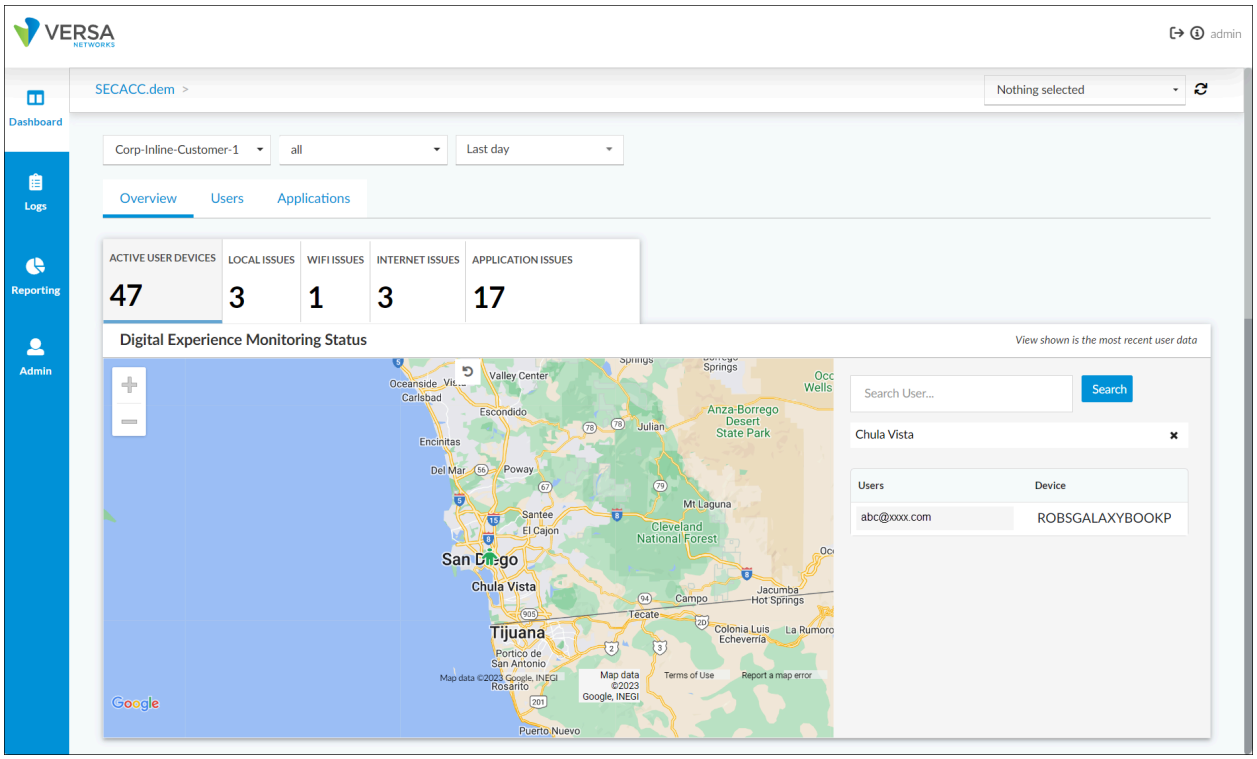
The Overview tab displays DEM status at the tenant level. For the tenants, user devices are grouped geographically map by country. The screen displays the number of user devices per country and city and the performance statistics for each location (good, fair, or poor).



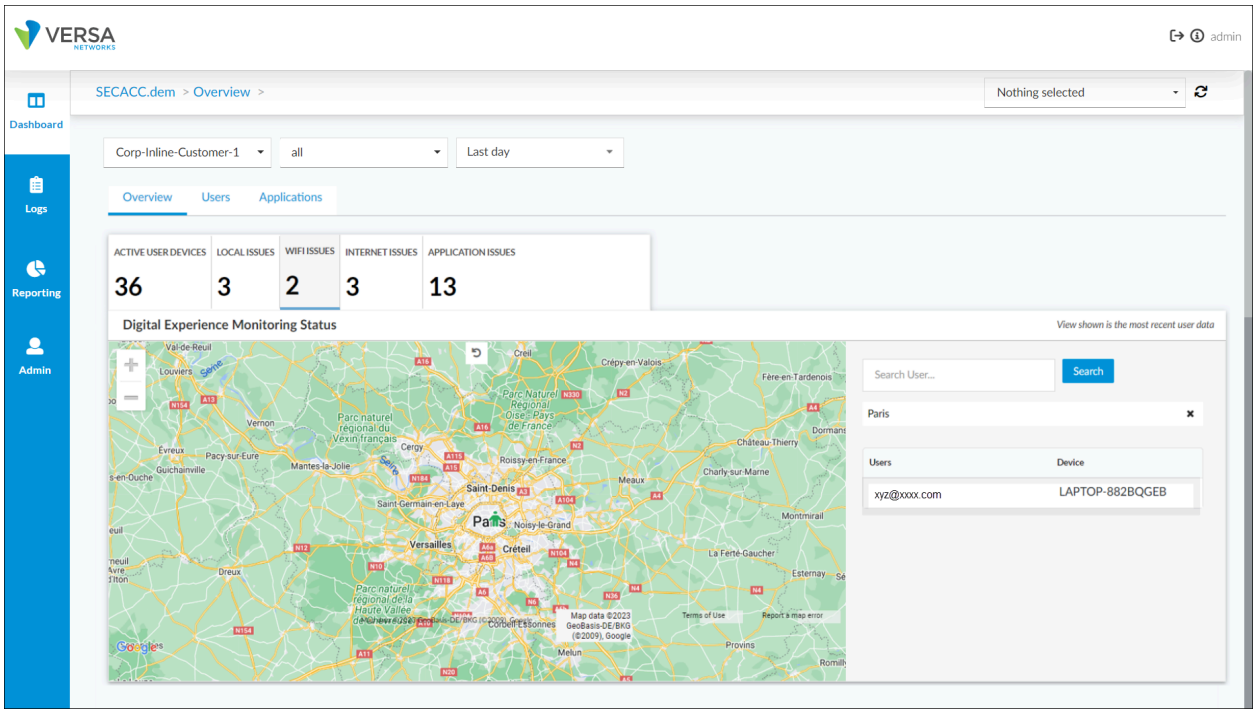
To view user devices by city, select a country in the table to the right of the map.



To view the active user devices in a city, select the city in the table. The following screenshot shows the city of Chula Vista selected on the map. The active users are listed to the right of the map.

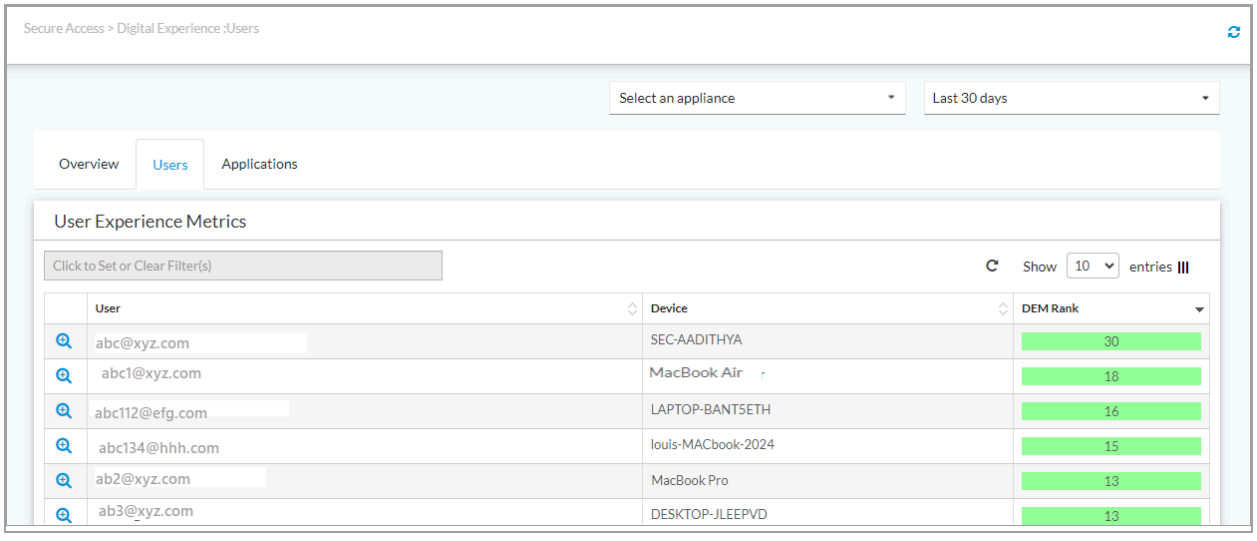


To view local, WiFi, internet, and application issues for a tenant, select the item in the horizontal menu bar above the map. Categorizing issues can help tenant operators quickly troubleshoot issues.



Users Tab

Select the Users tab to display the User Experience Metrics table. The table includes user information for the tenant and time period shown in the first and third drop-down menus at the top of the main pane.

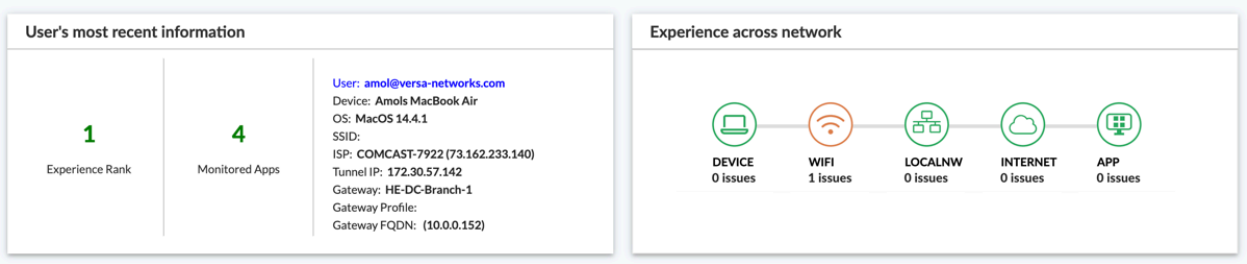


To search for a specific user, use the Set Filters box.

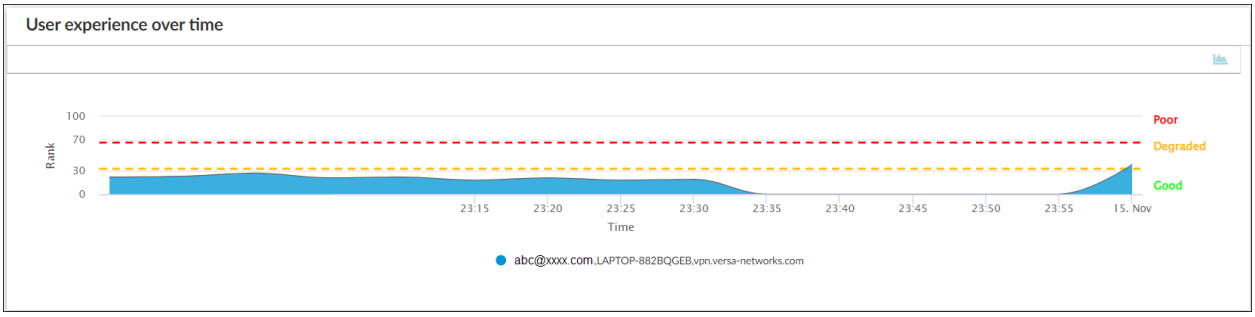
To display a detailed view for the user's device experience, select the Zoom icon to the left of a row.

The screen displays the following charts and tables:

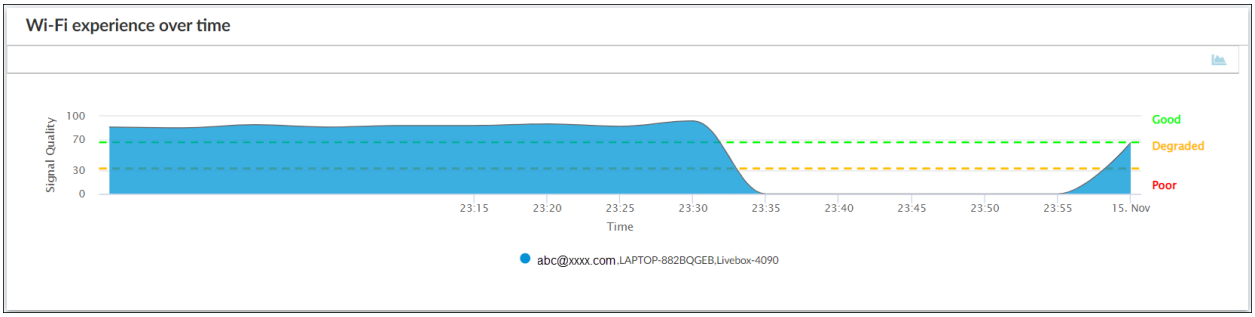
- User's Most Recent Information
- Experience Across Network



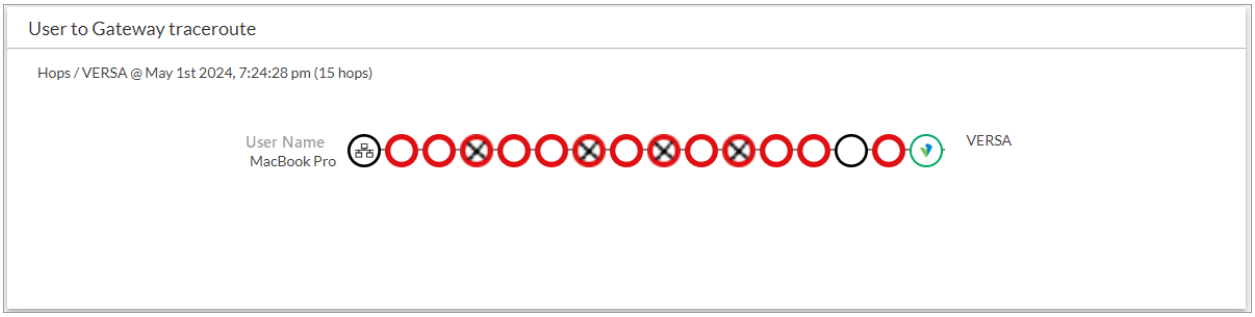
- User Experience Over Time—Performance of user's device over time. If the rank value is in the degraded or poor range, it is likely that the user's device experienced local or network issues.



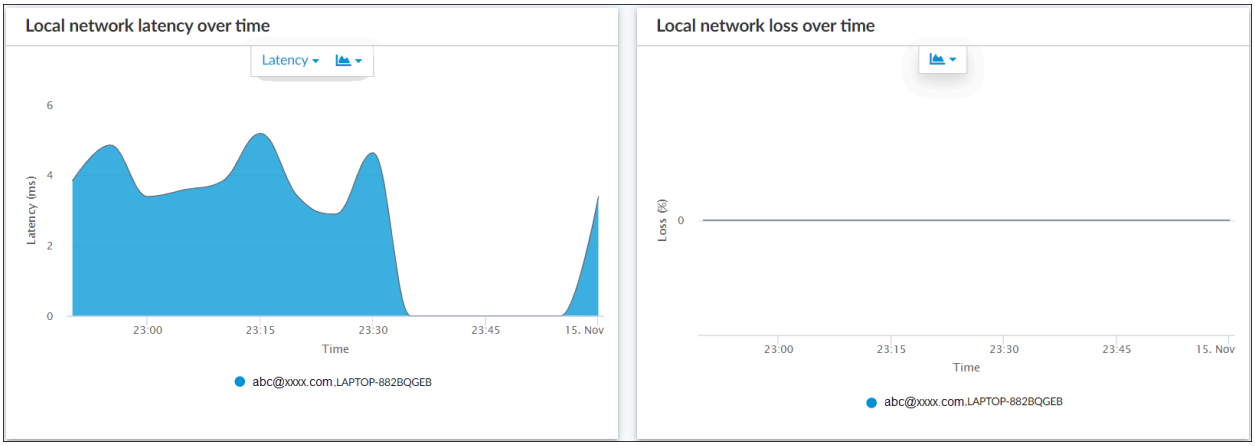
- WiFi Experience Over Time—Signal strength per WiFi SSID over time. A signal quality value of 0 through 33 is considered poor, 34 through 66 is degraded, and 67 through100 is good.



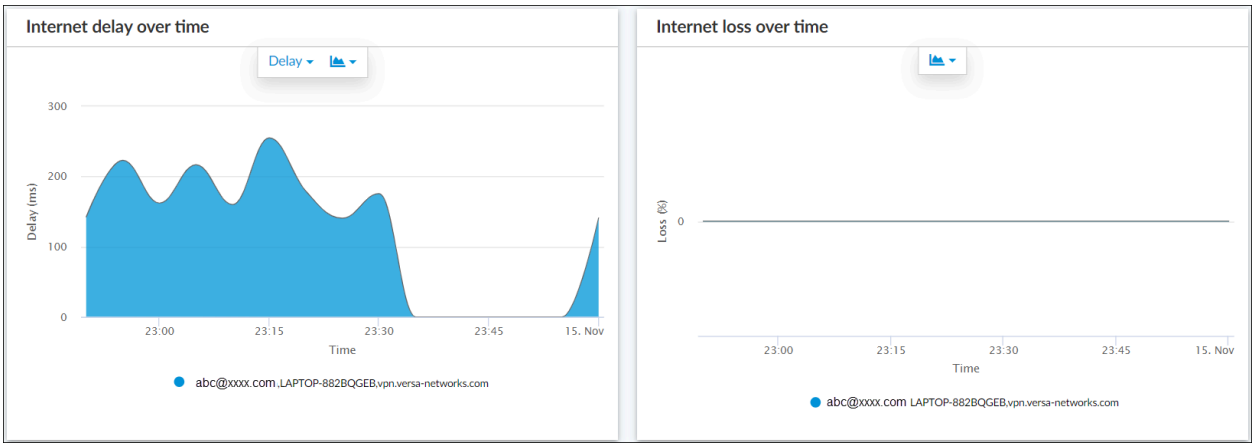
- User to Gateway Traceroute—Last known traceroute to the SASE gateway, and the reachability to the gateway through various hops.



- Local Network Latency Over Time—Local network latency and jitter metrics over time. Use this information to help determine whether there are issues connecting to the next-hop gateway.
- Local Network Loss Over Time—Local network loss metrics over time.

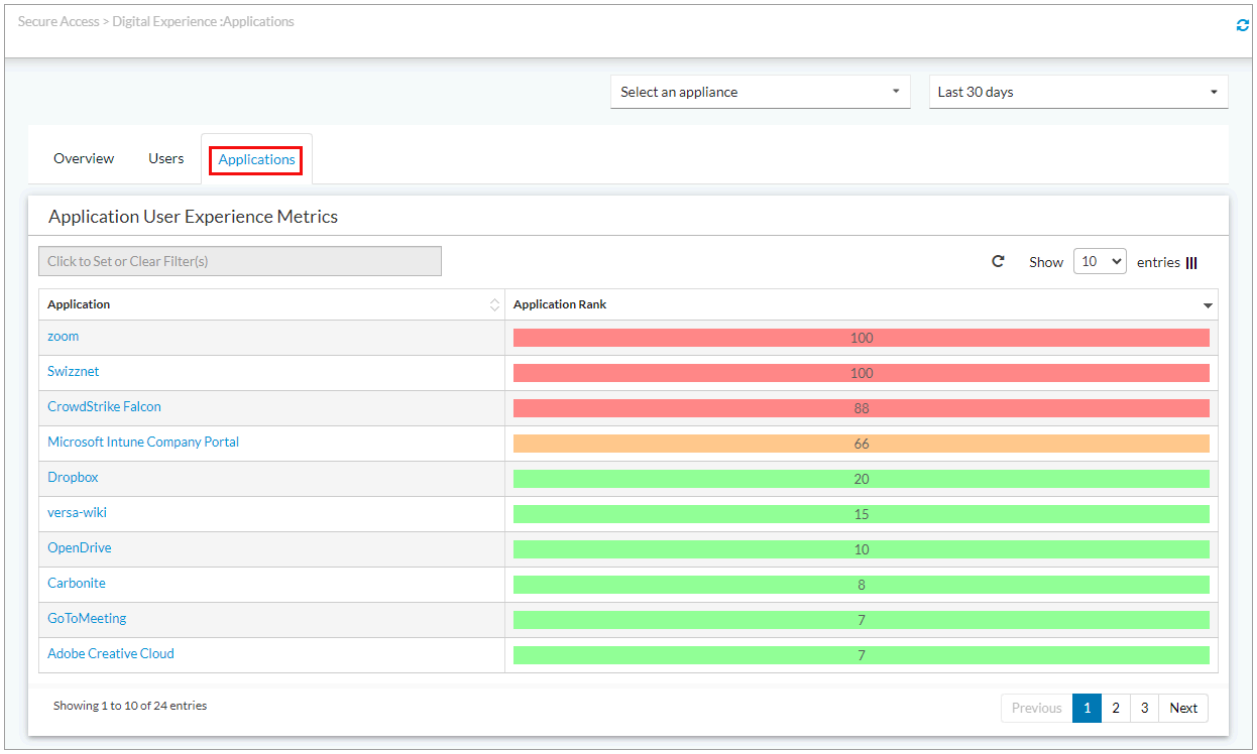


- Internet Delay Over Time—Internet delay and jitter metrics over time. Use this information to help determine whether there are network issues in the internet segment connecting to the SASE gateway.
- Internet Loss Over Time—Internet loss metrics over time.
- CPU Utilization—Device CPU status over time.
- Memory Utilization—Device memory utilization over time.
- Battery Status—Device battery status over time.
- Disk Utilization—Device disk utilization over time.



Applications Tab

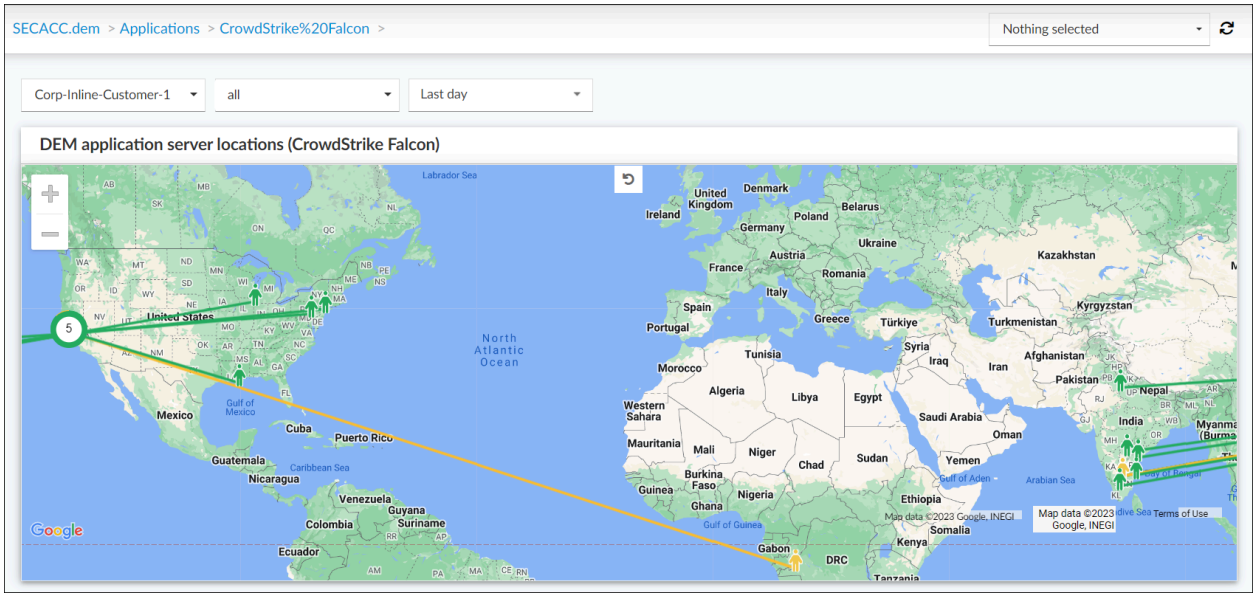
To view the list of applications and overall application performance for a tenant, select the Applications tab to display the Application User Experience Metrics table. The table includes application information and application rank for the tenant.



To search for a specific application, use the Set Filters box.

To view a map of the application server locations and the application performance for the users connected to the servers, select an application in the table.

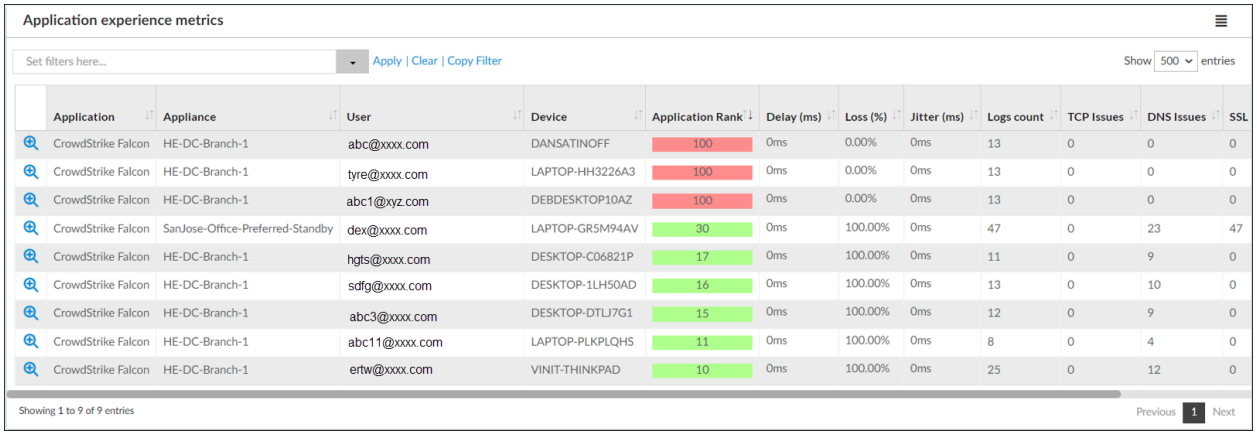
The following example shows the locations of the application servers accessed by users of the CrowdStrike Falcon application.



To view the users connected to an application server, click the application server location on the map. The following example displays the users connected to an application server. The colors of the users connected to an application server represent the following user experience levels:

- Green—Good
- Yellow—Degraded
- Red—Poor

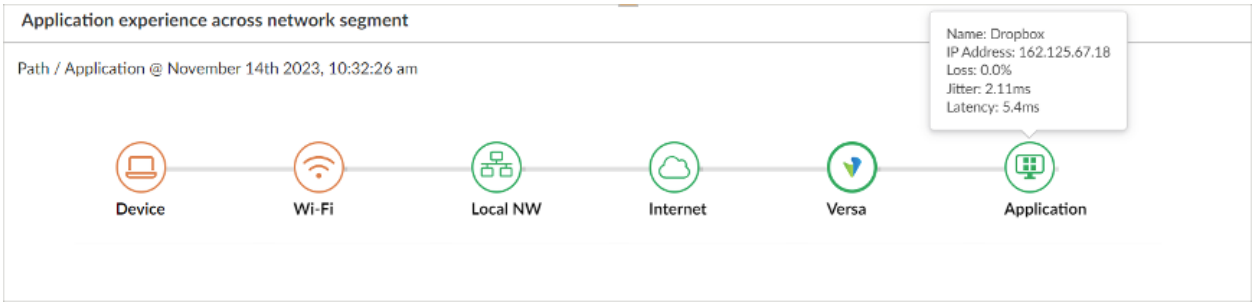
The Application Experience Metrics table displays the application rank and related metrics for the selected application for each user device.



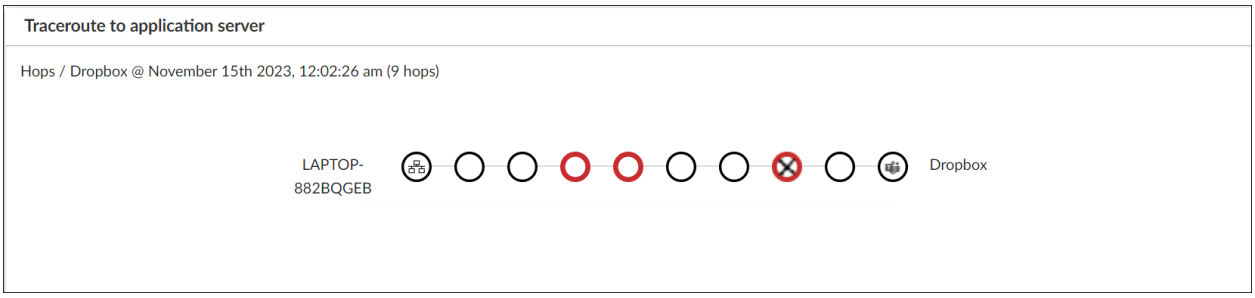
To display application performance details for the user, device, and application listed in the row, select the Zoom icon to the left of a row.

You can view the following charts and tables:

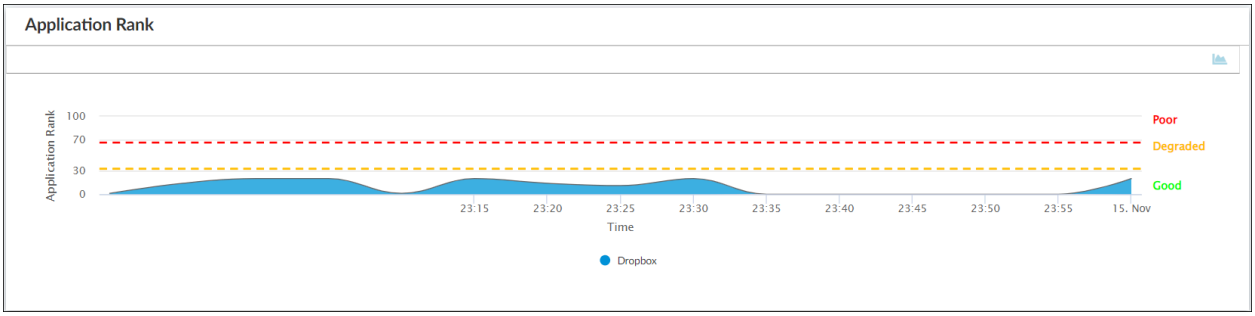
- Application Experience Across Network Segment—Last reported performance at different points in the network.



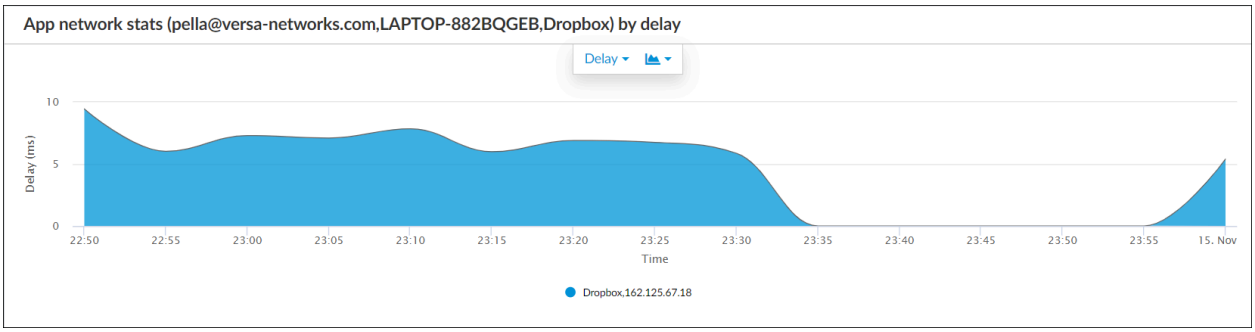
- Application Traceroute—Last known traceroute results for an application server through various network hops.



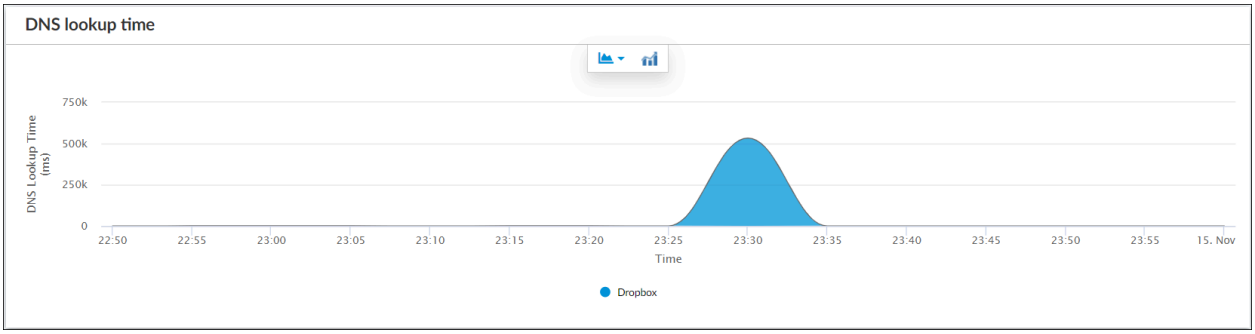
- Application Rank—User device's application performance over time for a specific application.



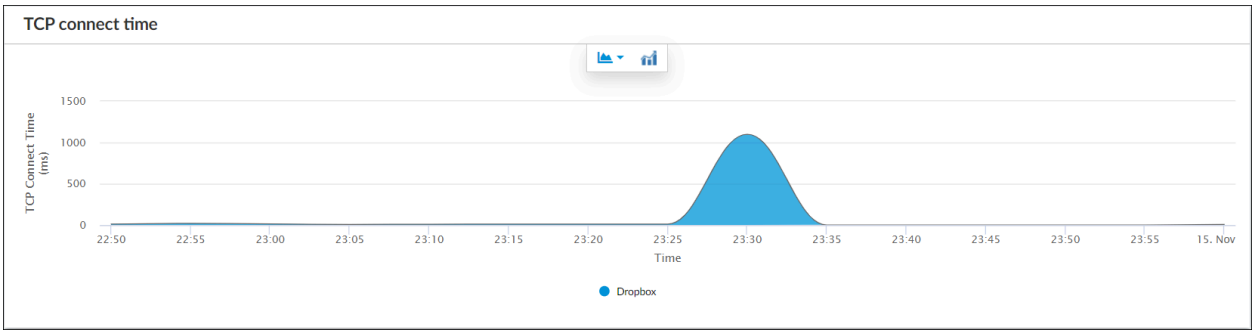
- Application Network Statistics—User device's application network performance metrics for delay, jitter and loss, over time for a specific application.



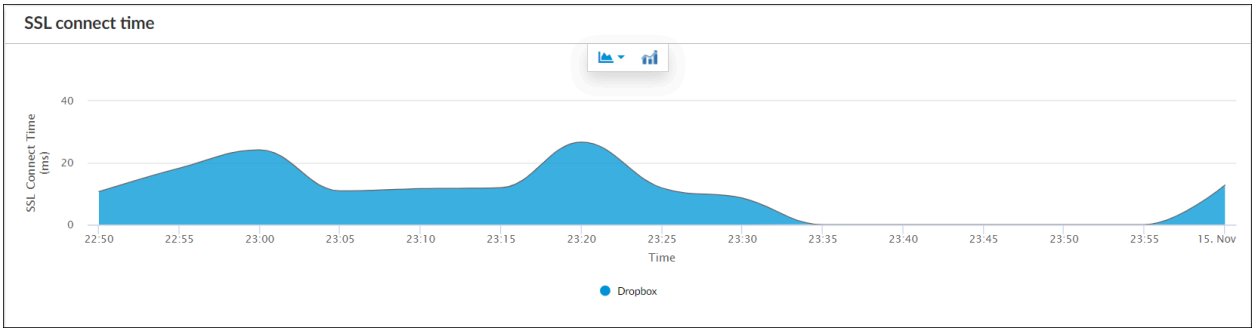
- DNS Lookup Time—Time taken to perform DNS operations over time for a specific application.



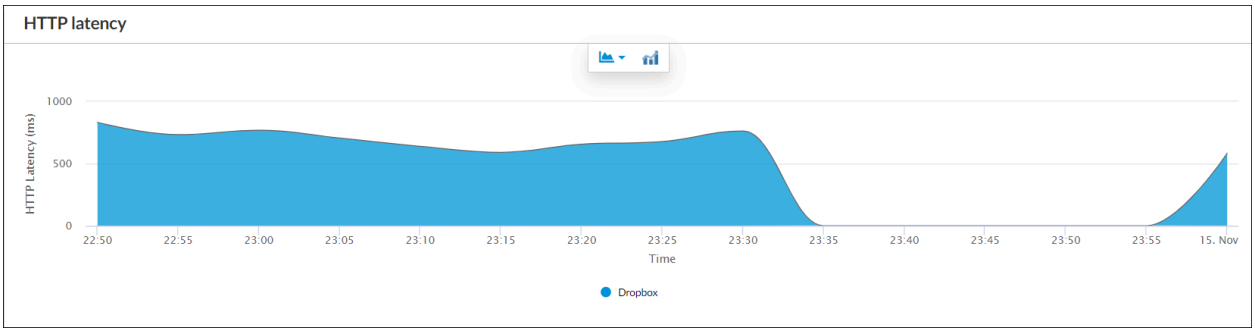
- TCP Connect Time—Time taken to establish TCP connectivity over time for a specific application.



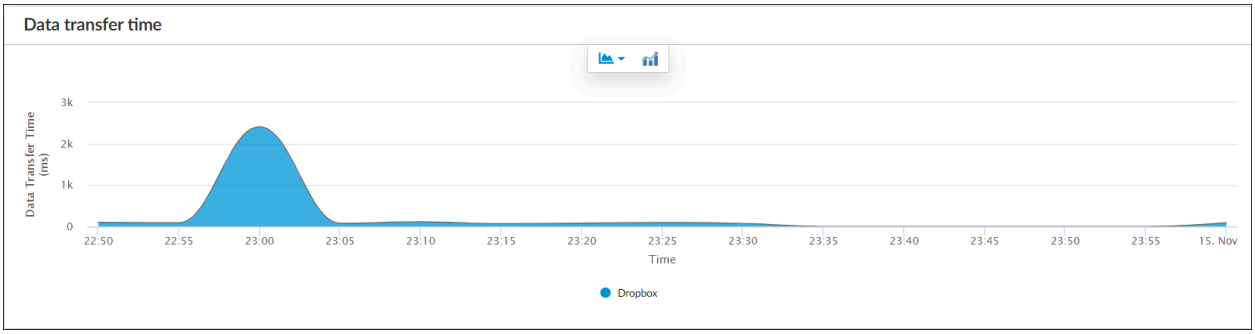
- SSL Connect Time—Time taken to perform SSL handshake over time for a specific application.



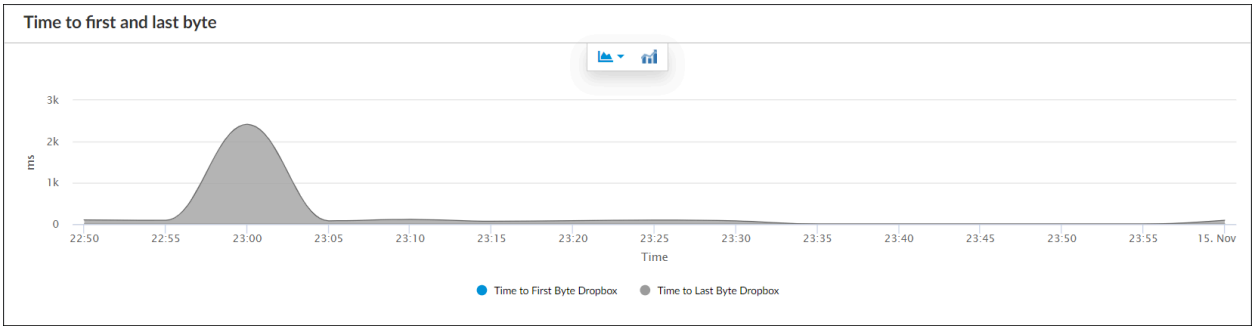
- HTTP Latency—Time taken to perform HTTP operations over time for a specific application.



- Data Transfer Time—Time taken to transfer data from the client to the server over time for a specific application.



- Time to First and Last Byte—Time time taken to transfer first and last byte over time for a specific application.

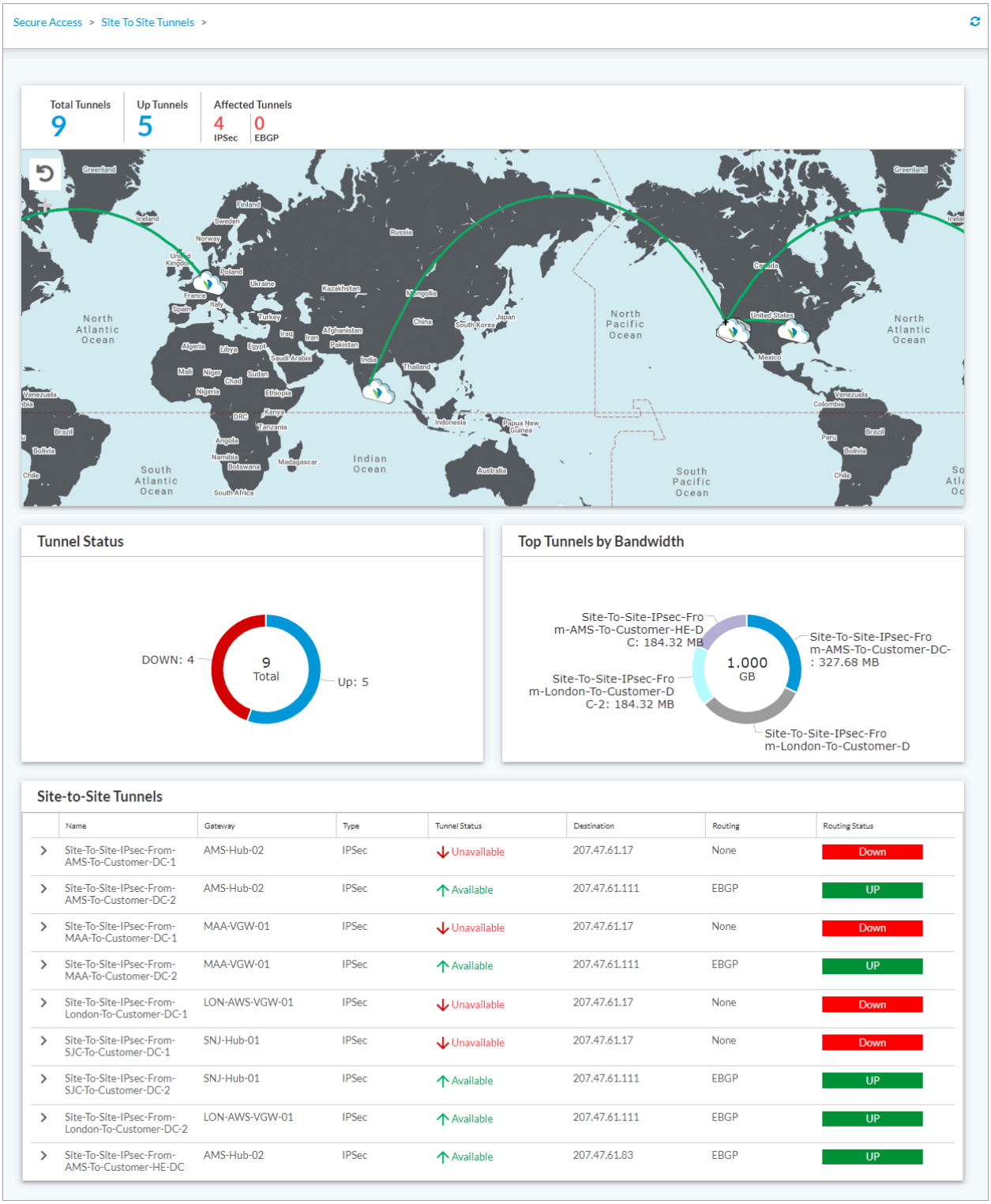


Site-to-Site Tunnels View

Site-to-Site Tunnels view shows statistics about a tenant's site-to-site tunnels, including tunnel status and top tunnels by bandwidth.

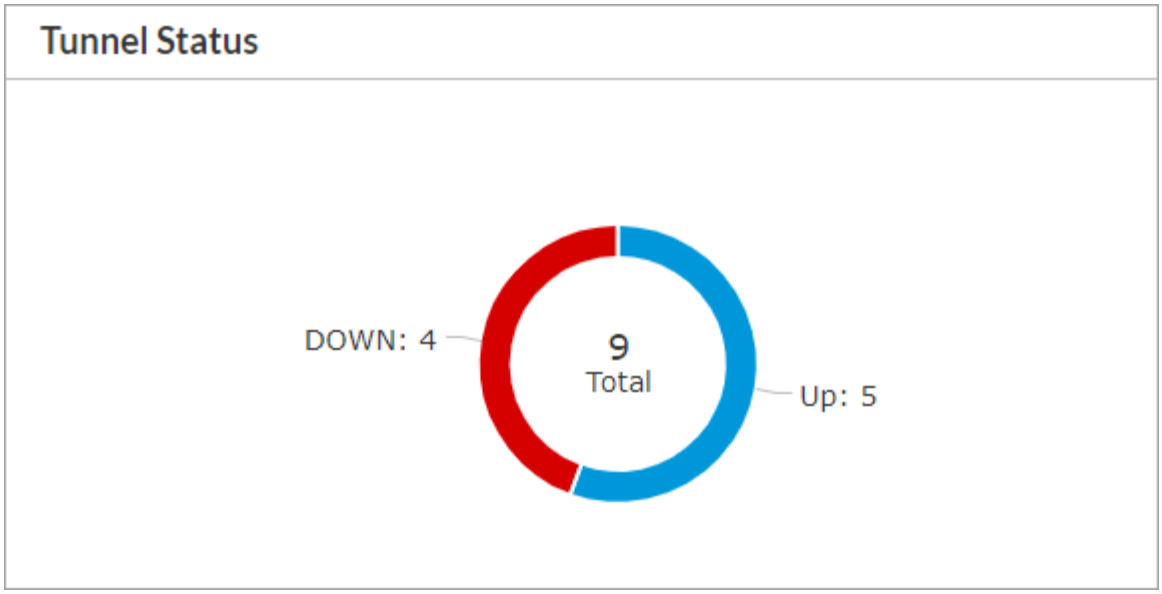
To display VSPA site-to-site tunnel information for a tenant:

1. Select View in the left navigation pane.
2. Select Secure Access > Site-to-Site Tunnels. The Site-to-Site Tunnels screen displays.

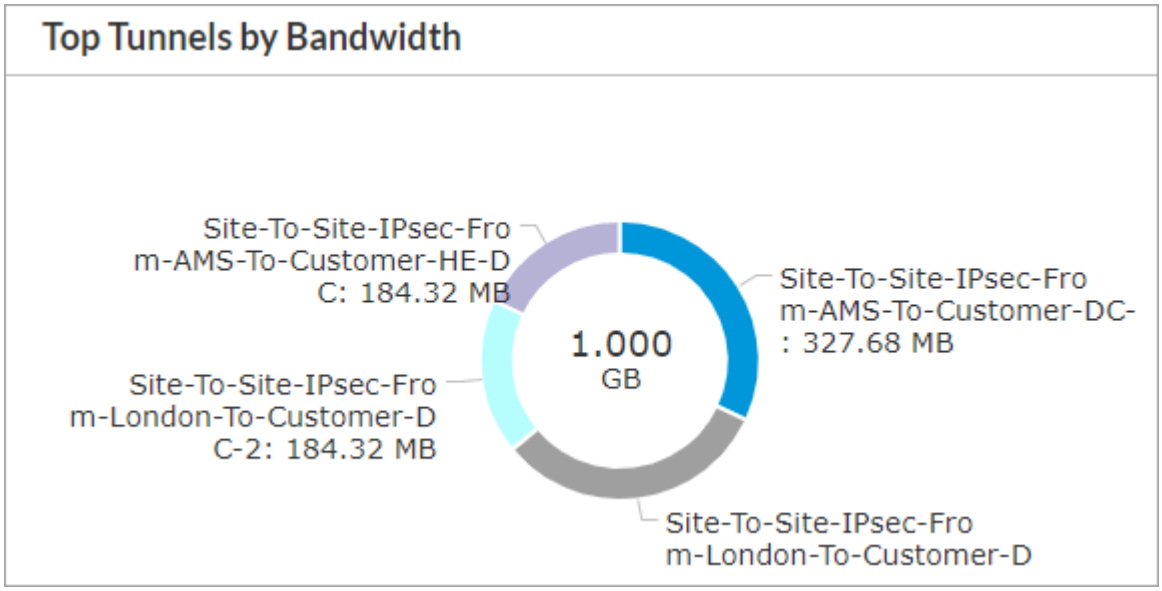


3. The Site-to-Site Tunnels screen displays the following panes:

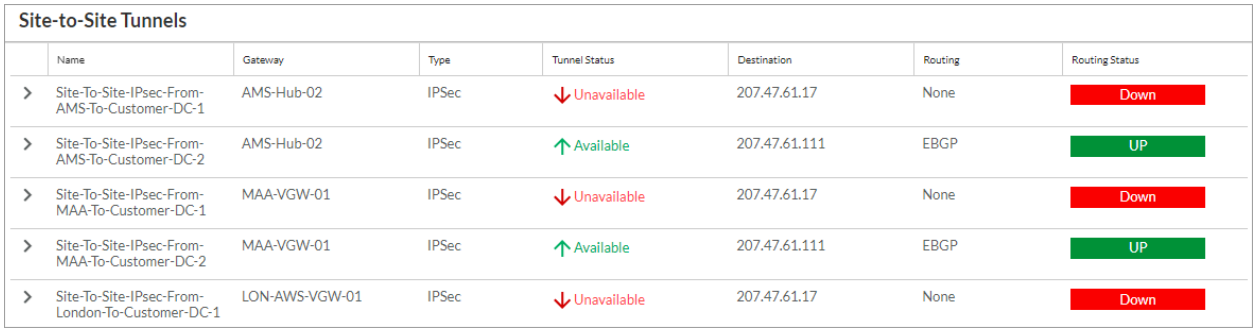
   - Tunnel status



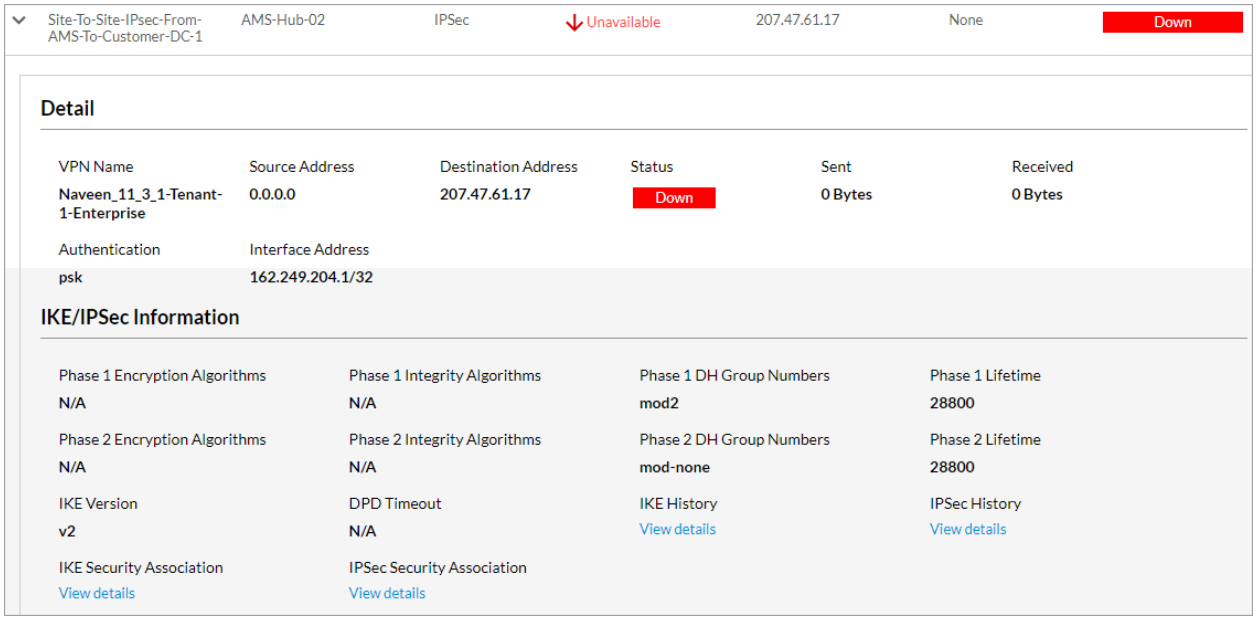
- Top tunnels by bandwidth



- Site-to-site tunnel details displays tunnel name, gateway connected to, type of tunnel, status, destination IP address, type of routin, and routing status



- Click the down arrow to show details about the tunnel

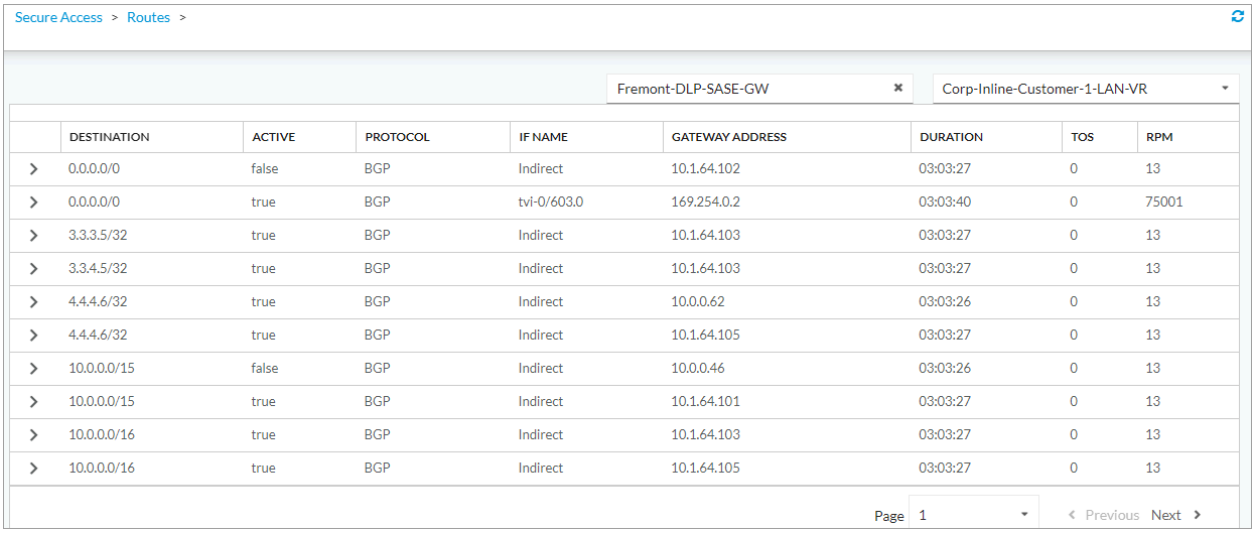


Routes View

Routes view shows statistics about the SASE gateway routes that are used by the tenant for secure access connection.

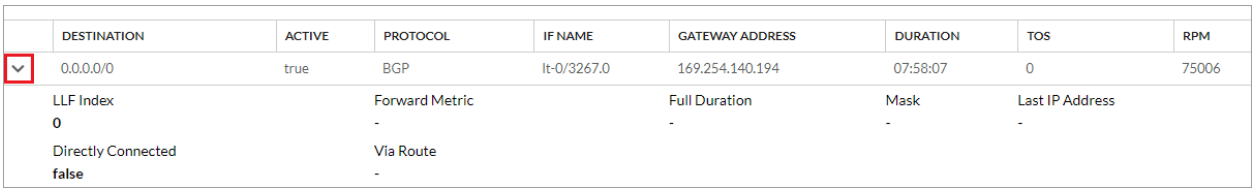
To display SASE gateway routes information for a tenant:

1. Select View in the left navigation pane.
2. Select Secure Access > Routes. The Routes screen displays.



Field	Description
Destination	Displays the destination IP address of the SASE gateway route.
Active	Displays if the gateway is active.
Protocol	Displays the protocol used by the route.
If Name	Displays the interface used by the route.
Gateway Address	Displays the SASE gateway IP address of the route.
Duration	Displays the duration for which the route has been active.
TOS	Displays the type of service (TOS) bits in the IPv4 header.
RPM	Displays the real-time performance monitoring details for the route.

3. Click the down arrow to display for details for the route.

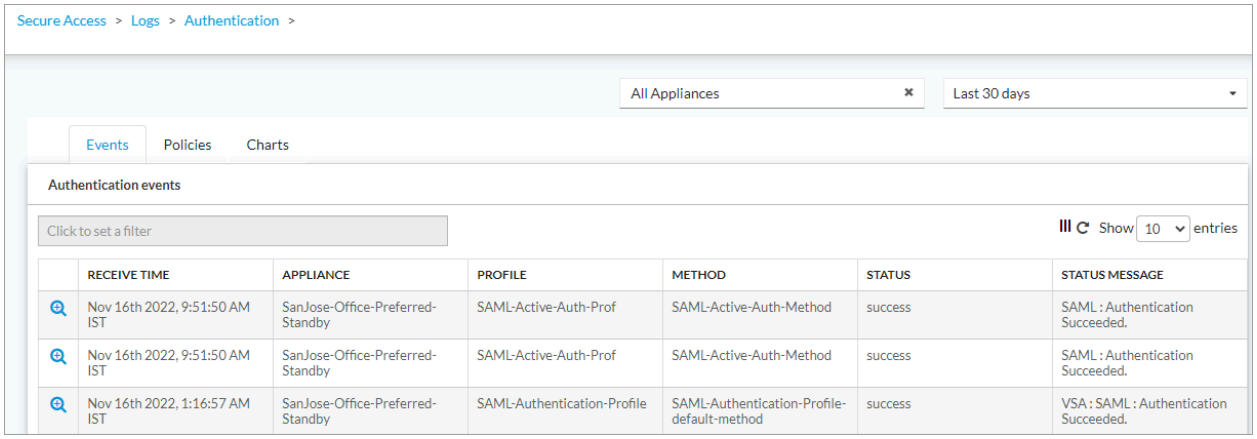


Authentication Logs View

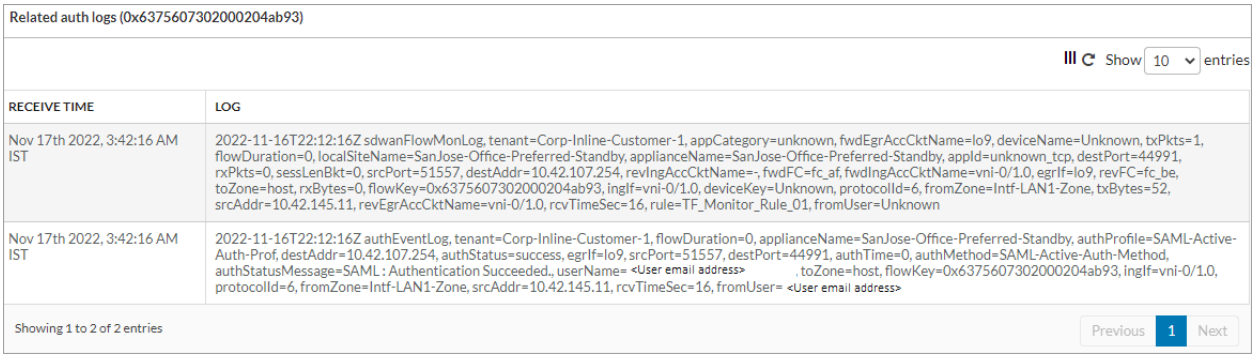
Authentication logs view shows the authentication events and policies, and top authentication statistics for a tenant.

To display secure access authentication logs:

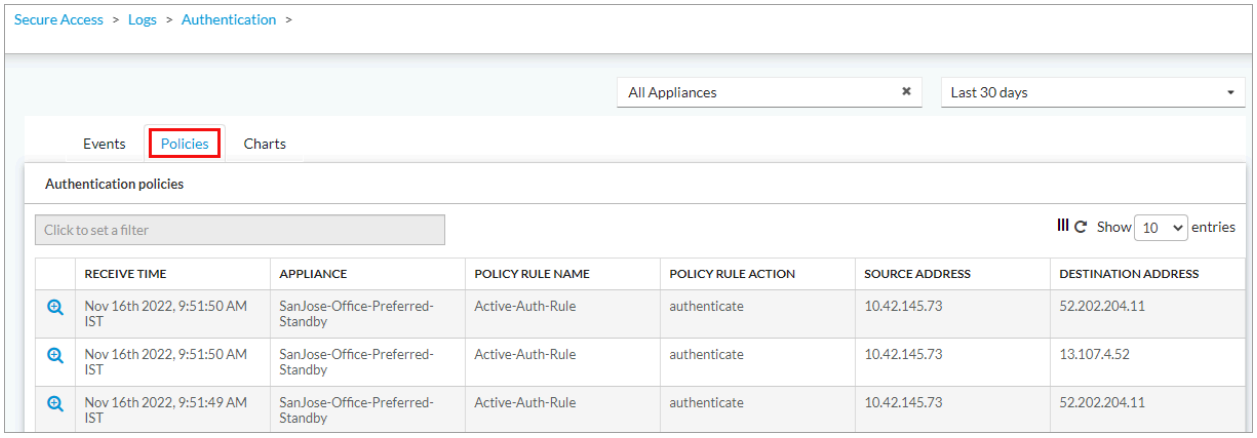
1. Select View in the left navigation pane.
2. Select Secure Access > Logs > Authentication. The Events tab displays by default and shows secure access authentication event logs.



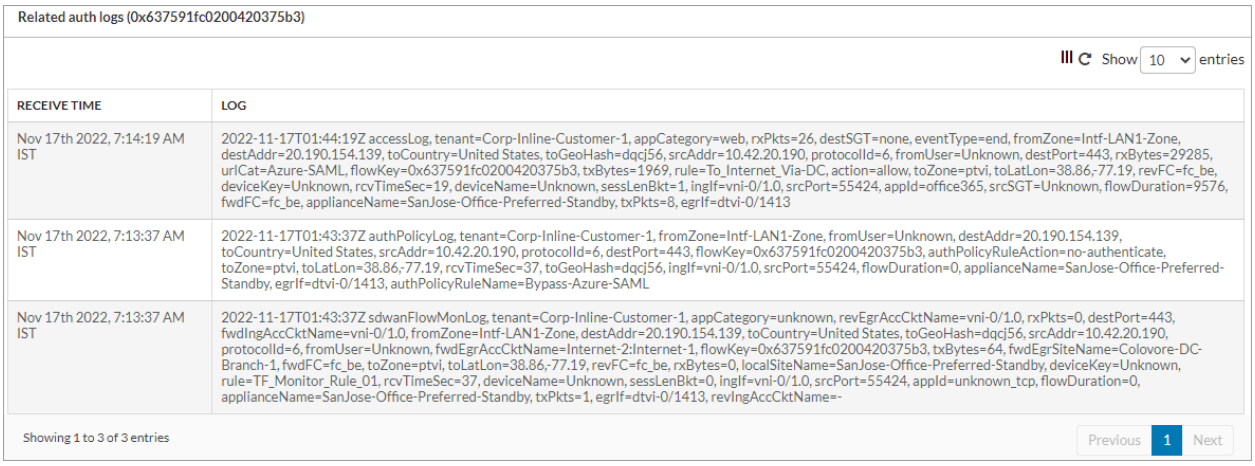
a. Click the Zoom icon to view more information about an authentication event.



3. Select the Policies tab to view details of VSPA authentication policies used by the tenant.

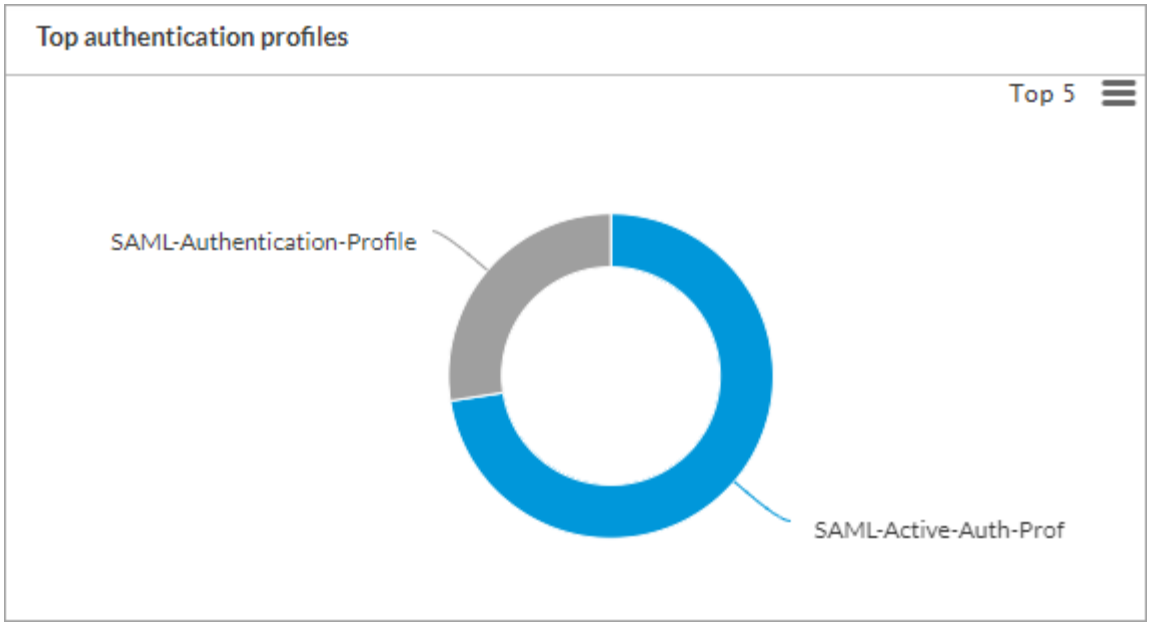


a. Click the Zoom icon to view more information about an authentication policy.

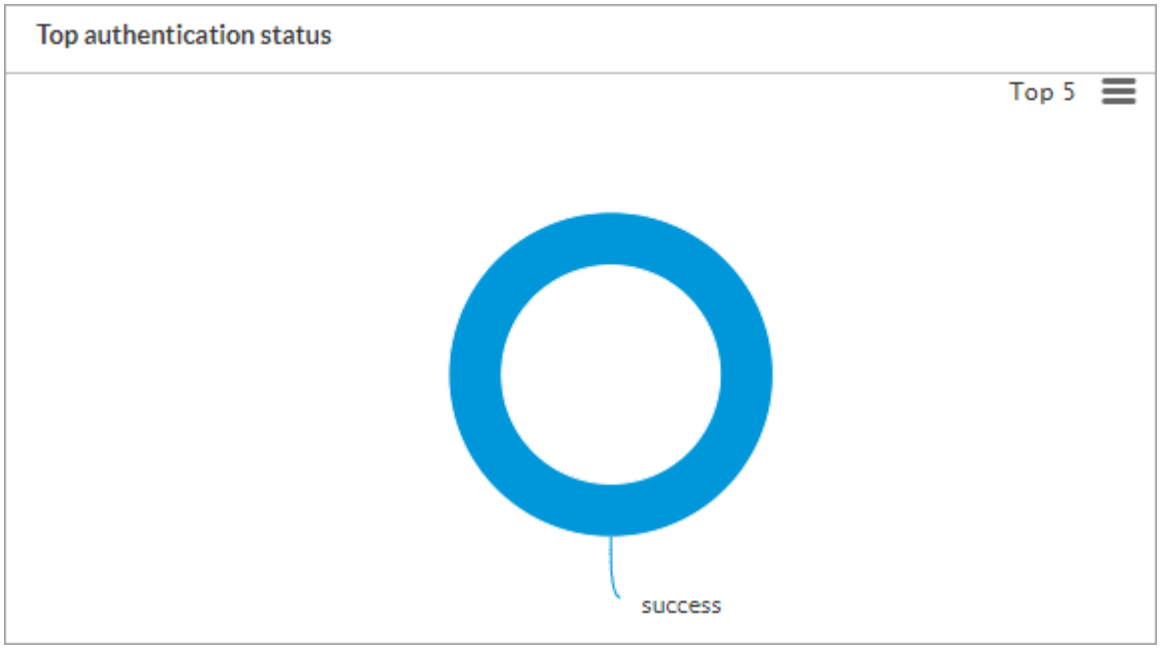


4. Select the Charts tab to view metrics about the top authentication profiles, authentication status, rules, and rule actions. The Charts tab displays the following panes:

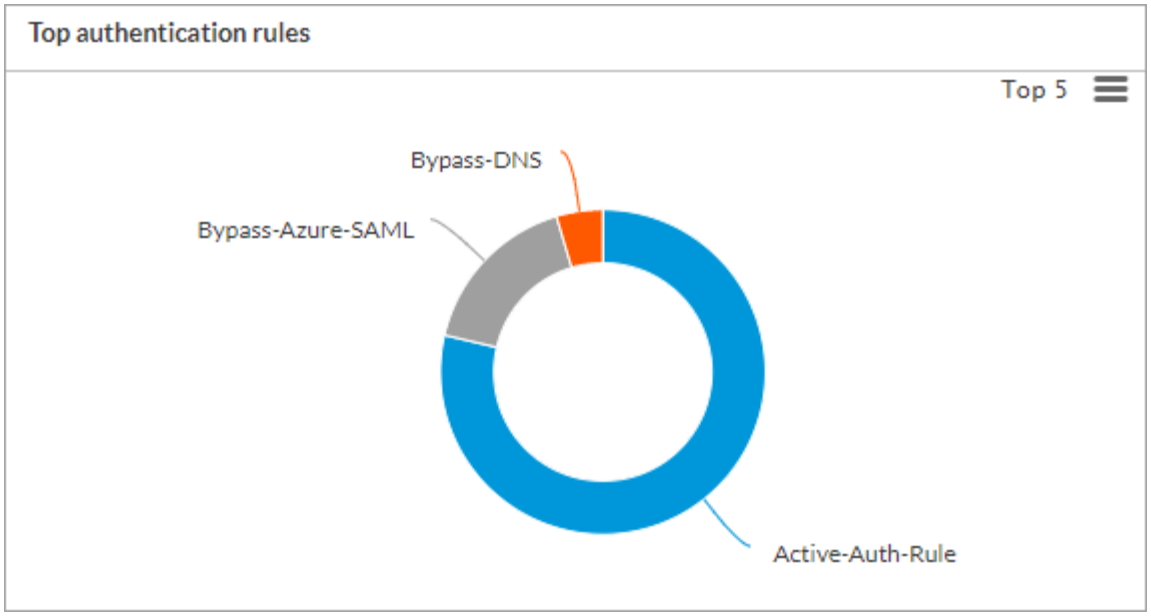
   - Top authentication profiles



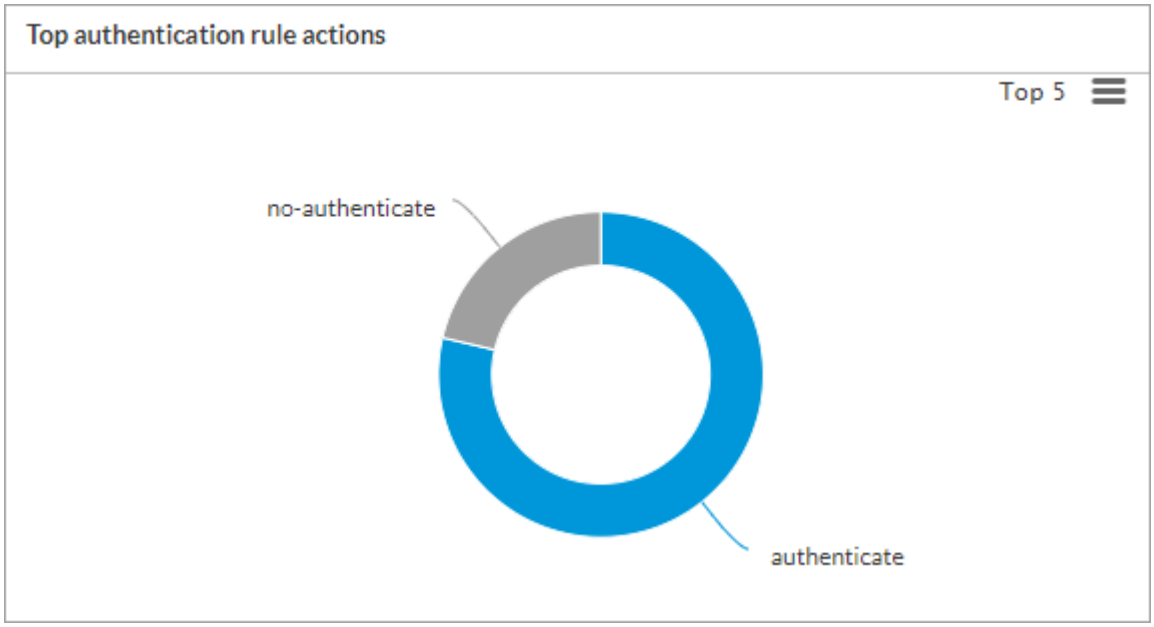
- Top authentication status



- Top authentication rules



- Top authentication rule actions



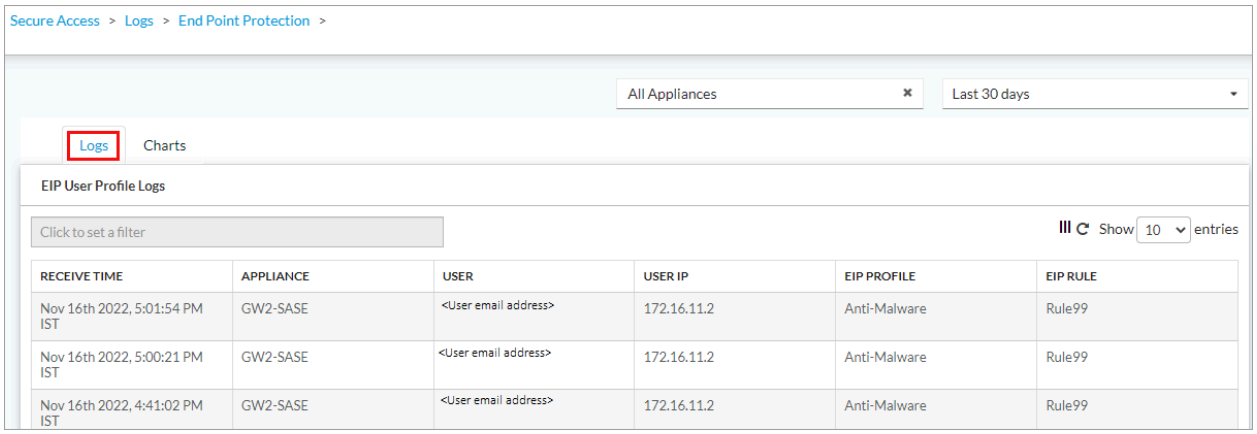
EIP Logs View

Endpoint information profile (EIP) logs view shows the authentication logs for EIP user profiles and top statistics for users, IP addresses, EIP profiles, and rules.

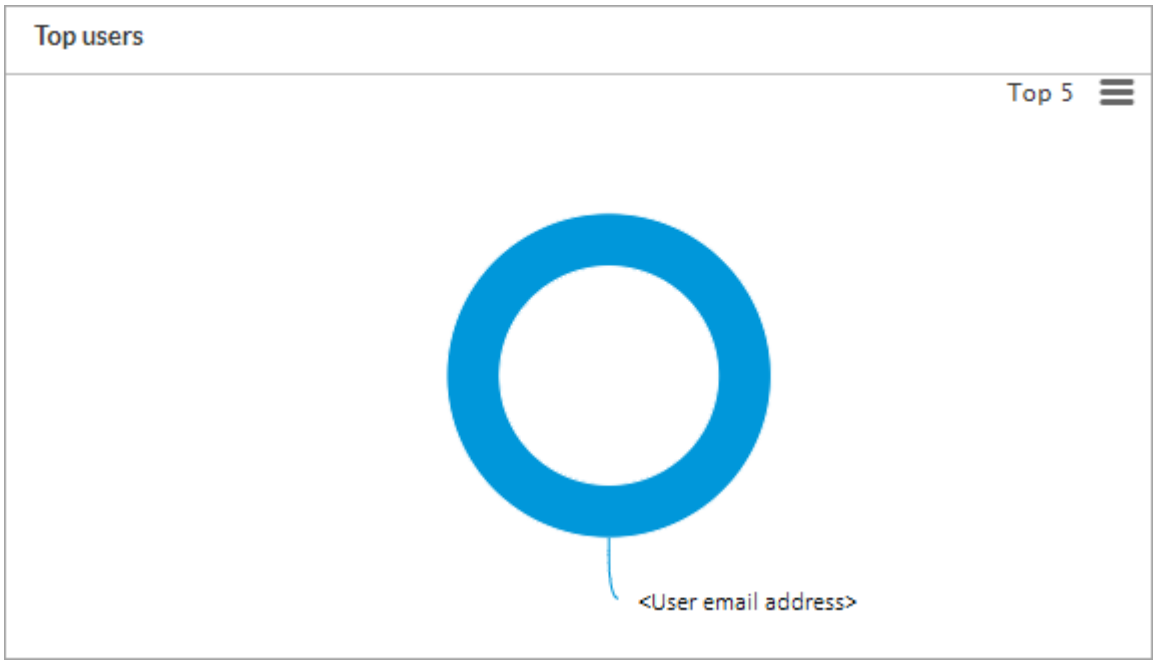
To display EIP authentication logs:

1. Select View in the left navigation pane.

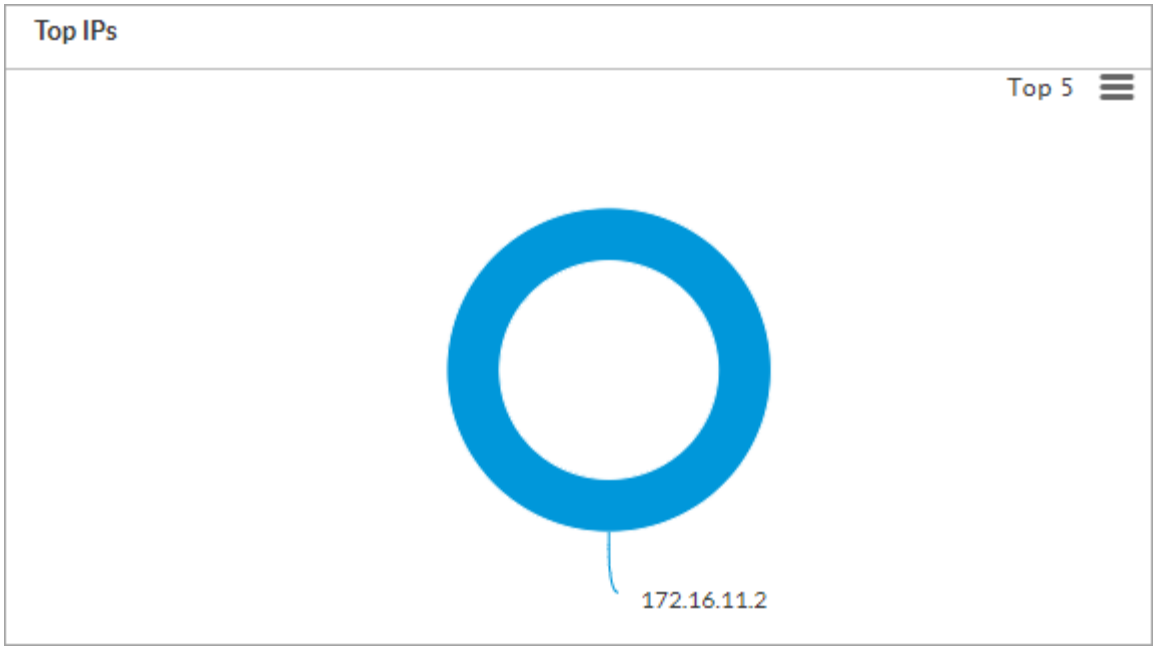
2. Select Secure Access > Logs > Endpoint Information Profiles. The Logs tab displays by default and shows EIP user profile logs.



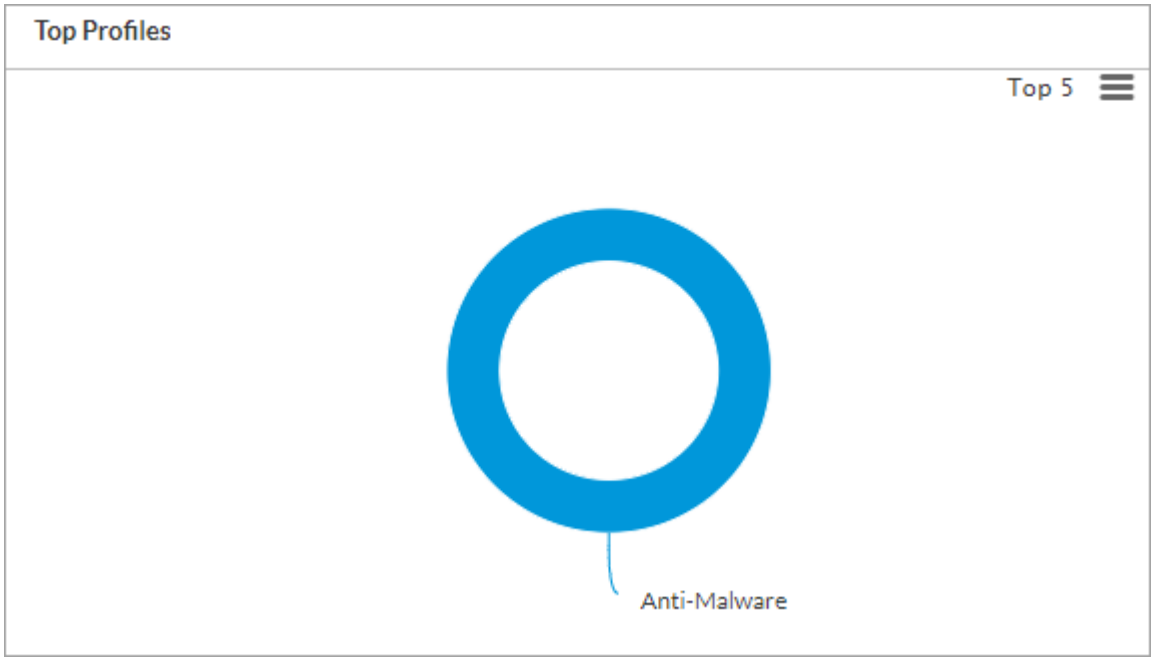
3. Select the Charts tab to view statistics for top EIP users, IP addresses, profiles, and rules. The Charts tab displays the following panes:
   - Top users



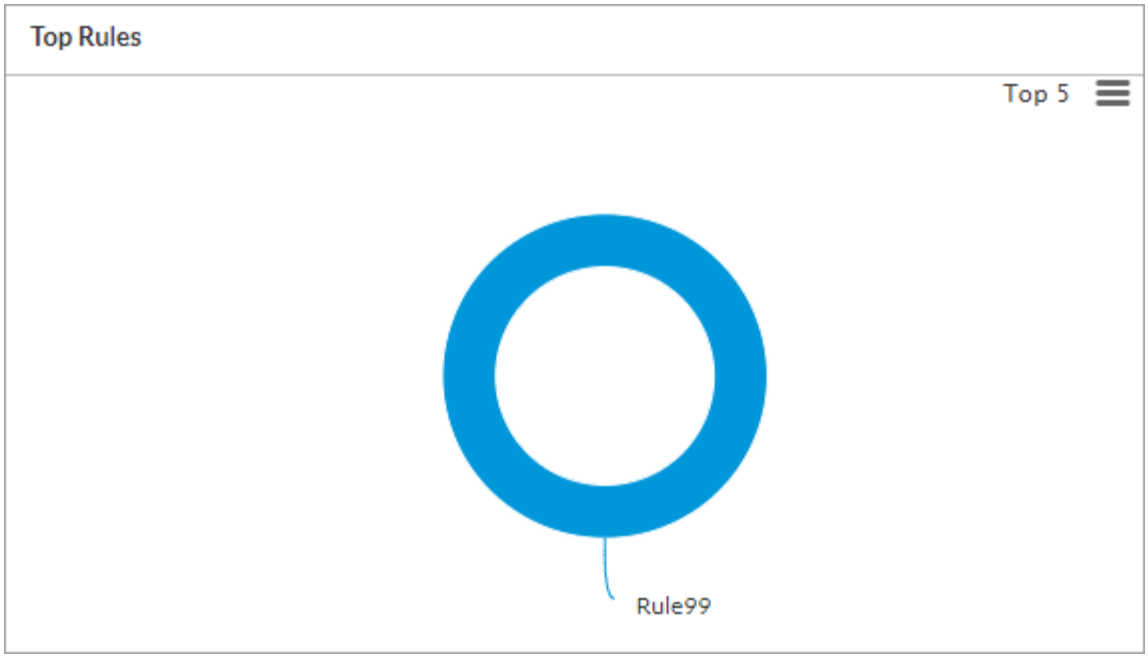
   - Top IP addresses



- Top EIP profiles



- Top EIP rules



View Security Information

Concerto collects various security statistics for a tenant that you can display from the View tab. For each tenant, the Security tab displays information about the following:

- Overview—Summary of security actions and threats.
- Internet Protection—Displays the statistics for internet protection rules by web, Firewall, threat filtering, threat detection, and Data Loss Prevention (DLP).
- Private App Protection—Displays the statistics for private applications and usage or private applications by users.

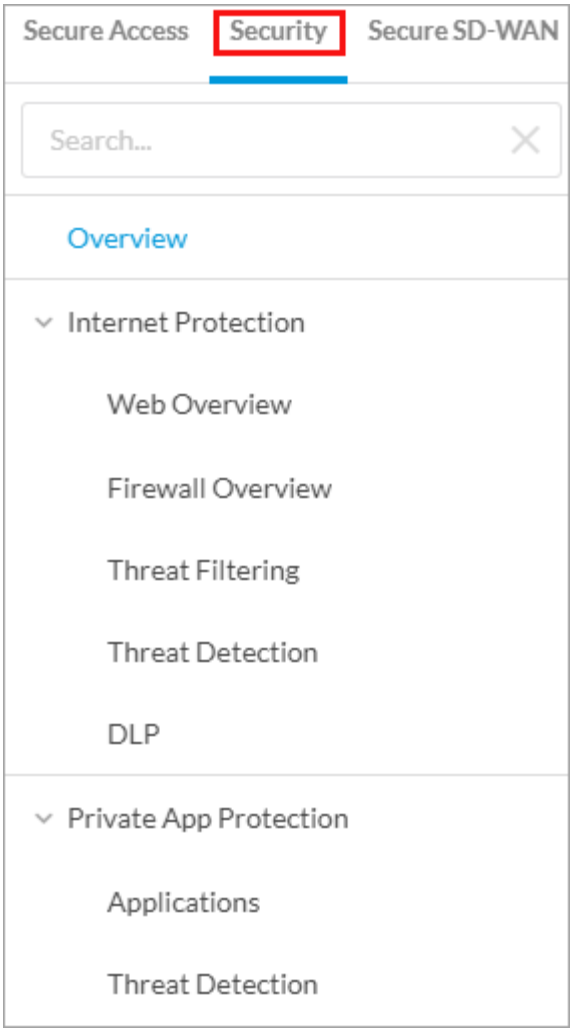
Security Overview Tab

The security Overview tab displays the following:

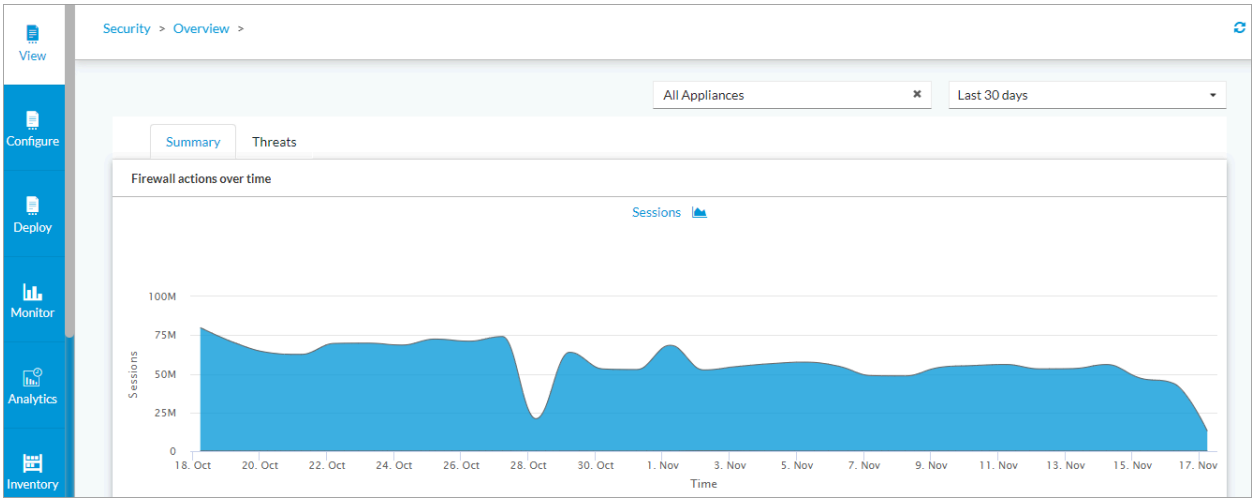
- Summary of Firewall actions and statistics for applications, URL categories, and rules
- Statistics for threats

To display security overview information:

1. Select View in the left navigation pane and then select the Security tab.



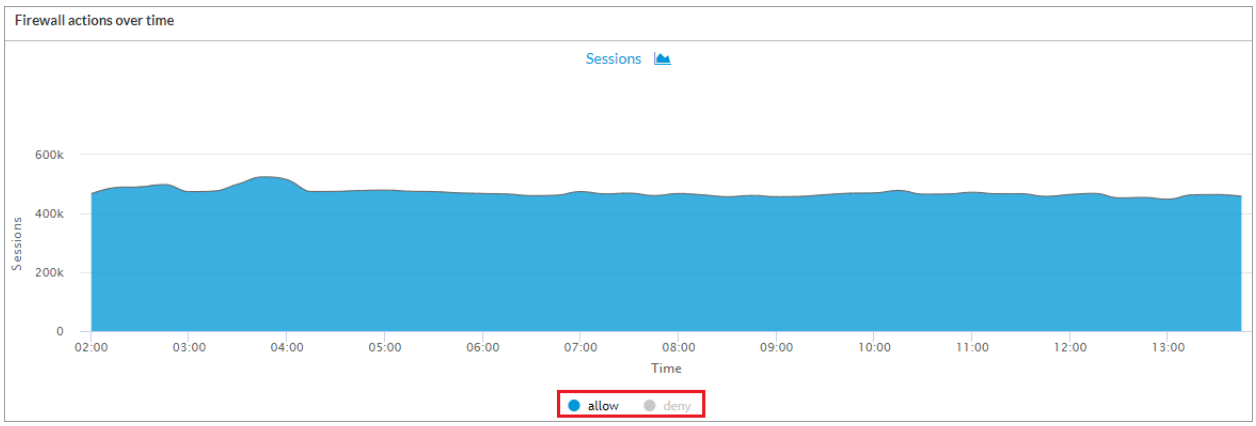
The Summary tab displays by default.



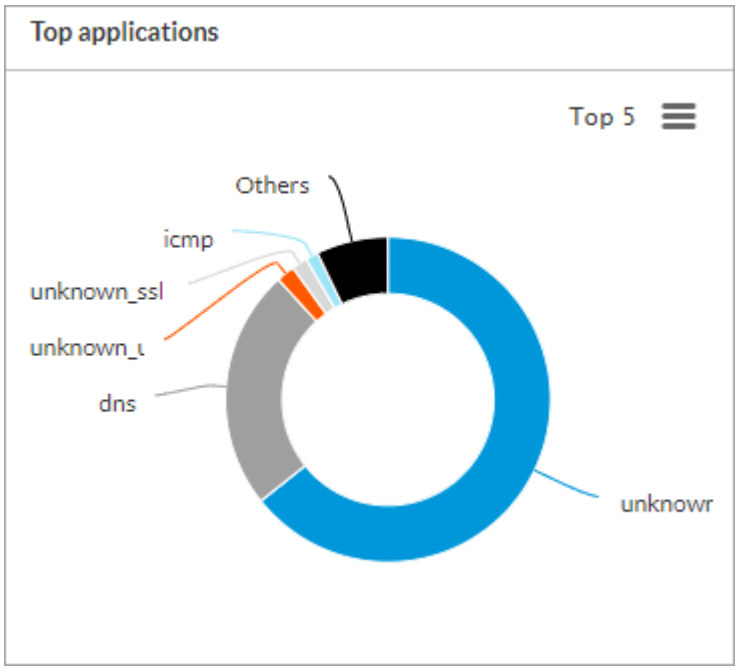
2. Summary tab display the following panes. For applications, URL categories and rules charts, click each category

to view the drilldown details:

- Firewall actions over time. Select Allow or Deny below the graph to display the Firewall actions that were allowed or denied:

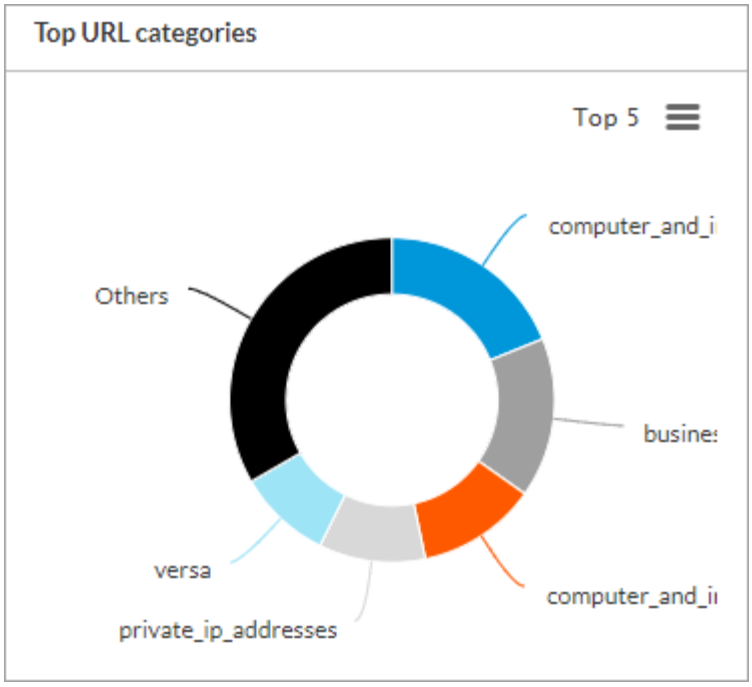


- Top applications

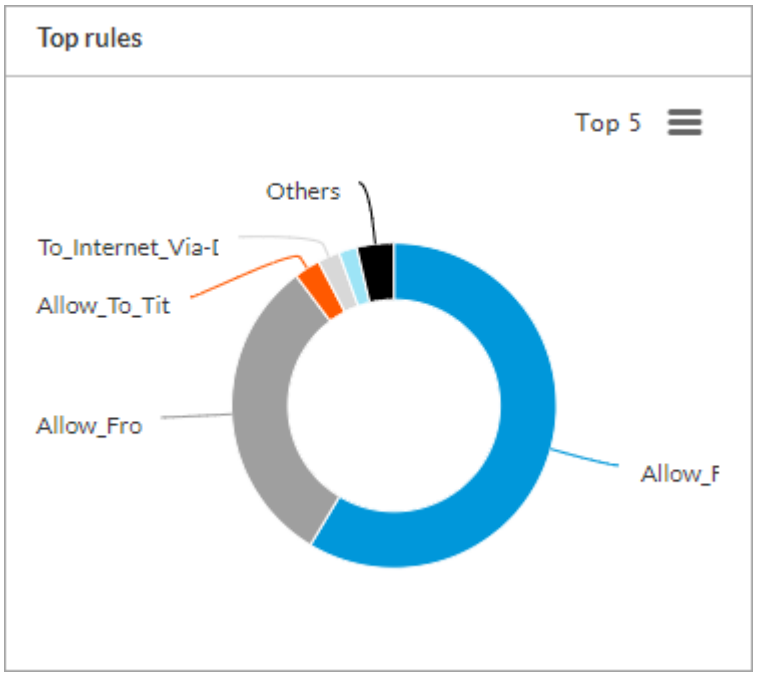


- Top URL categories

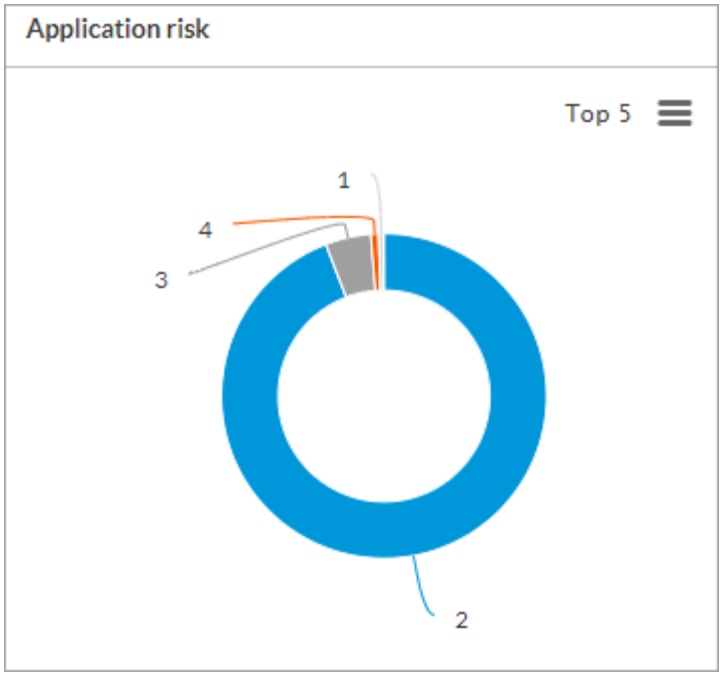
Updated: Wed, 23 Oct 2024 08:54:28 GMT



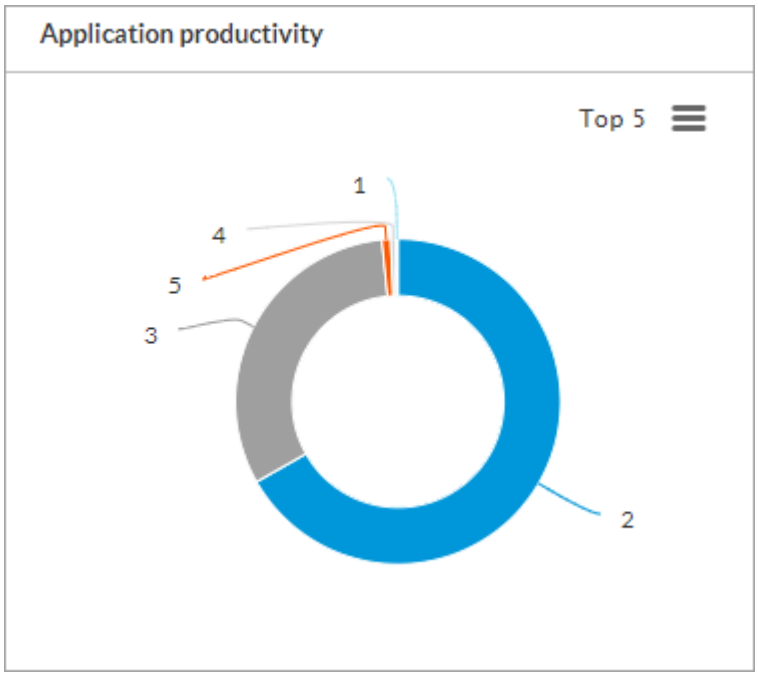
- Top security rules



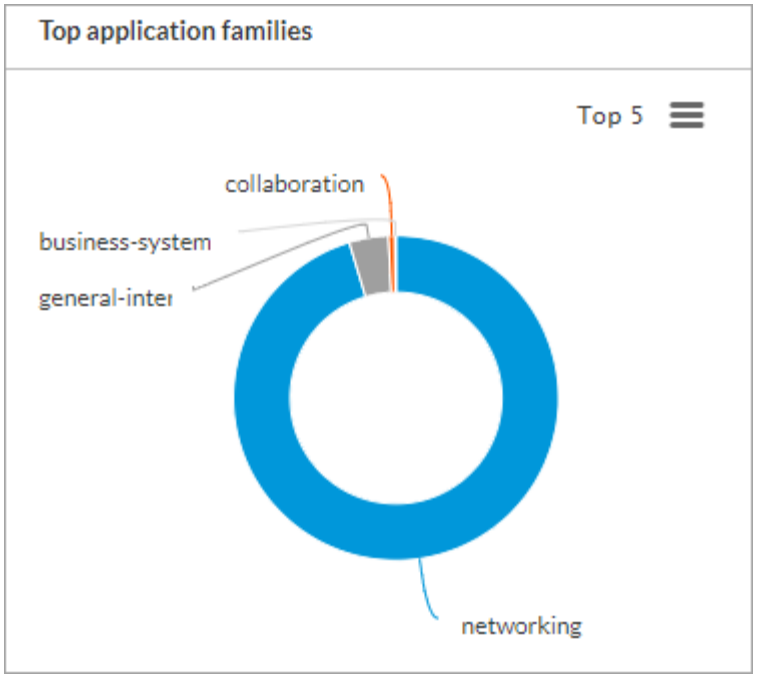
- Application risk



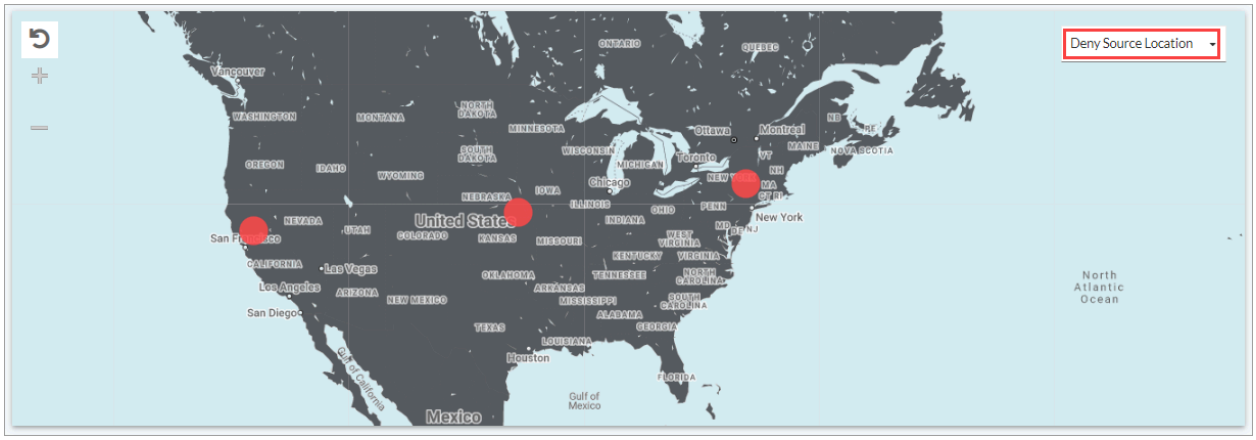
- Application productivity



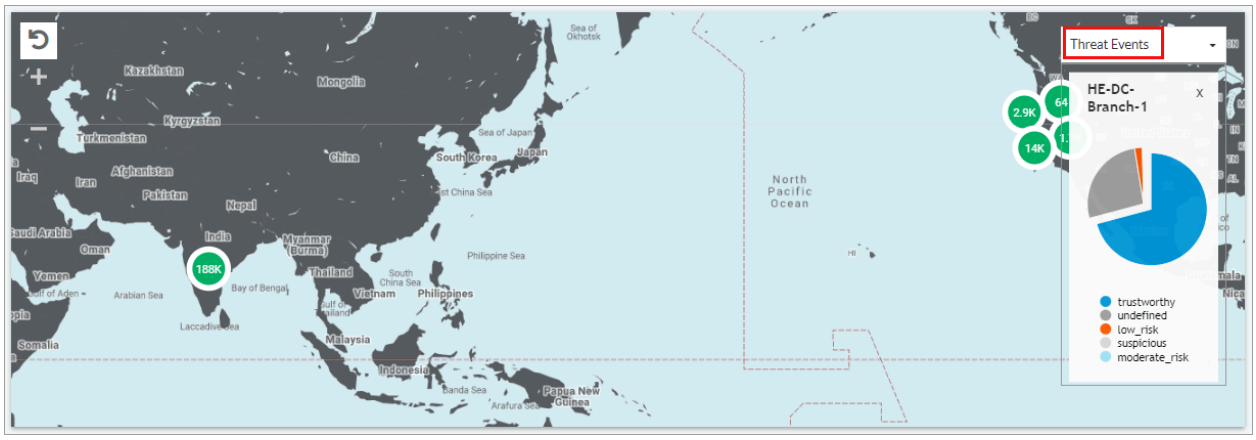
- Top application families



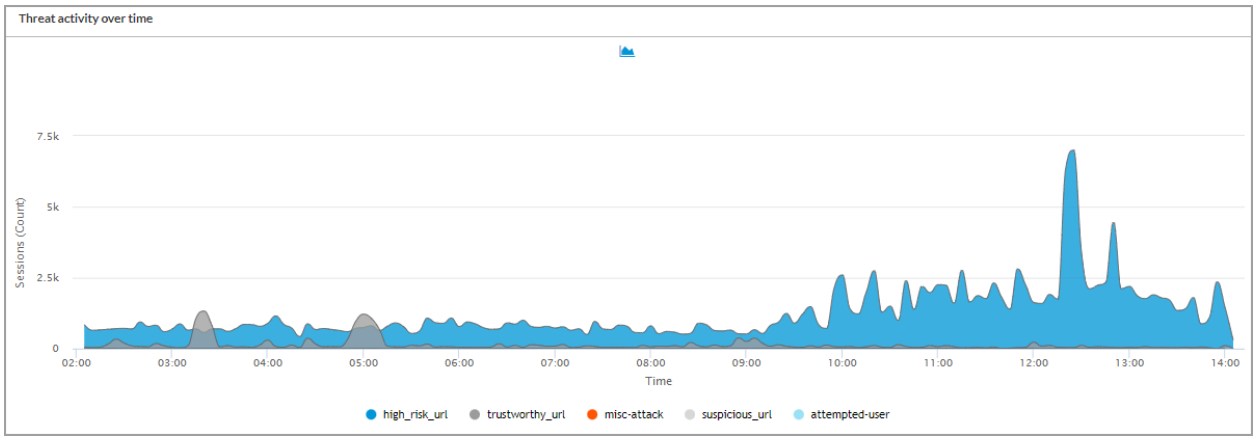
3. Select the Threat tab to display threat statistics. The Threat tab displays the following panes:
   - Region-wise threat events—From the drop-down list, select Threat Events or Deny Source Location.



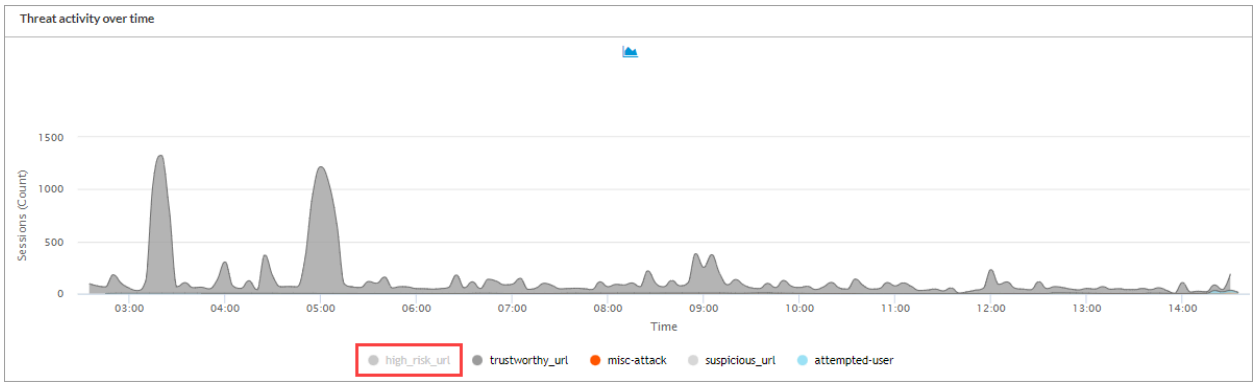
   - Click the green or red circle, for Threat Events and Deny Source Location to display details for that area. For example:



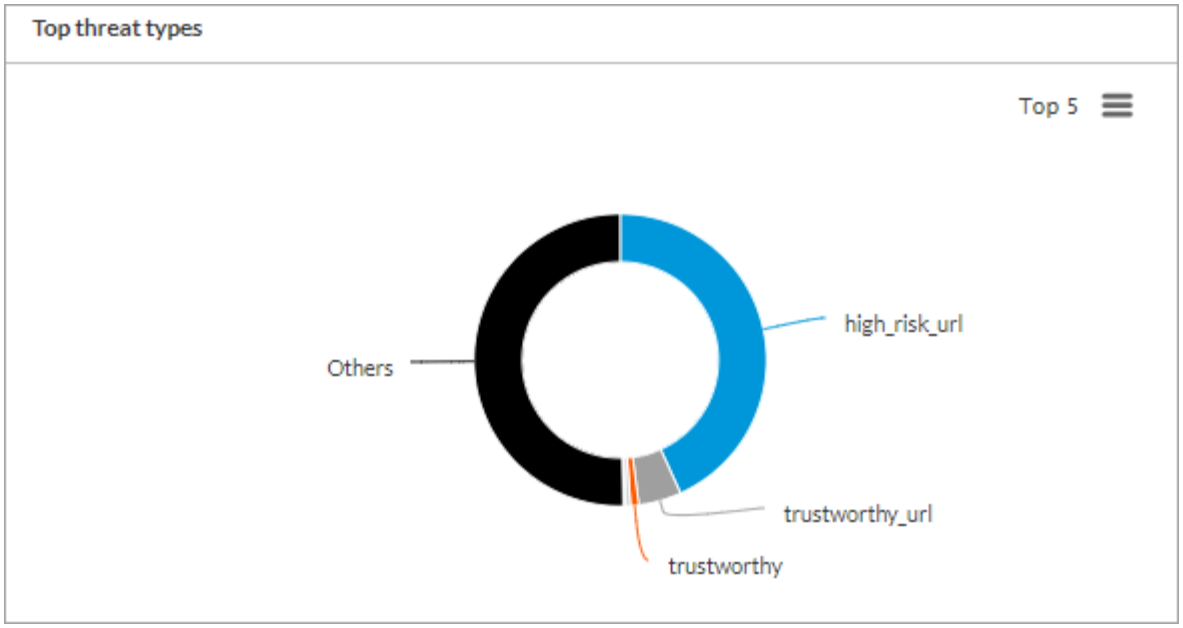
- Threat activity over time



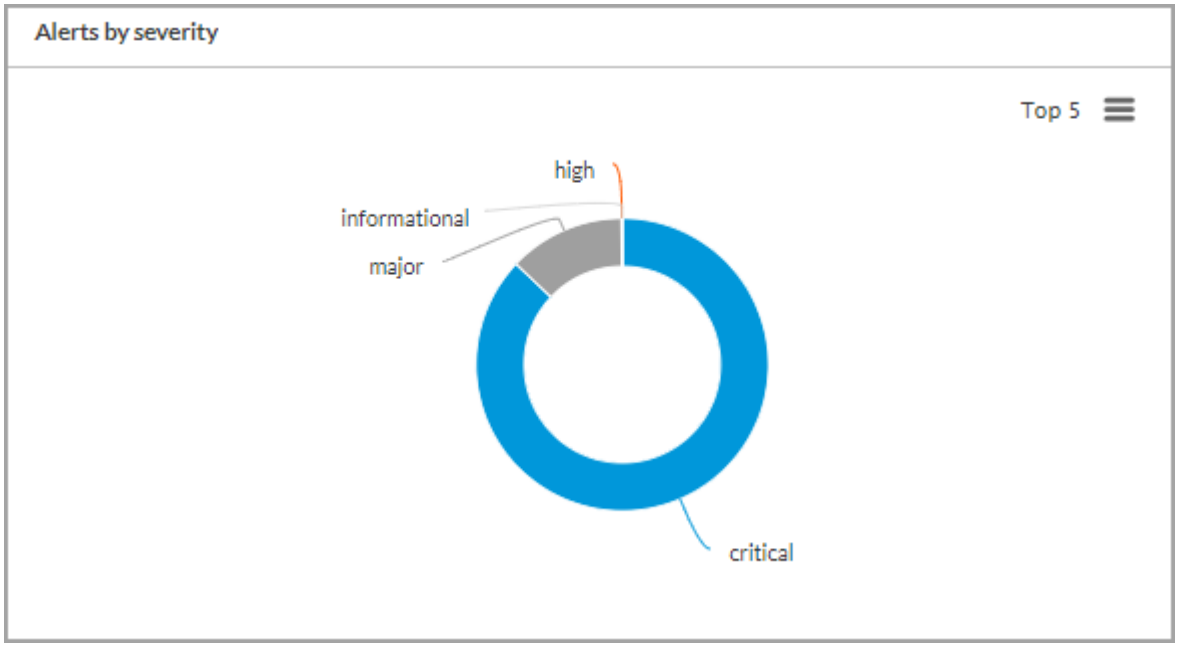
- You can select to display high risk URL, trustworthy URL, miscellaneous attack, suspicious URL, or attempted user, or select all or a combination of these. For example, in the following screenshot, high risk URL is not selected:



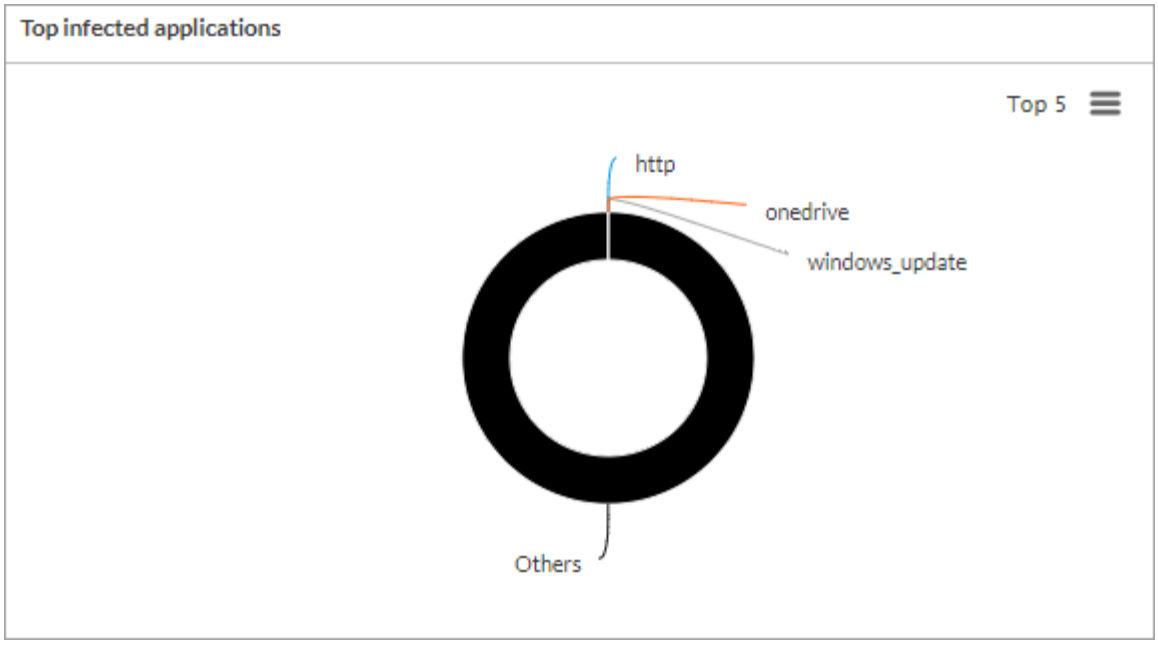
- Top threat types. Click any category for these charts to drill down and view details.



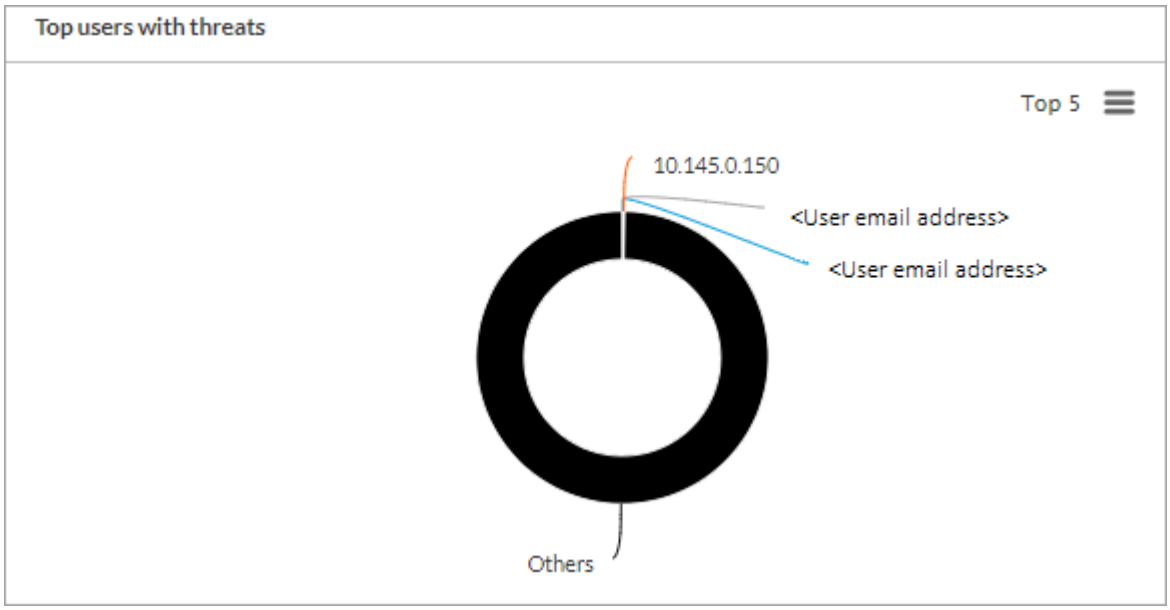
- Alerts by severity



- Top infected applications



- Top users with threats

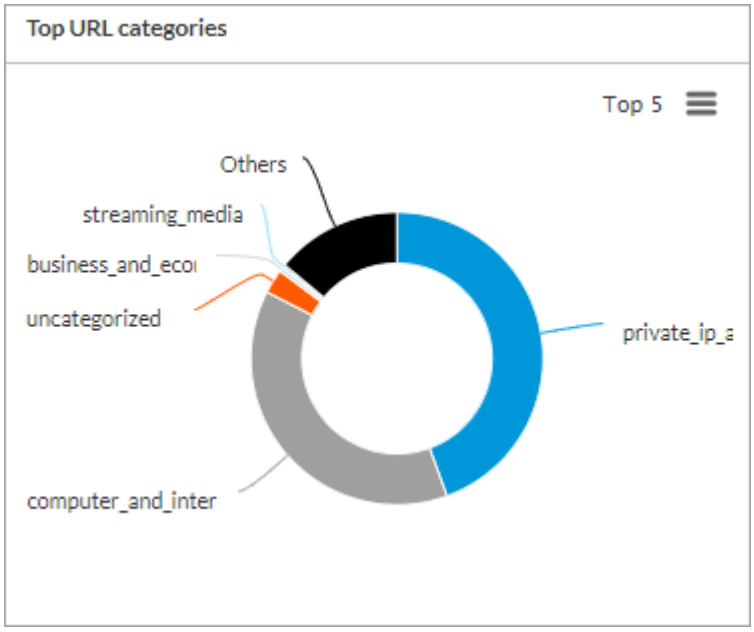


View Internet Protection Web Overview

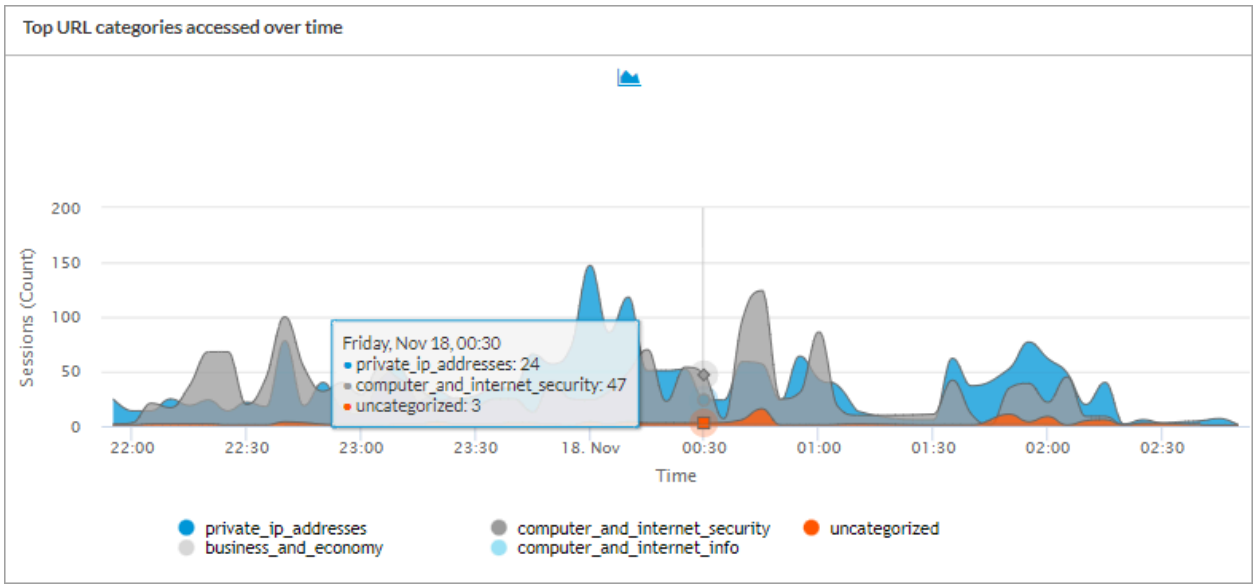
Internet protection rules are firewall rules that are applied to internet-bound traffic on a per-tenant basis. They provide network protection by establishing match criteria and enforcement actions. The Web Overview screen displays statistics for top URL categories, applications, and HTTP protocol.

To display web overview information:

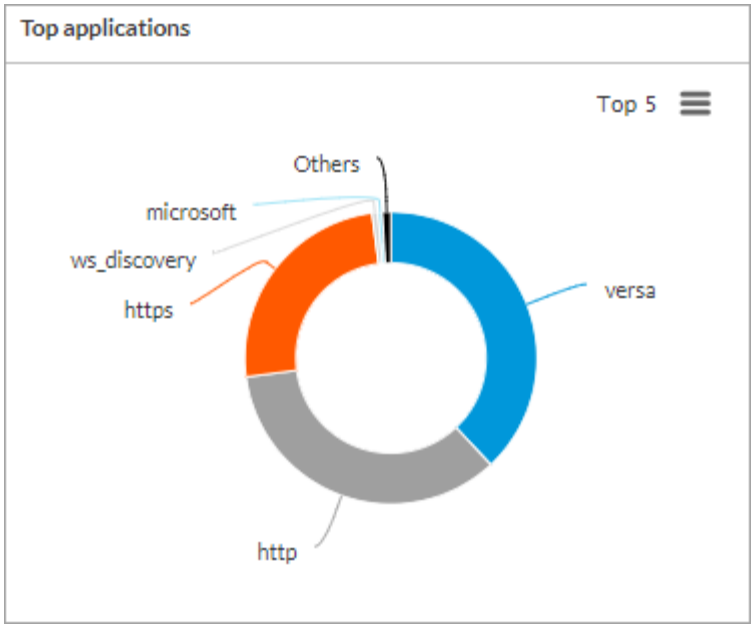
1. Select View in the left navigation pane and then select the Security tab.
2. Select Internet Protection > Web Overview. The Web Overview screen displays the following panes:
   - Top URL categories



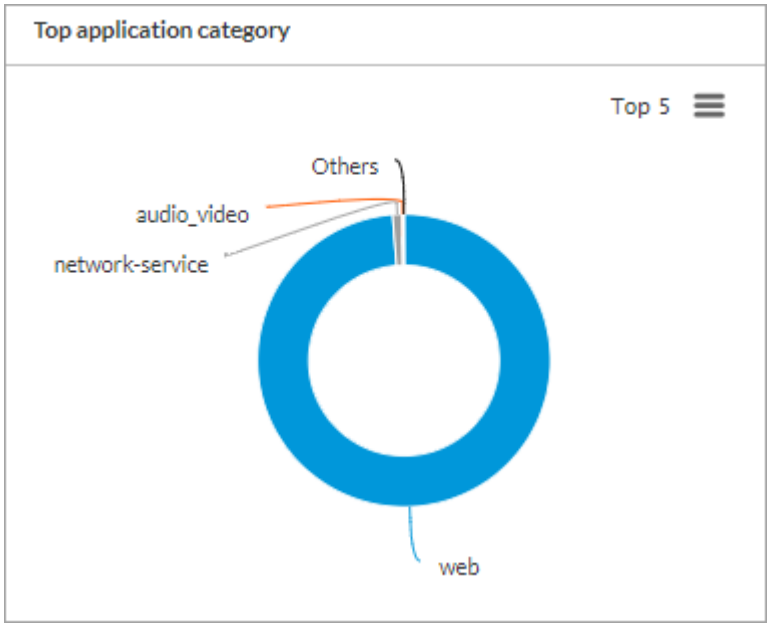
   - Top URL categories accessed over time



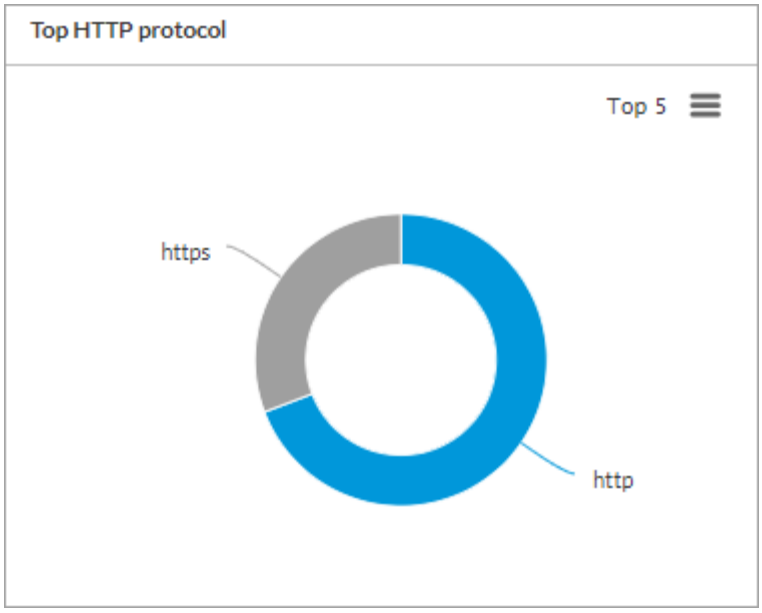
   - Top applications



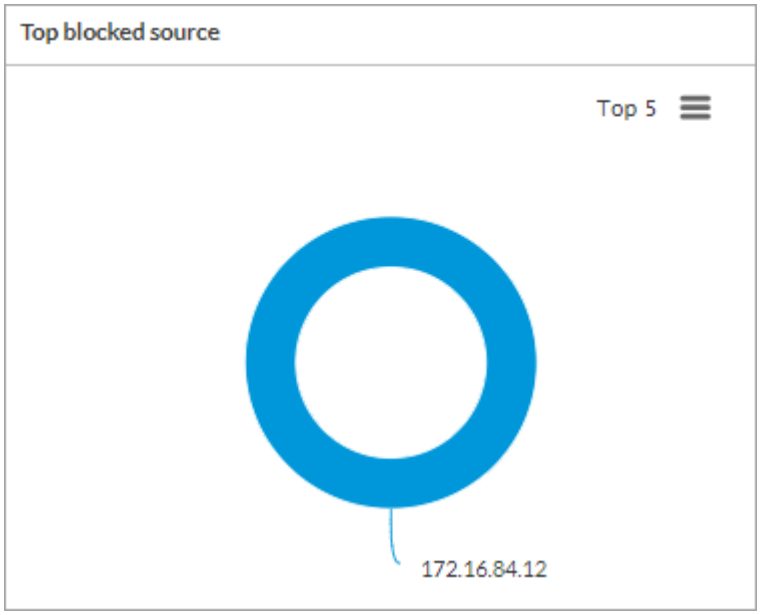
- Top application category



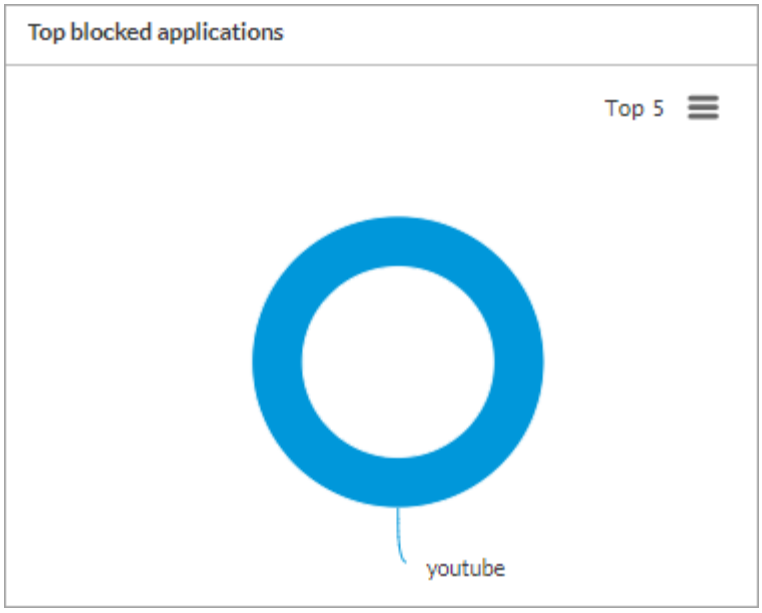
- Top HTTP protocol



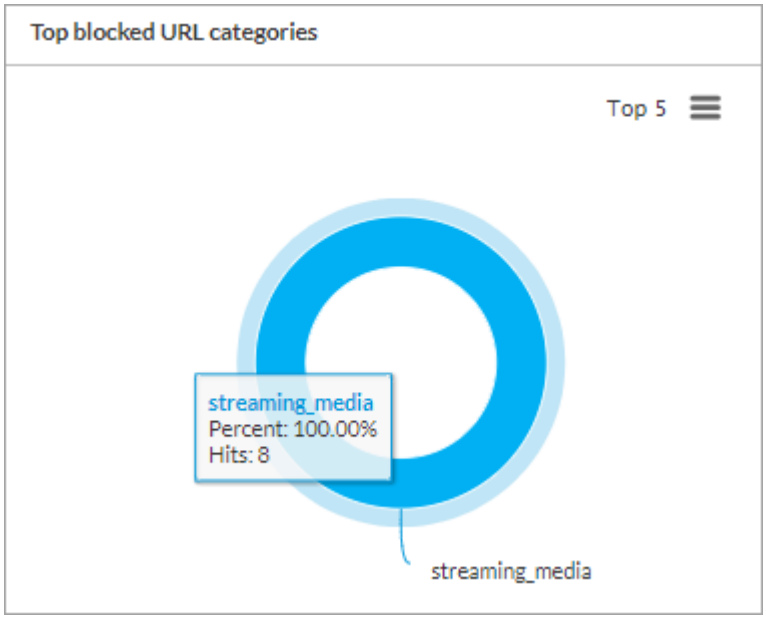
- Top blocked source



- Top blocked applications



- Top blocked URL categories



View Internet Protection Firewall Overview

The Firewall Overview screen displays the following information:

- Usage statistics for firewall rules
- Usage statistics for source IP address
- Usage statistics for destination IP address

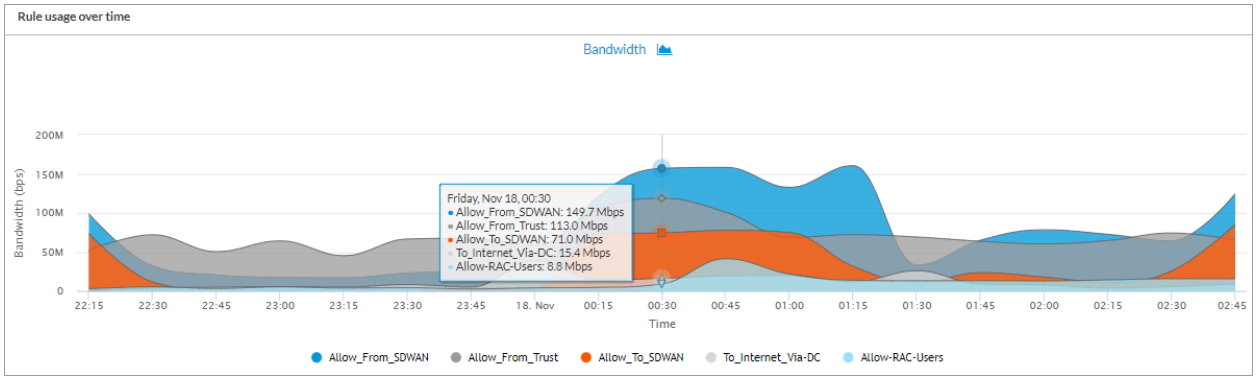
- Usage statistics for internet protection zones
- Usage statistics for forwarding class

To display firewall overview information:

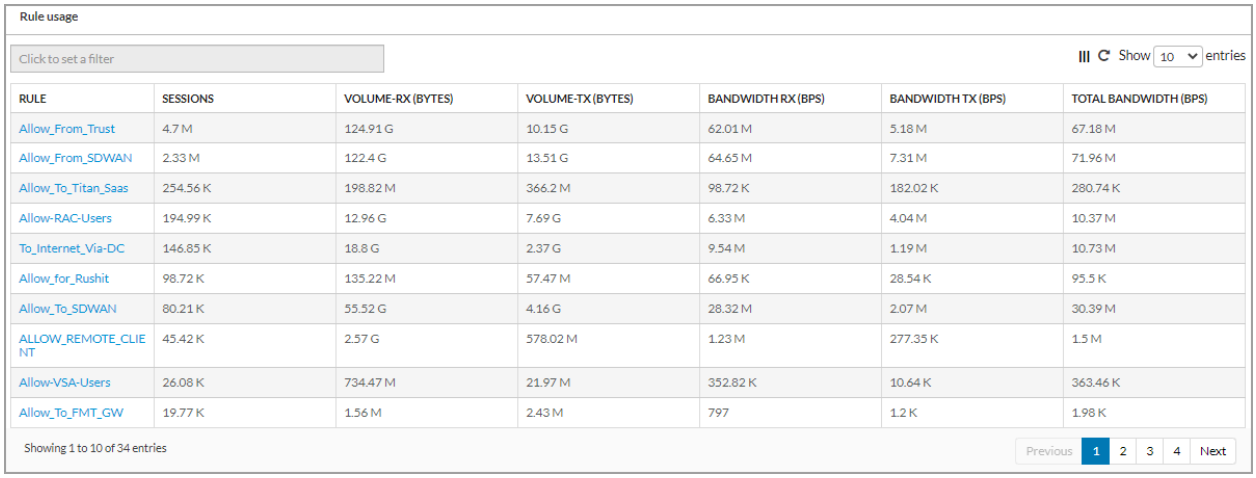
1. Select View in the left navigation pane and then select the Security tab.
2. Select Internet Protection > Firewall Overview. The Rules tab displays by default:

The Rules tab displays the following panes for firewall rules:

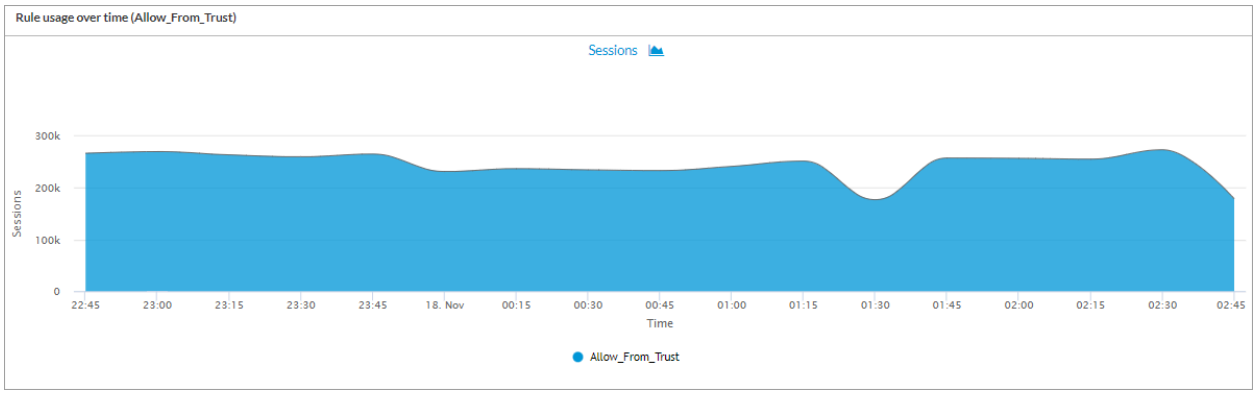
- Rule usage over time (graph)



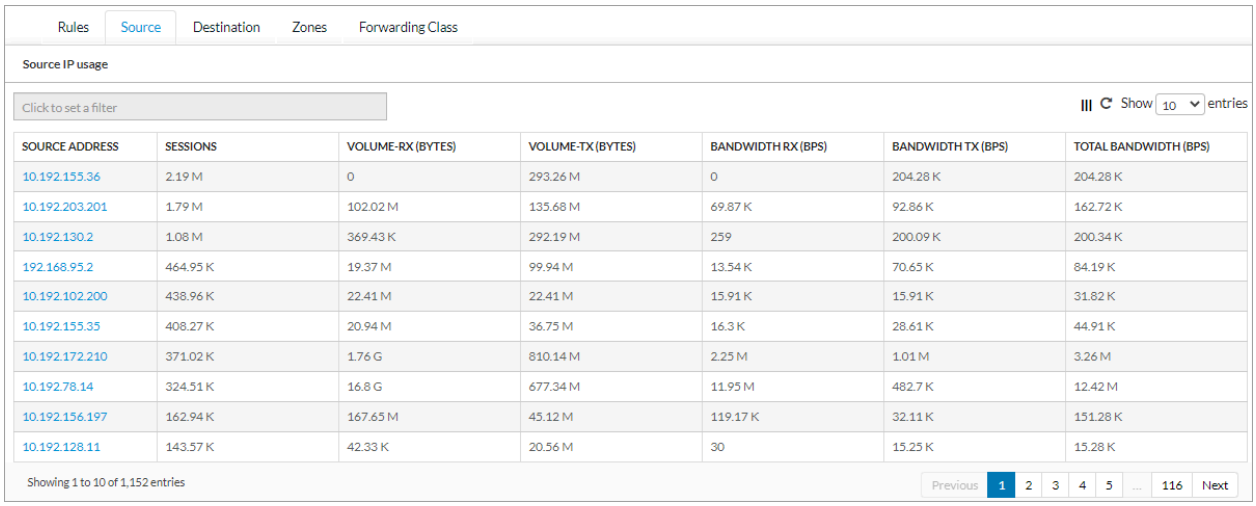
- Rule usage (table) by Bandwidth, Sessions, Volume Rx, Volume Tx, Volume Tx Rx



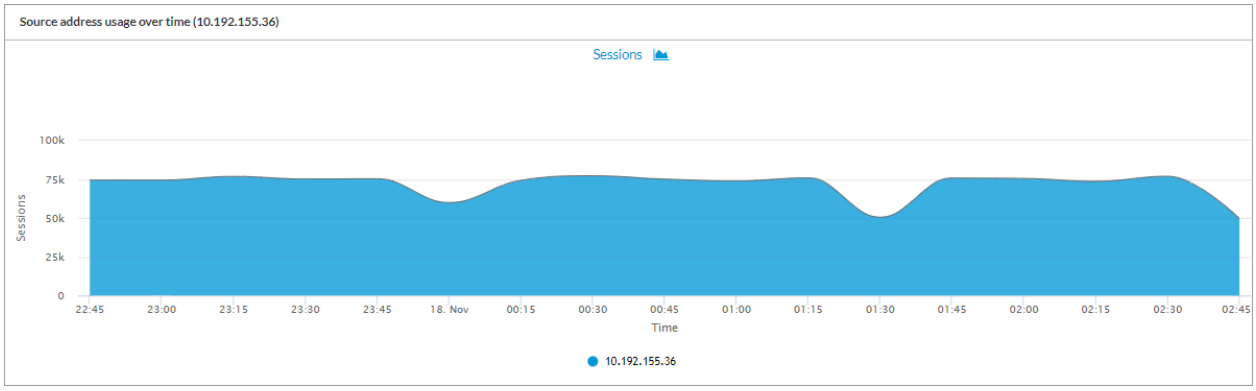
- Click a rule to display usage information over time in a graph. For example:



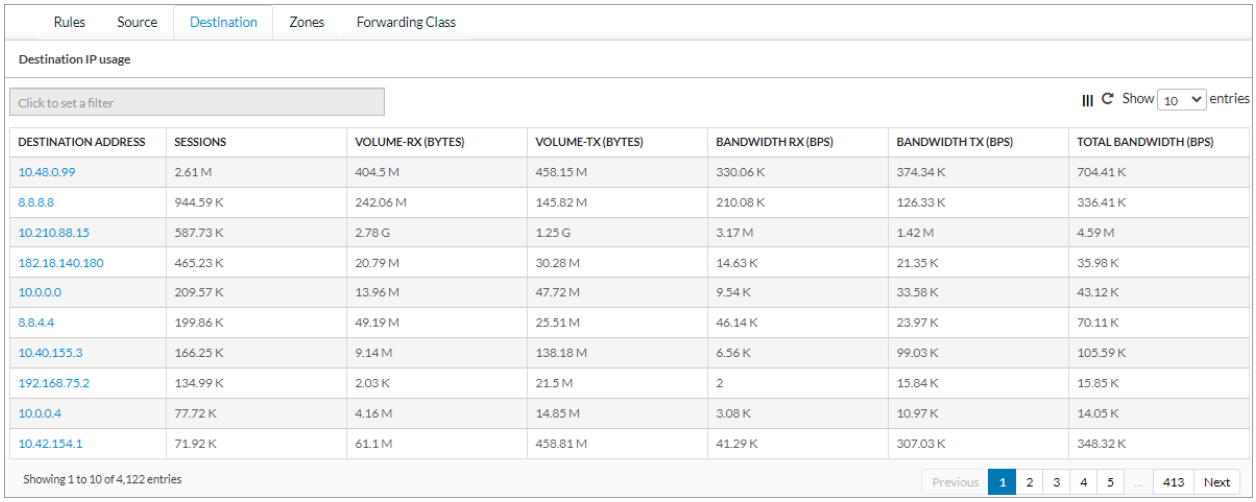
3. Select the Source tab to view usage statistics for source IP addresses. The Source tab displays the following panes:
   - Source IP usage table by Bandwidth, Sessions, Volume Rx, Volume Tx, Volume Tx Rx



- Click a source address to display the IP address usage over time in a graph. For example:

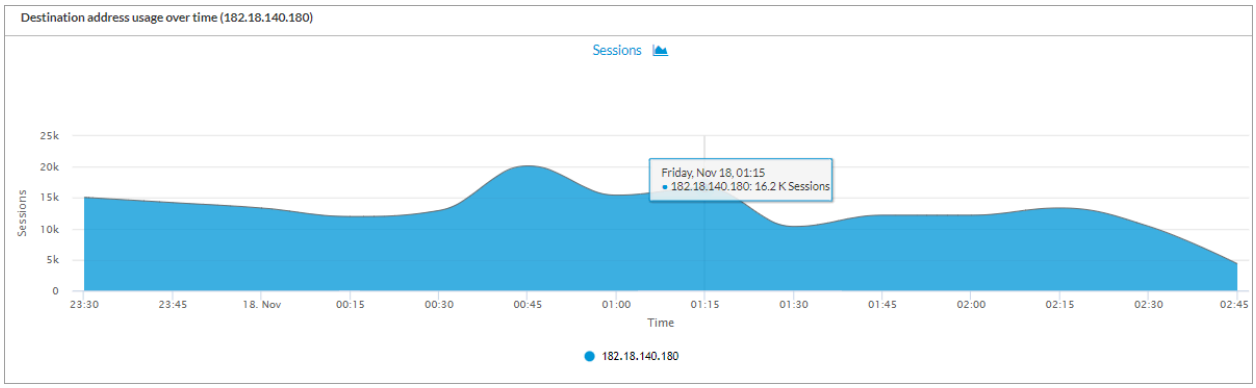


4. Select the Destination tab to view usage statistics for destination IP addresses. The Destination tab displays the following panes:
   - Destination IP address usage table by Bandwidth, Sessions, Volume Rx, Volume Tx, Volume Tx Rx.

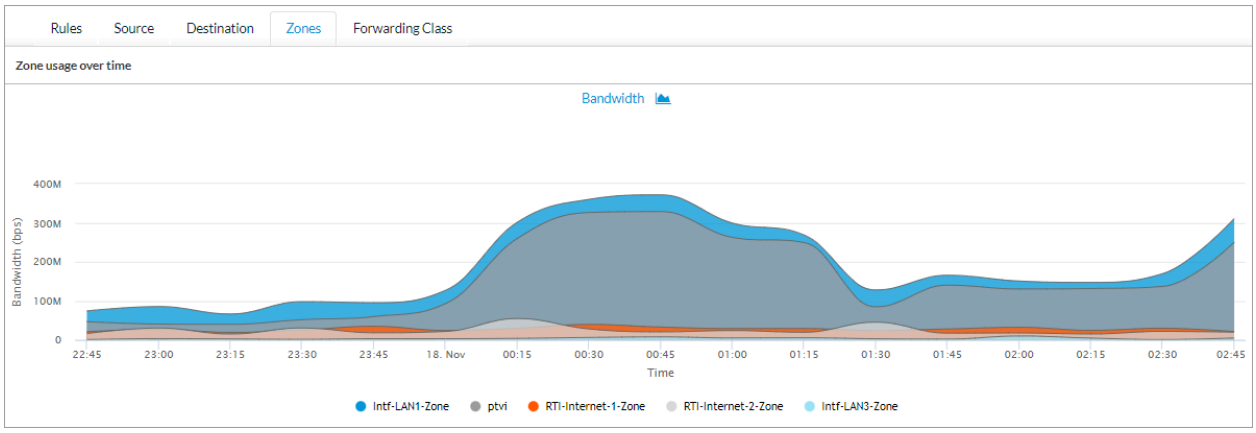


DESTINATION ADDRESS	SESSIONS	VOLUME-RX (BYTES)	VOLUME-TX (BYTES)	BANDWIDTH RX (BPS)	BANDWIDTH TX (BPS)	TOTAL BANDWIDTH (BPS)
10.48.0.99	2.61 M	404.5 M	458.15 M	330.06 K	374.34 K	704.41 K
8.8.8.8	944.59 K	242.06 M	145.82 M	210.08 K	126.33 K	336.41 K
10.210.88.15	587.73 K	2.78 G	1.25 G	3.17 M	1.42 M	4.59 M
182.18.140.180	465.23 K	20.79 M	30.28 M	14.63 K	21.35 K	35.98 K
10.0.0.0	209.57 K	13.96 M	47.72 M	9.54 K	33.58 K	43.12 K
8.8.4.4	199.86 K	49.19 M	25.51 M	46.14 K	23.97 K	70.11 K
10.40.155.3	166.25 K	9.14 M	138.18 M	6.56 K	99.03 K	105.59 K
192.168.75.2	134.99 K	2.03 K	21.5 M	2	15.84 K	15.85 K
10.0.0.4	77.72 K	4.16 M	14.85 M	3.08 K	10.97 K	14.05 K
10.42.154.1	71.92 K	61.1 M	458.81 M	41.29 K	307.03 K	348.32 K

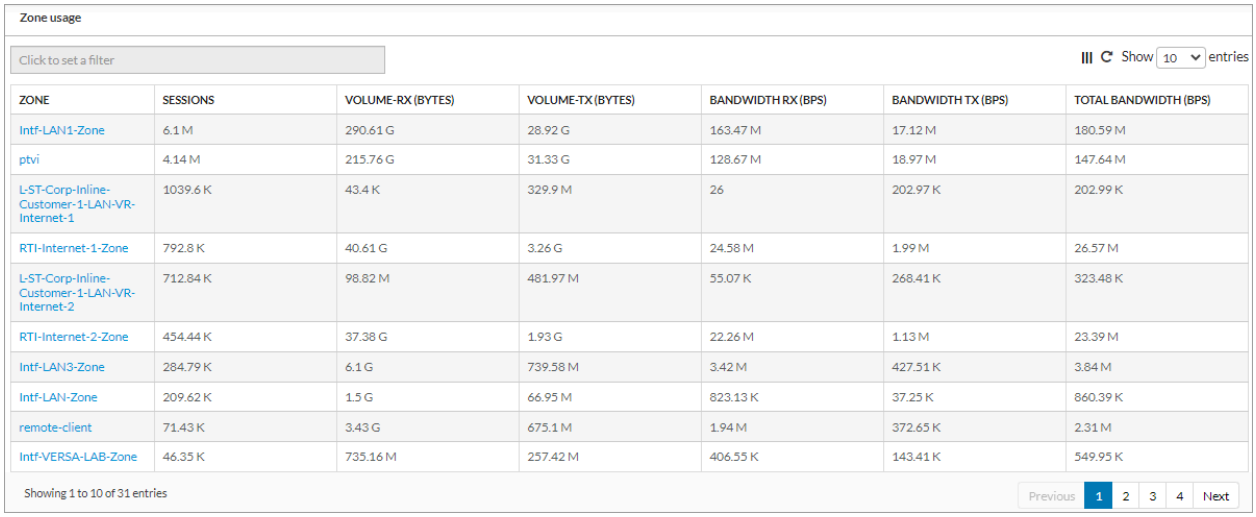
   - Click a destination address to display the IP address usage over time in a graph. For example:



5. Select the Zones tab to view usage statistics for internet protection zone. The Zones tab displays the following panes:
   - Zone Usage over Time (chart)

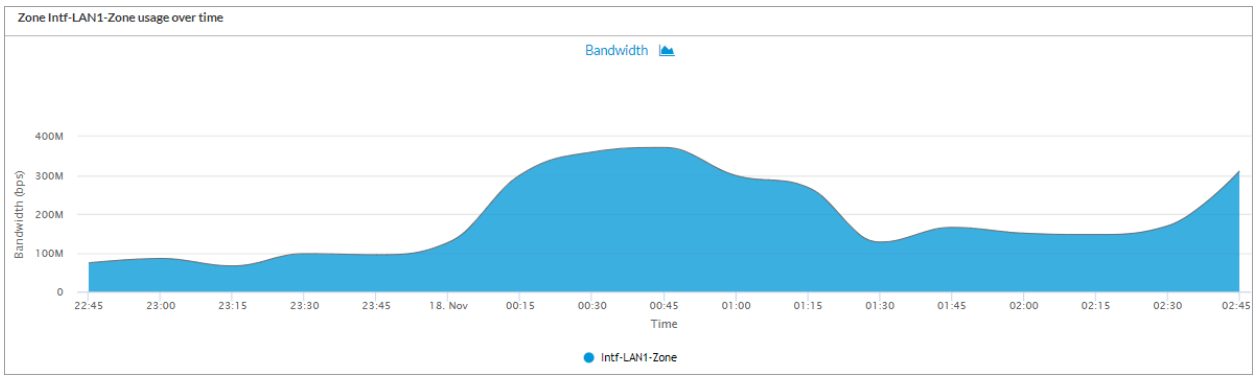


- Zone usage (table) by Bandwidth, Sessions, Volume Rx, Volume Tx, Volume Tx Rx

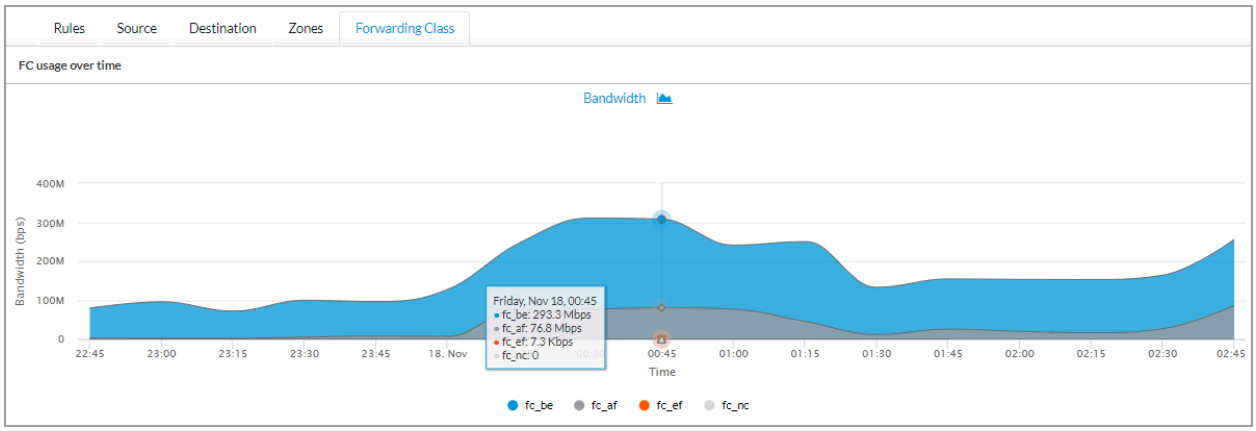


ZONE	SESSIONS	VOLUME-RX (BYTES)	VOLUME-TX (BYTES)	BANDWIDTH RX (BPS)	BANDWIDTH TX (BPS)	TOTAL BANDWIDTH (BPS)
Intf-LAN1-Zone	6.1 M	290.61 G	28.92 G	163.47 M	17.12 M	180.59 M
ptvi	4.14 M	215.76 G	31.33 G	128.67 M	18.97 M	147.64 M
L-ST-Corp-Inline-Customer-1-LAN-VR-Internet-1	1039.6 K	43.4 K	329.9 M	26	202.97 K	202.99 K
RTI-Internet-1-Zone	792.8 K	40.61 G	3.26 G	24.58 M	1.99 M	26.57 M
L-ST-Corp-Inline-Customer-1-LAN-VR-Internet-2	712.84 K	98.82 M	481.97 M	55.07 K	268.41 K	323.48 K
RTI-Internet-2-Zone	454.44 K	37.38 G	1.93 G	22.26 M	1.13 M	23.39 M
Intf-LAN3-Zone	284.79 K	6.1 G	739.58 M	3.42 M	427.51 K	3.84 M
Intf-LAN-Zone	209.62 K	1.5 G	66.95 M	823.13 K	37.25 K	860.39 K
remote-client	71.43 K	3.43 G	675.1 M	1.94 M	372.65 K	2.31 M
Intf-VERSA-LAB-Zone	46.35 K	735.16 M	257.42 M	406.55 K	143.41 K	549.95 K

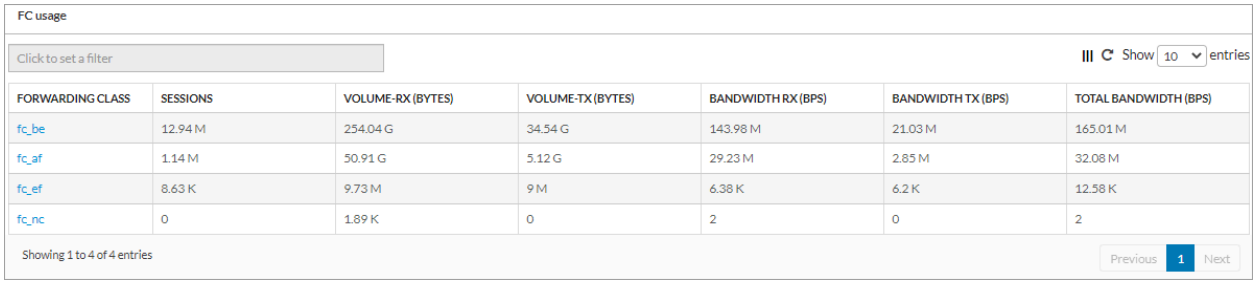
- Click a zone to display the zone usage over time in a graph. For example:



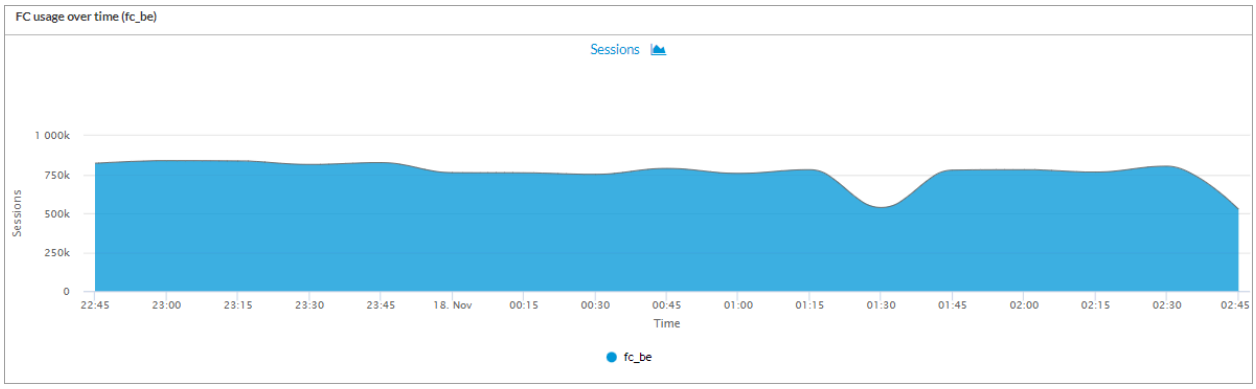
6. Select the Forwarding Class tab to view usage statistics for forwarding classes. The Forwarding Class tab displays the following panes:
   - FC usage over time (chart)



- FC usage (table) by Bandwidth, Sessions, Volume Rx, Volume Tx, Volume Tx Rx



- Click a forwarding class to display the FC usage over time in a graph. For example:



View Internet Protection Threat Filtering

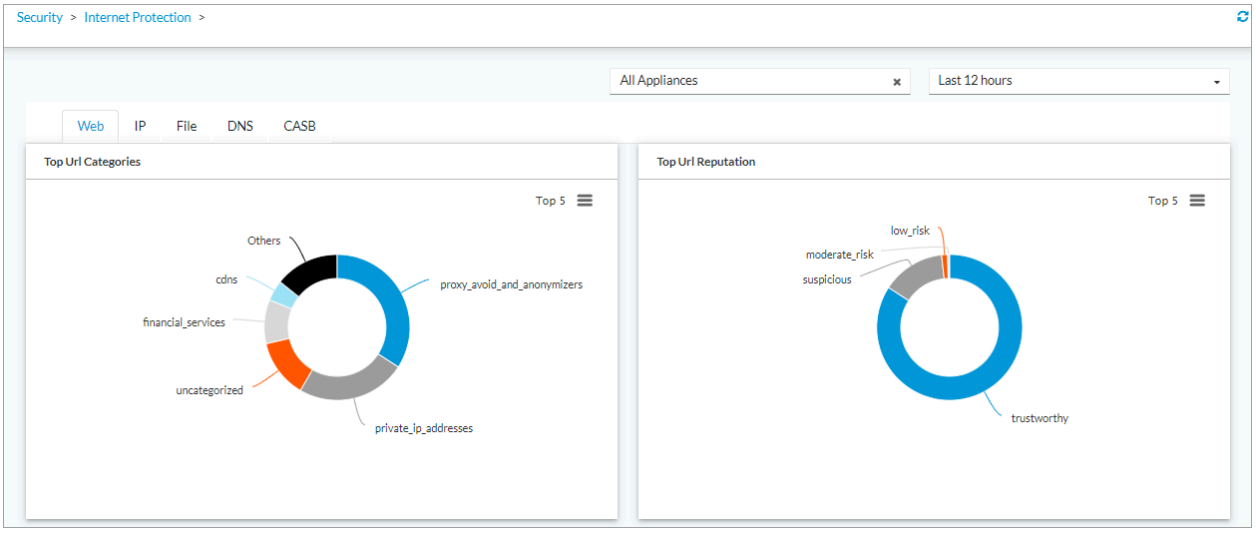
The Threat Filtering screen displays the following information:

- Statistics for top URL categories, reputation, profiles, and filtering source.
- Statistics for top IP filtering action, profiles, destination reputation, and source.
- Statistics for top file filtering action, profiles, file types, and source.
- Statistics for top DNS filtering profiles, message types, action, and domains.

- Statistics for top Cloud Access Security Broker (CASB) application, users, and rules.

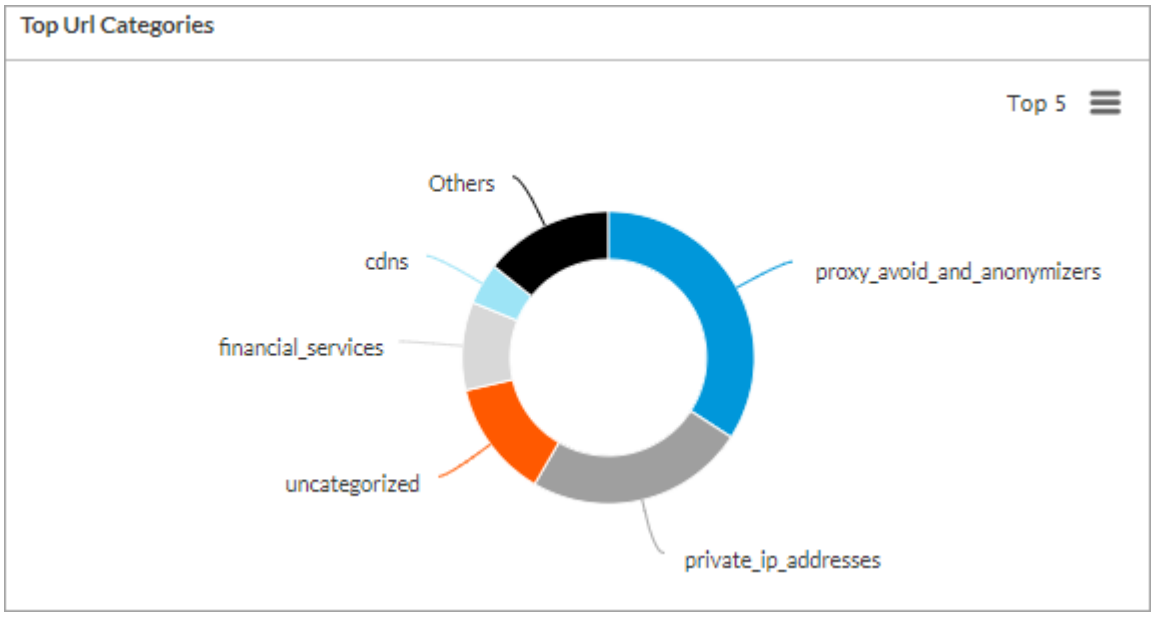
To display threat filtering information:

1. Select View in the left navigation pane and then select the Security tab.
2. Select Internet Protection > Threat Filtering. The Web tab displays by default:

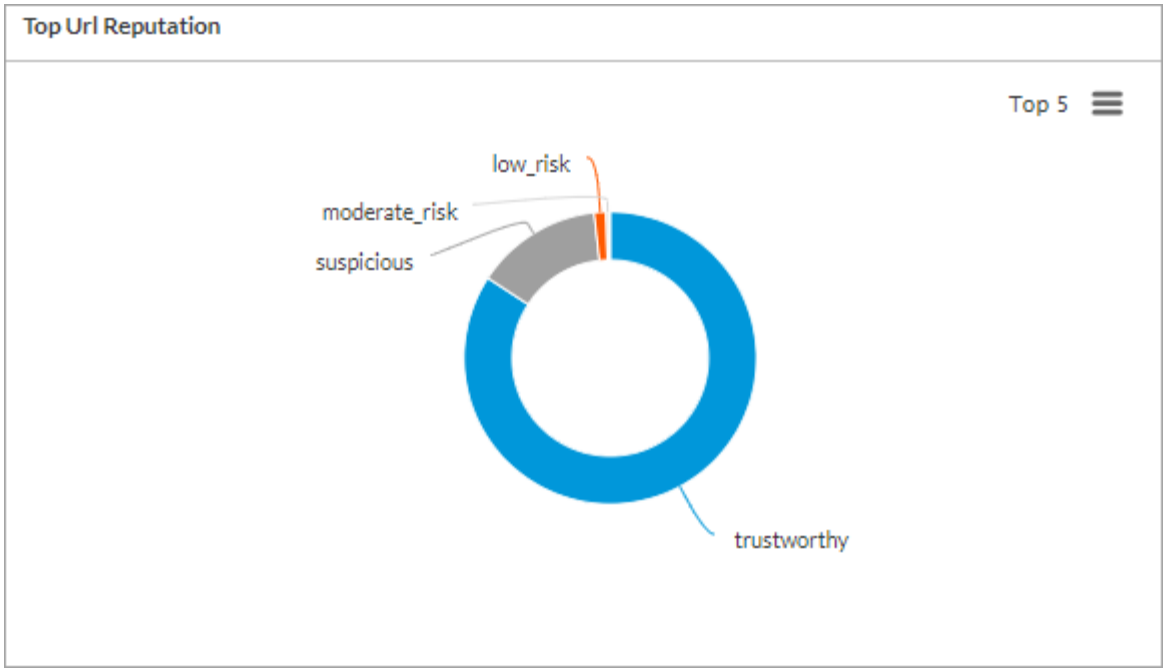


The Web tab displays the following panes for firewall rules:

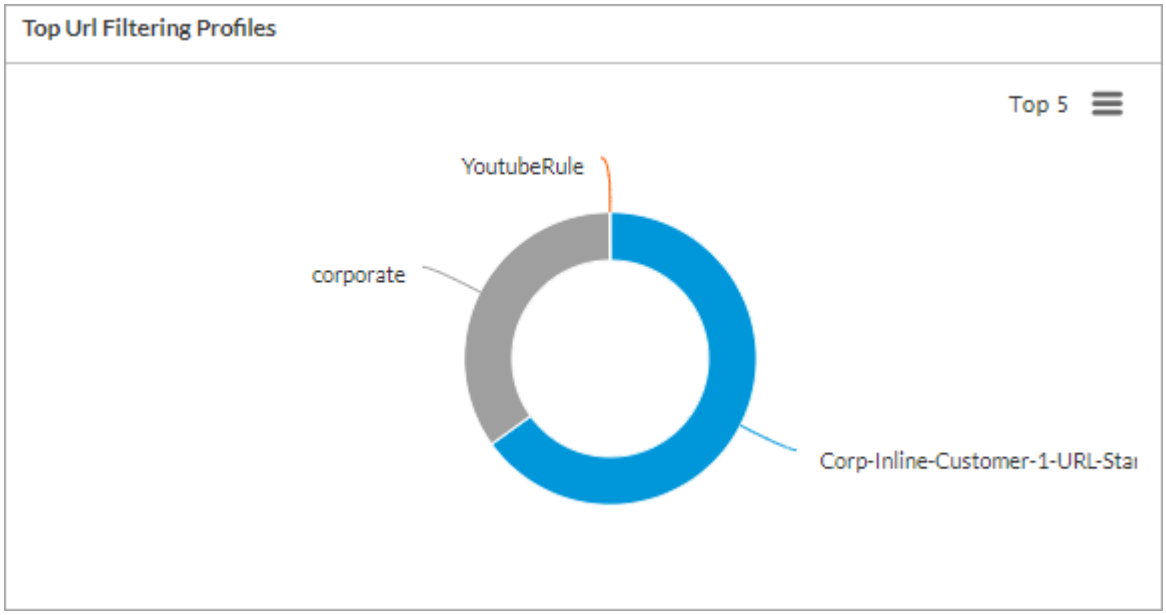
- Top URL categories



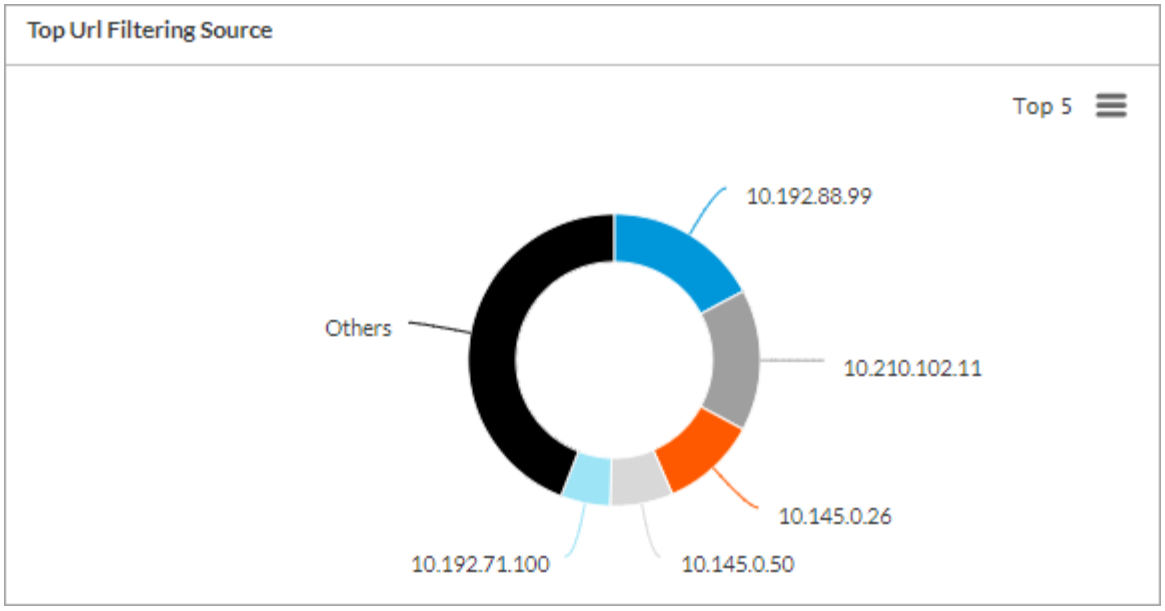
- Top URL reputation



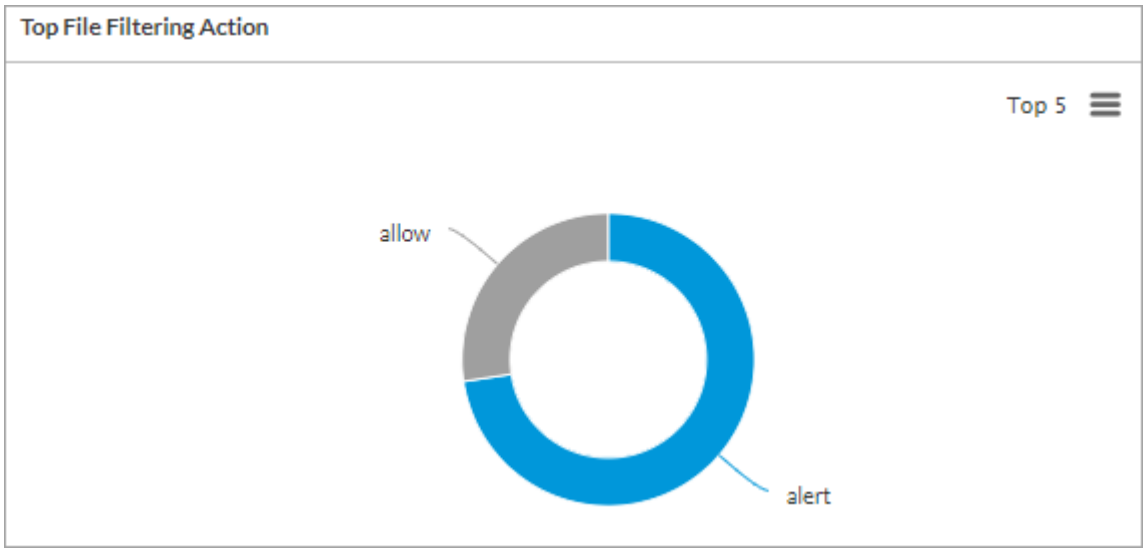
- Top URL filtering profiles



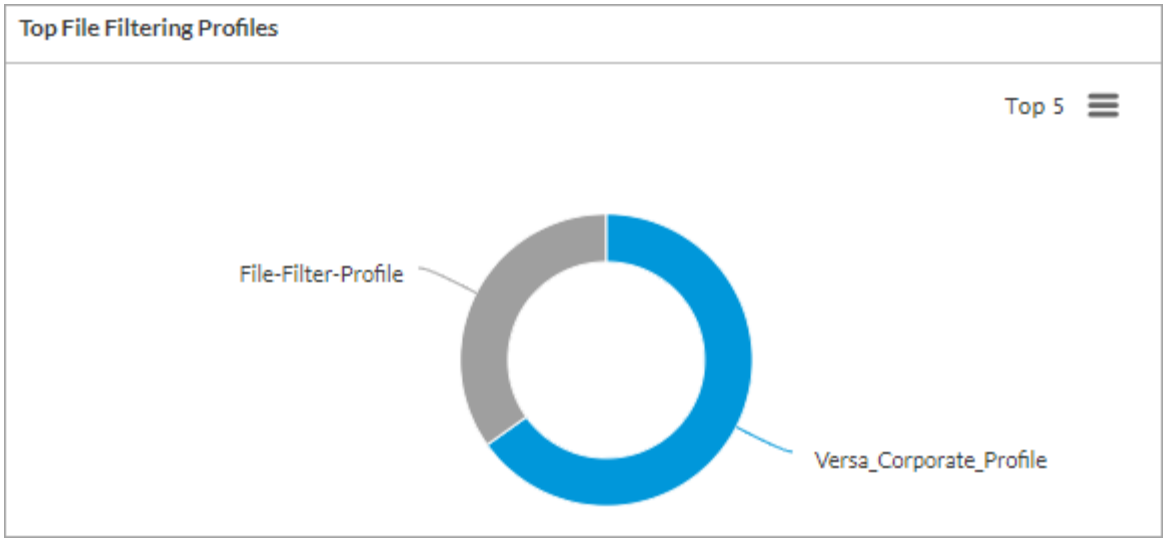
- Top URL filtering source



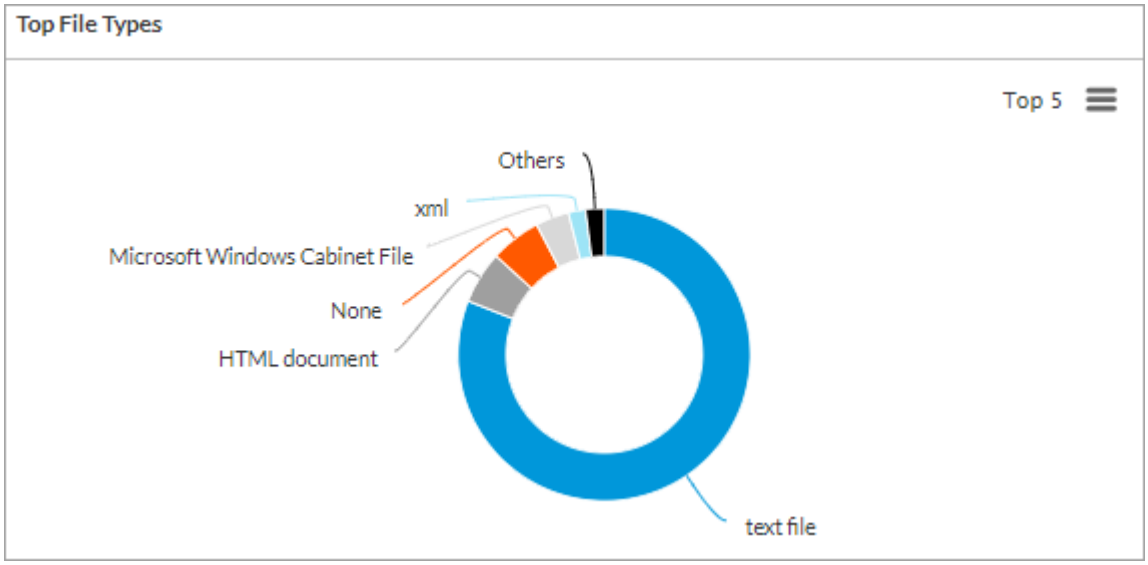
3. Select the File tab to view statistics for file filtering. The File tab displays the following panes:
   - Top file filtering action



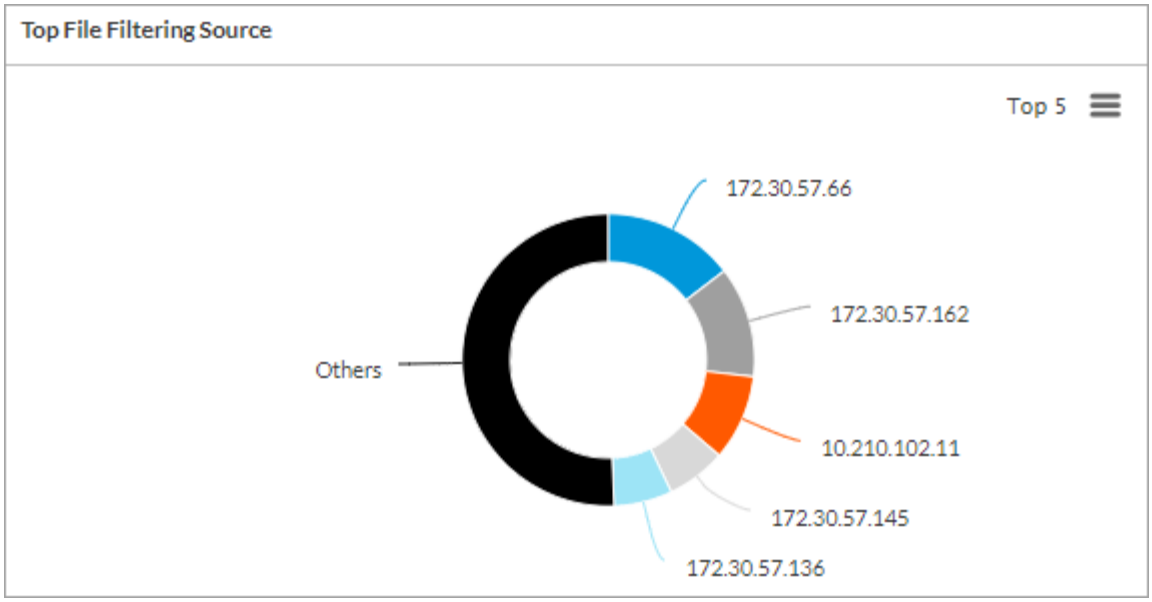
   - Top file filtering profiles



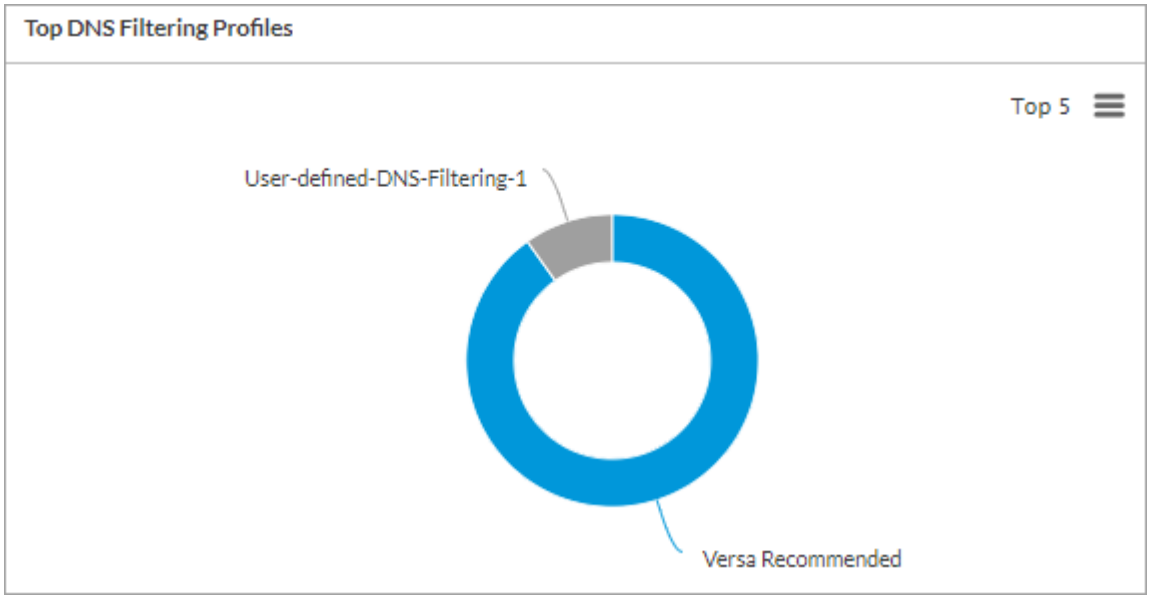
- Top file types



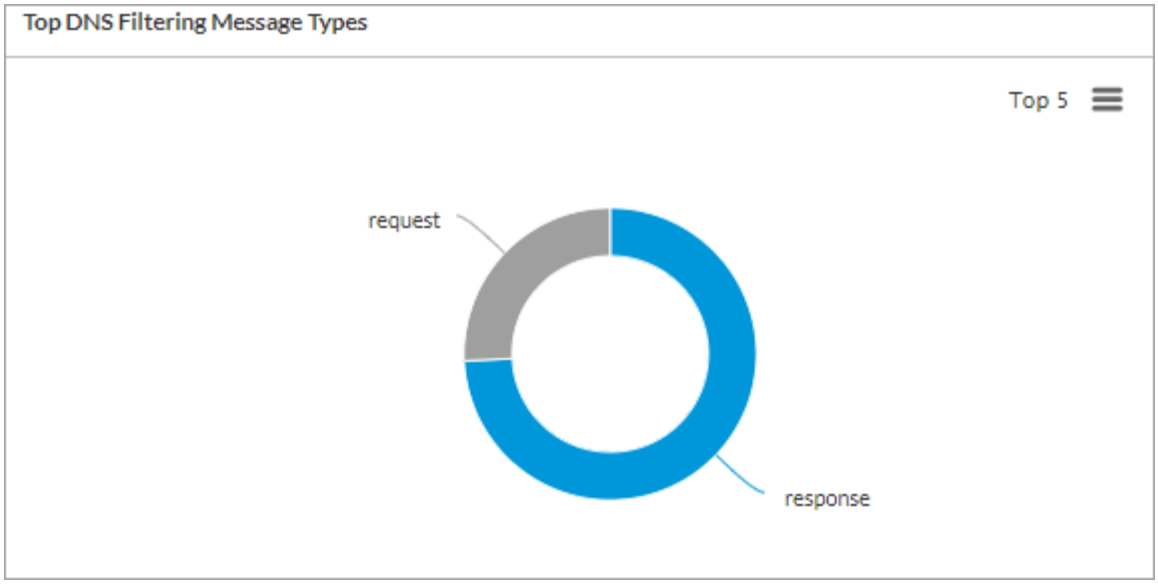
- Top file filtering source



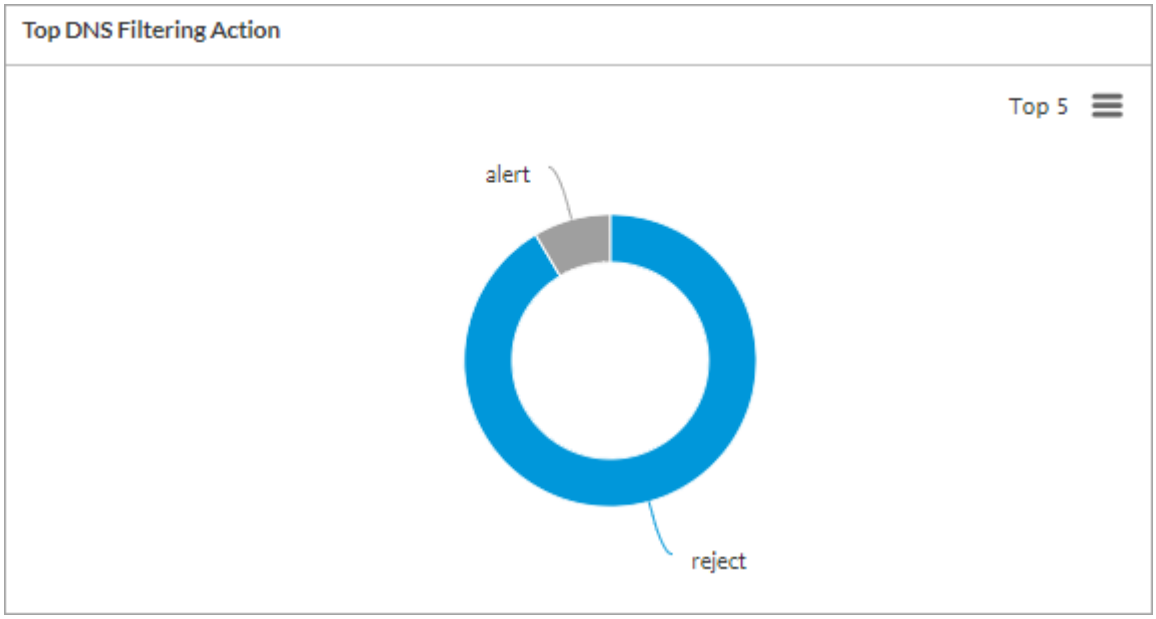
4. Select the DNS tab to view statistics for DNS filtering. The DNS tab displays the following panes:
   - Top DNS filtering profiles



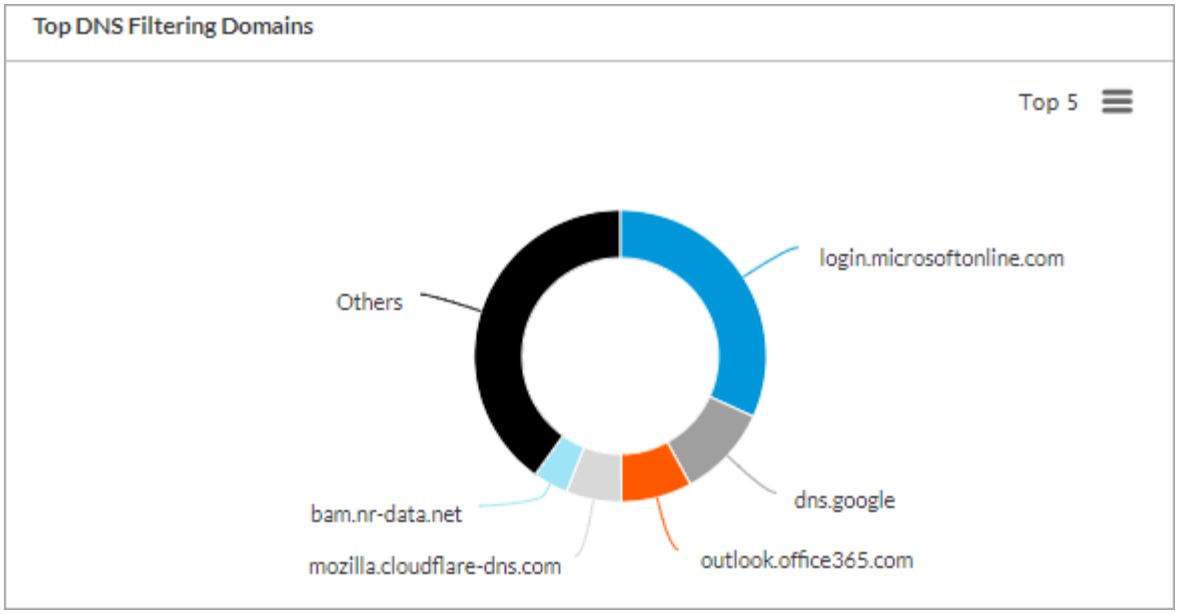
   - Top DNS filtering message types



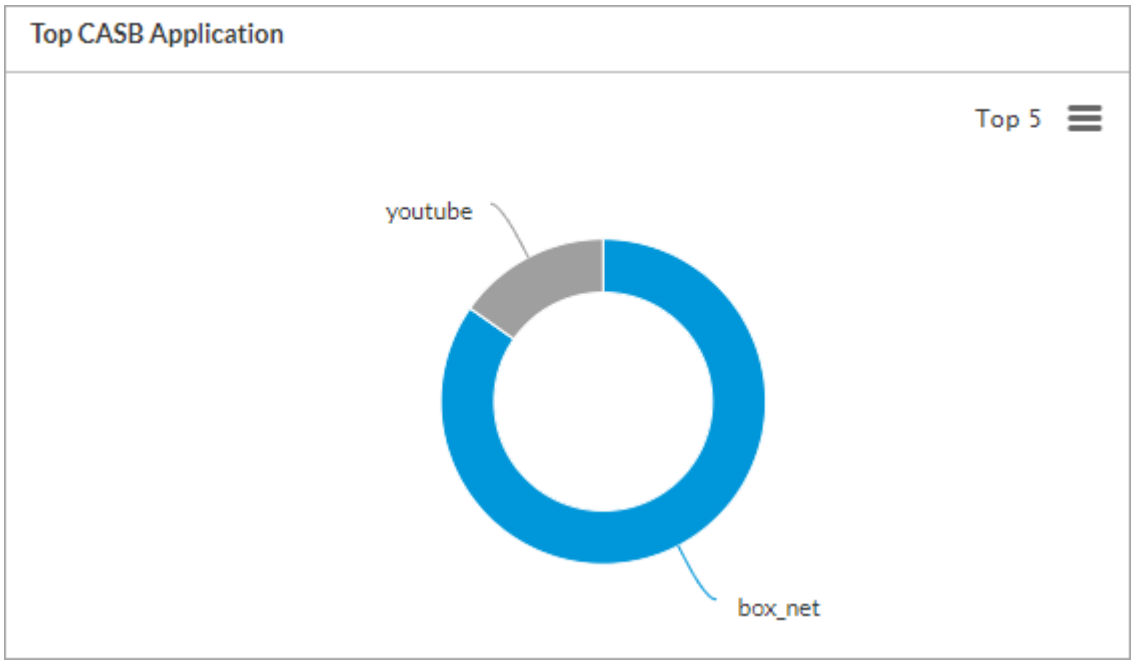
- Top DNS filtering action



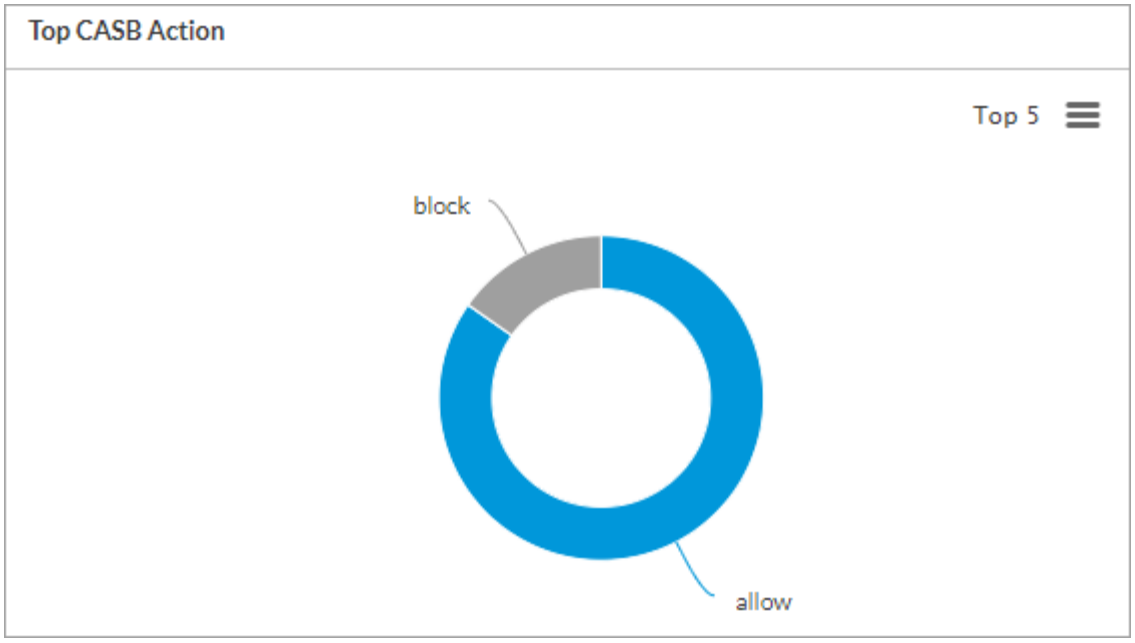
- Top DNS filtering domains



5. Select the CASB tab to view CASB statistics. The CASB tab displays the following panes:
   - Top CASB application

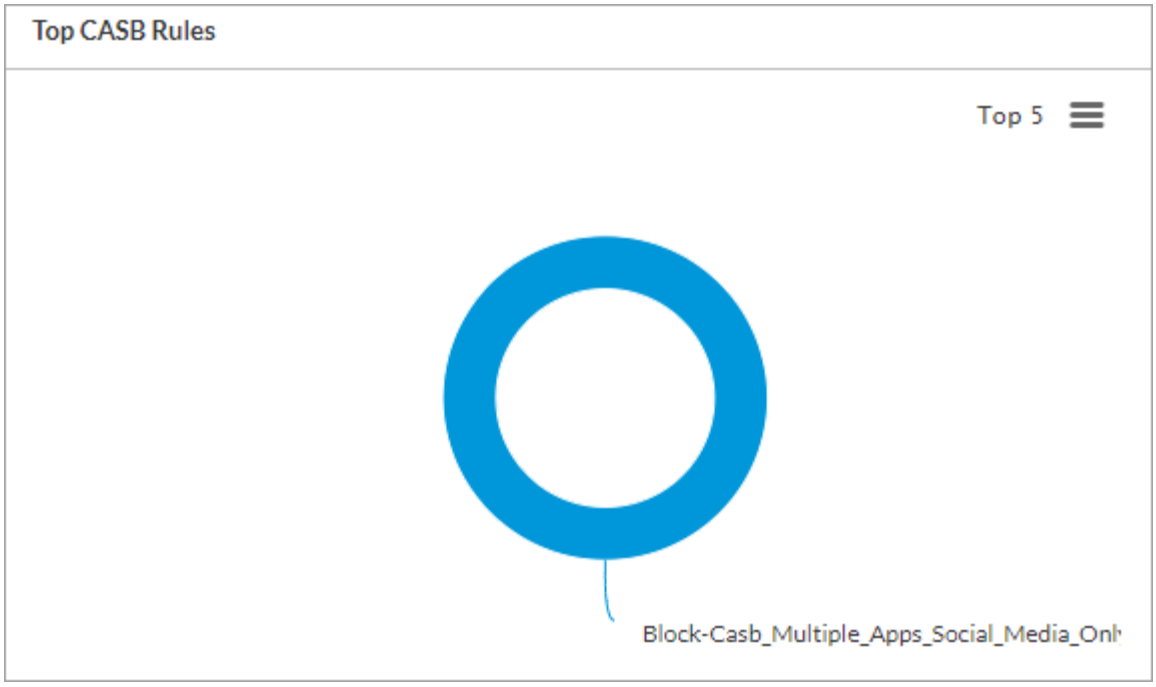


   - Top CASB action



- Top CASB users

- Top CASB rules



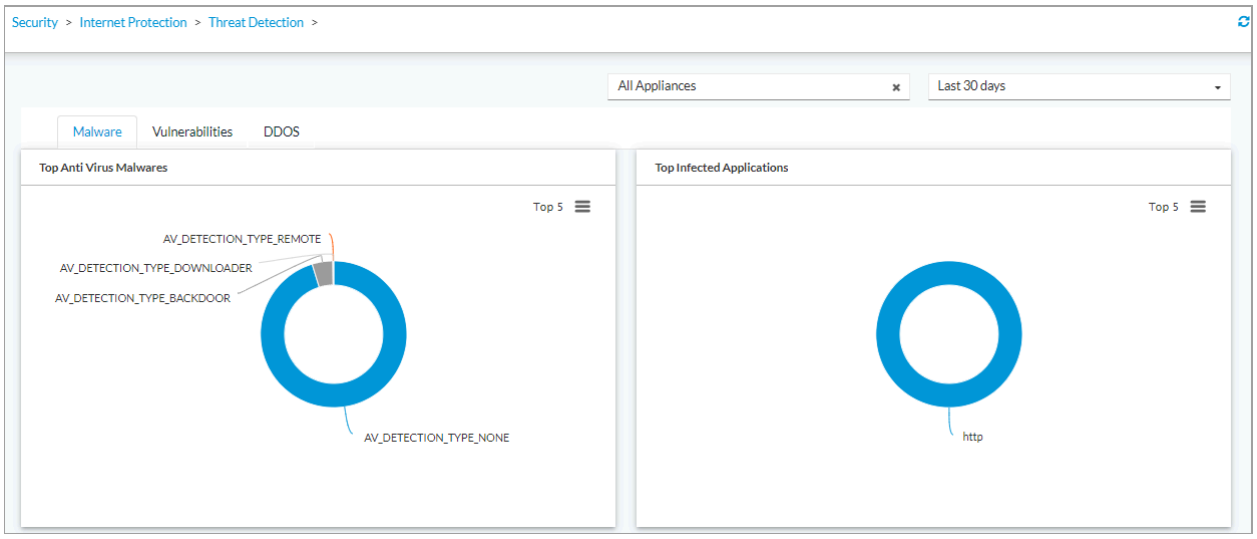
View Internet Protection Threat Detection

The Threat Filtering screen displays the following information:

- Malware—Statistics for top antivirus malware, infected applications, victims, and attackers.
- Vulnerabilities—Statistics for top threats, signature ID, source, and destination.
- Distributed denial-of-service (DDoS)—Statistics for DDoS attack.

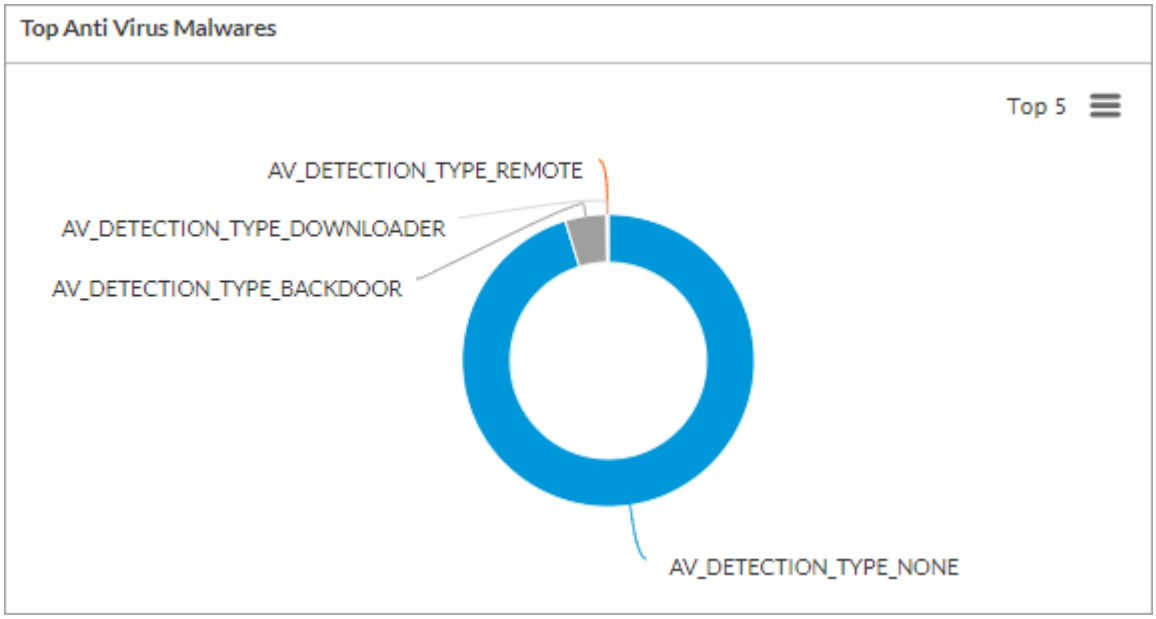
To display threat detection information:

1. Select View in the left navigation pane and then select the Security tab.
2. Select Internet Protection > Threat Detection. The Malware tab displays by default:

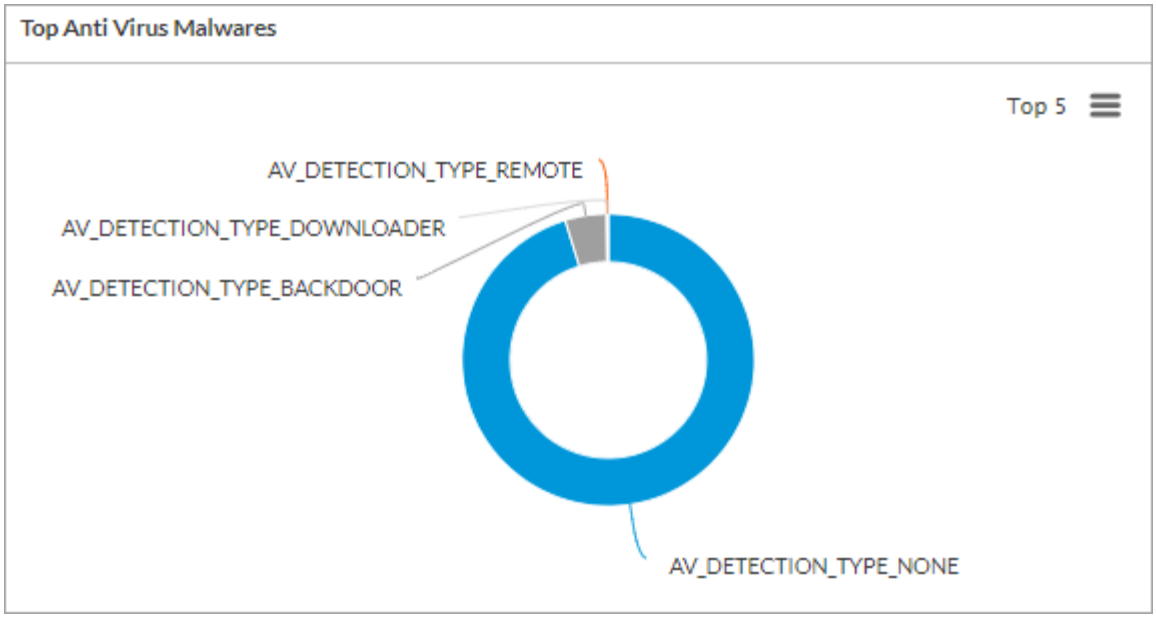


The Malware tab displays the following panes:

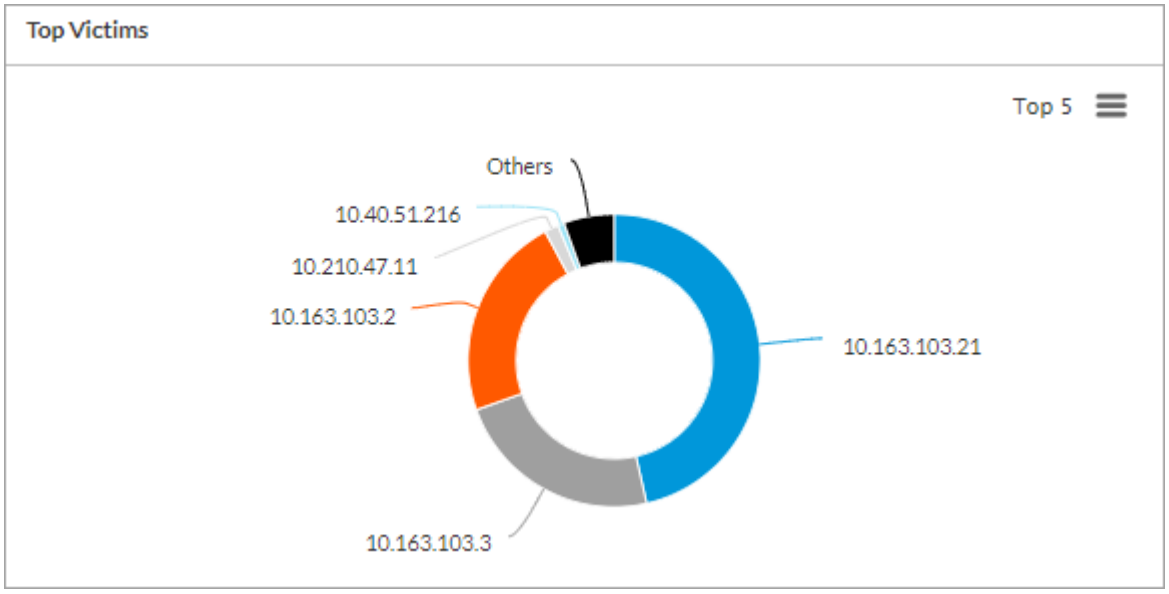
- Top antivirus malware



- Top infected applications

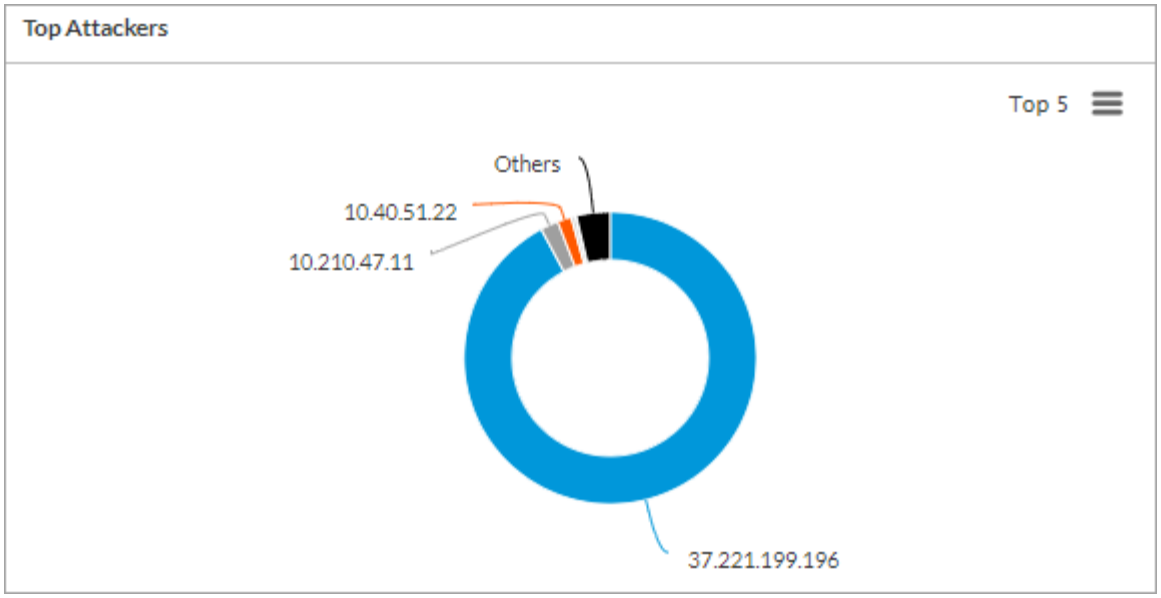


- Top victims

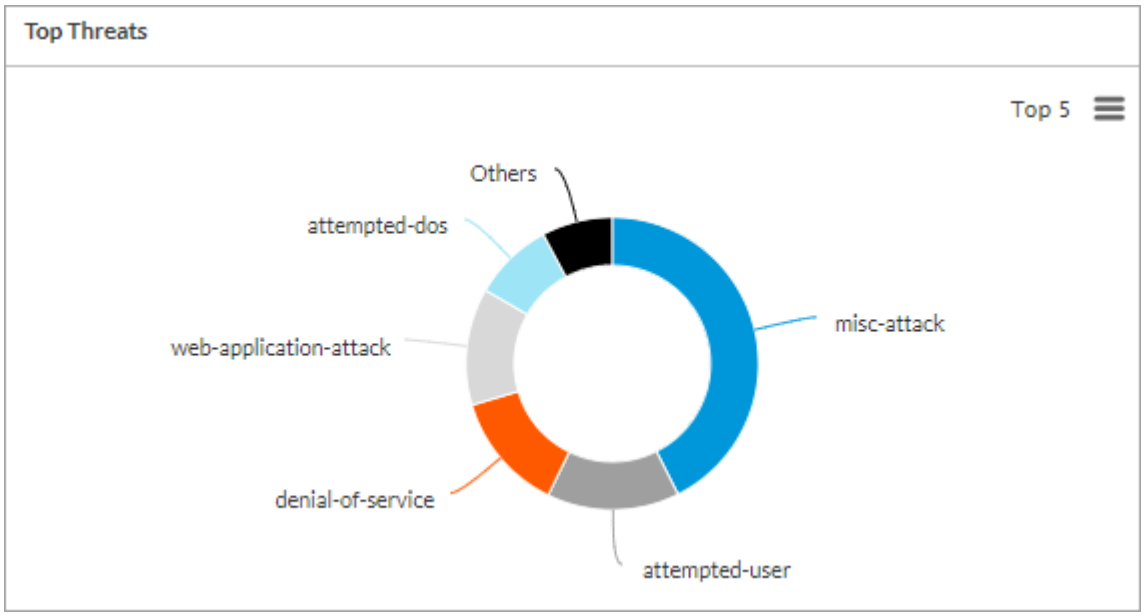


- Top attackers

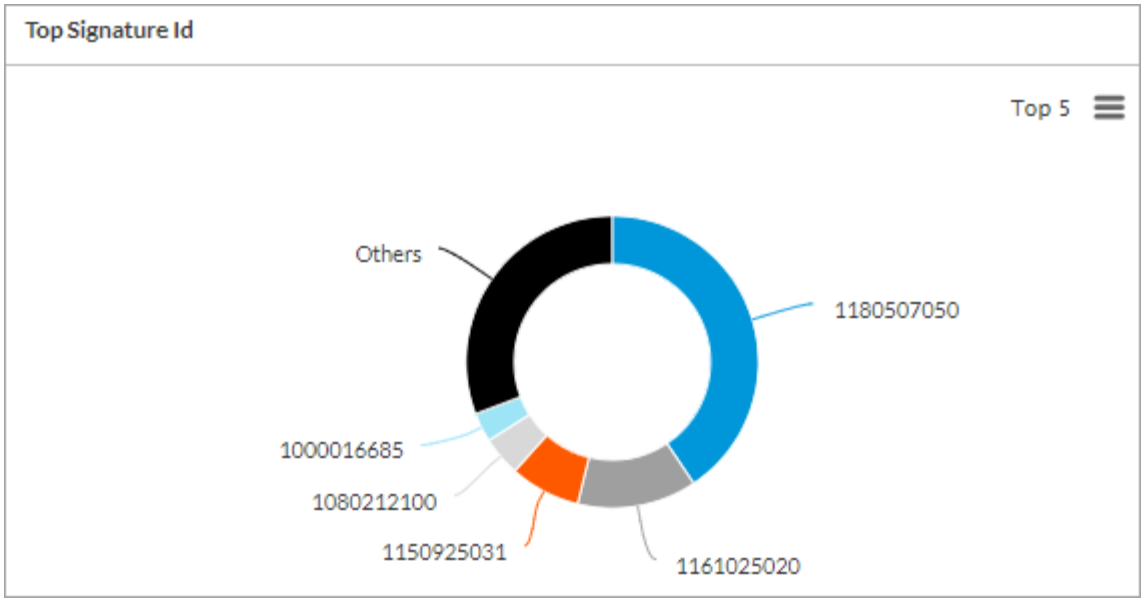
Updated: Wed, 23 Oct 2024 08:54:28 GMT



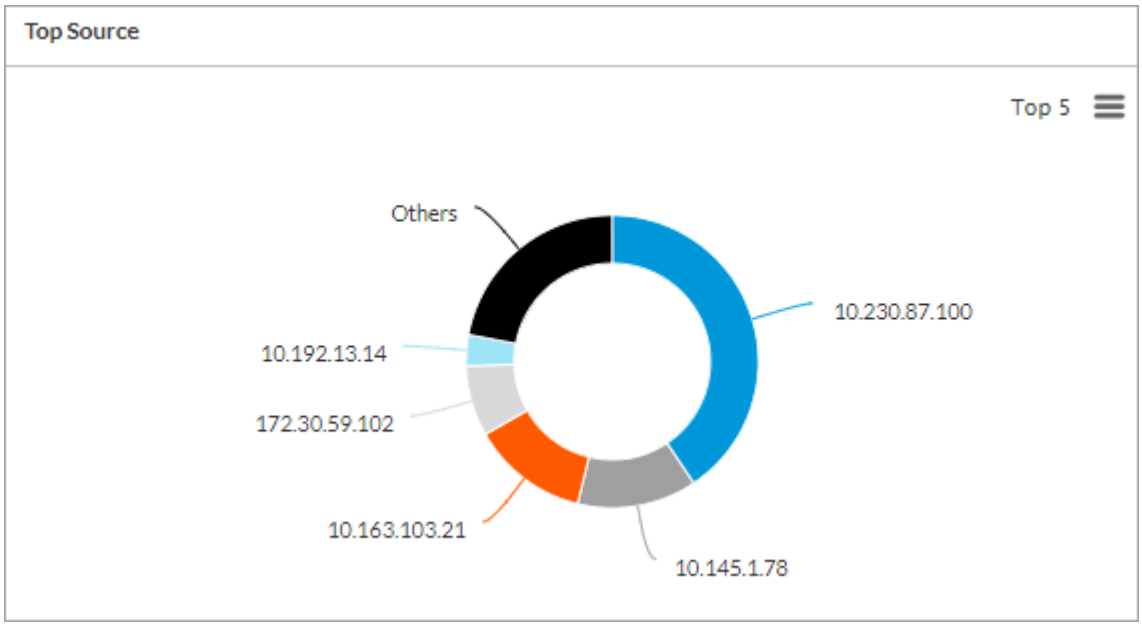
3. Select the Vulnerabilities tab to view vulnerabilities analytics. The Vulnerabilities tab displays the following panes:
   - Top threats



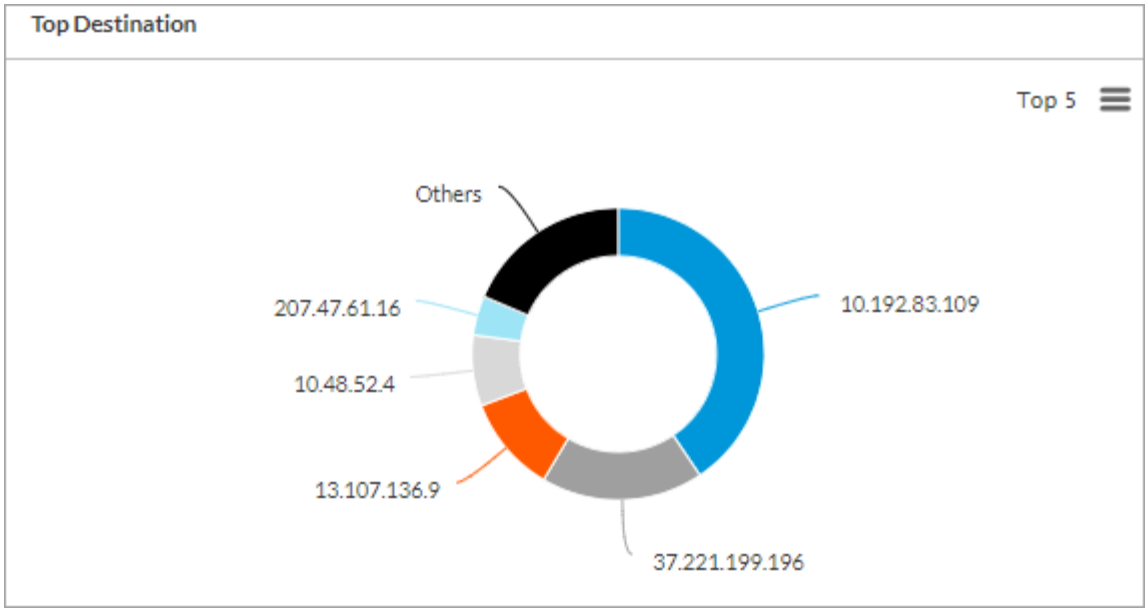
   - Top signature ID



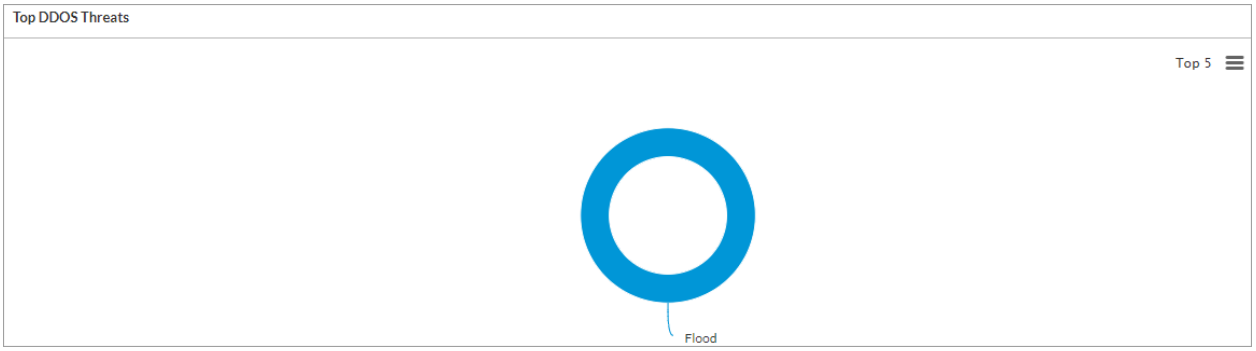
- Top source



- Top destination



4. Select the DDoS tab to view the analytical statistics for top DDoS attacks:



View Internet Protection DLP Statistics

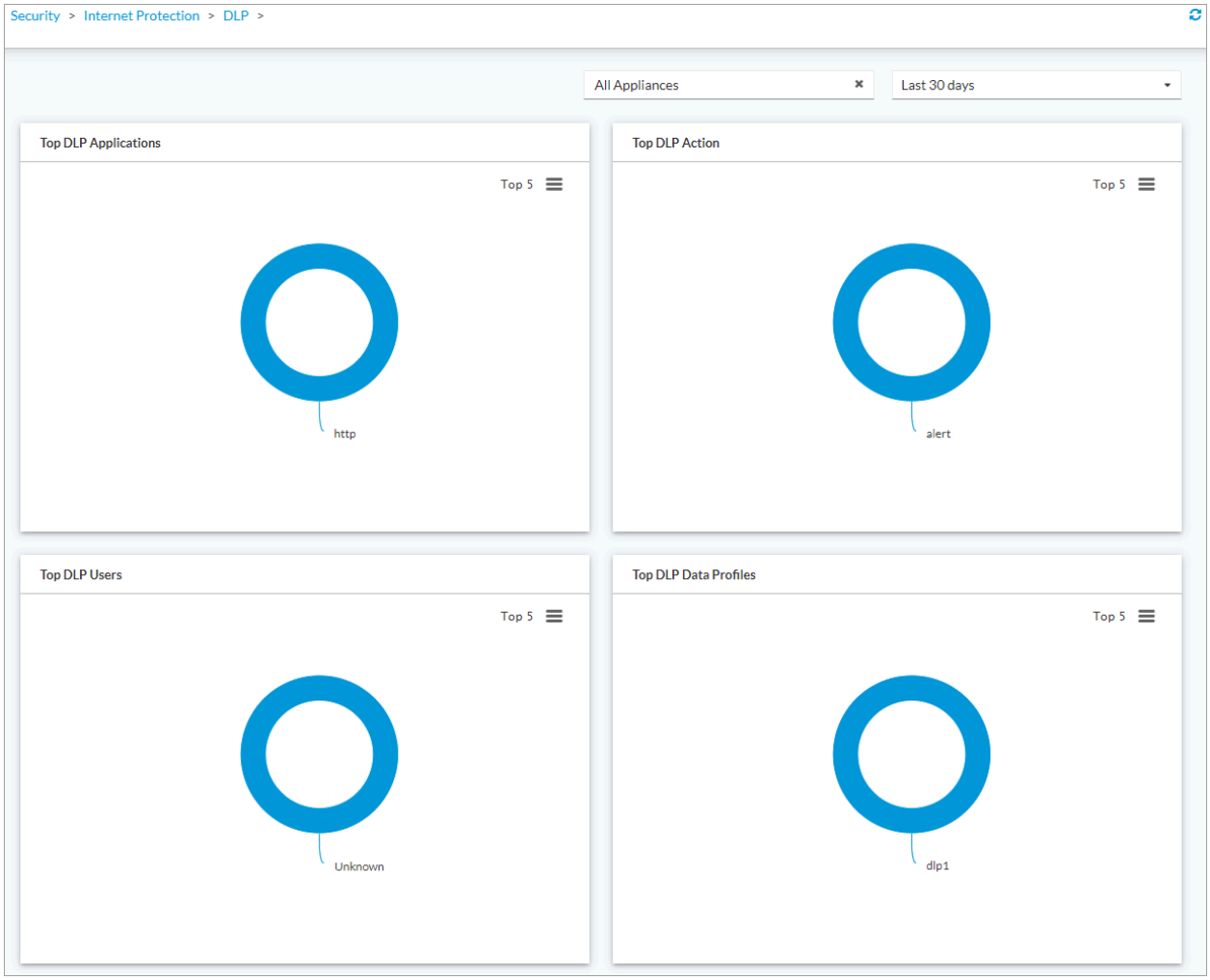
Data loss prevention (DLP) is a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. For more information, see Configure Data Loss Prevention in Concerto.

All Concerto DLP statistics are displayed on the View screen.

To display DLP statistics:

1. Select View in the left navigation pane and then select the Security tab.
2. Select Internet Protection > DLP. The DLP screen displays the following panes:
   - Top DLP applications
   - Top DLP action
   - Top DLP users

- Top DLP data profiles



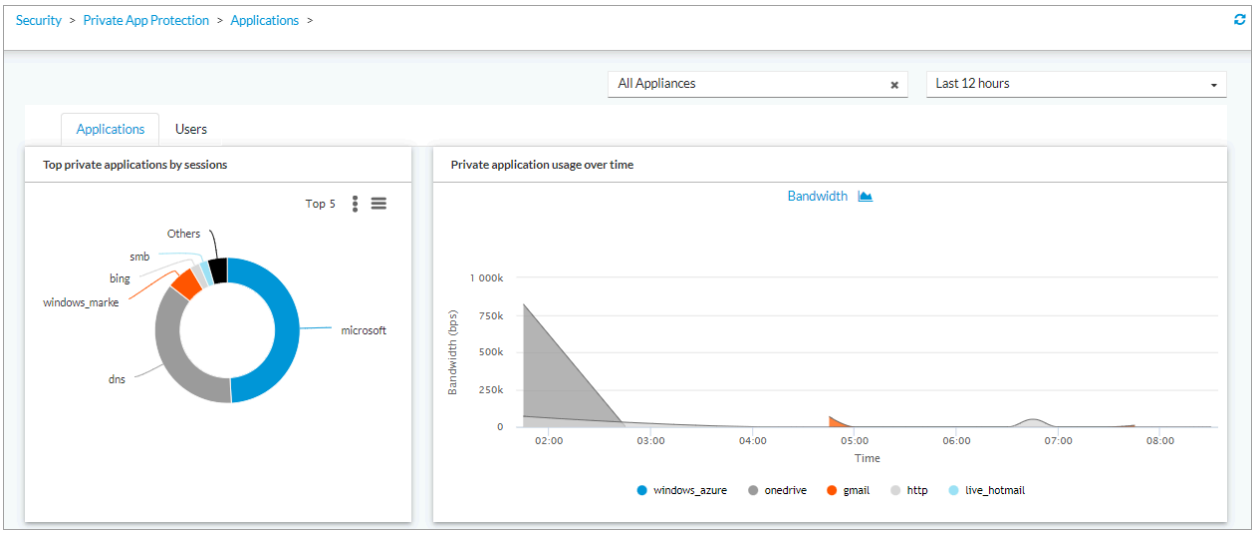
View Private Application Protection Information for Applications

The private application protection applications screen displays the analytical statistics of private application usage and usage of these applications by users:

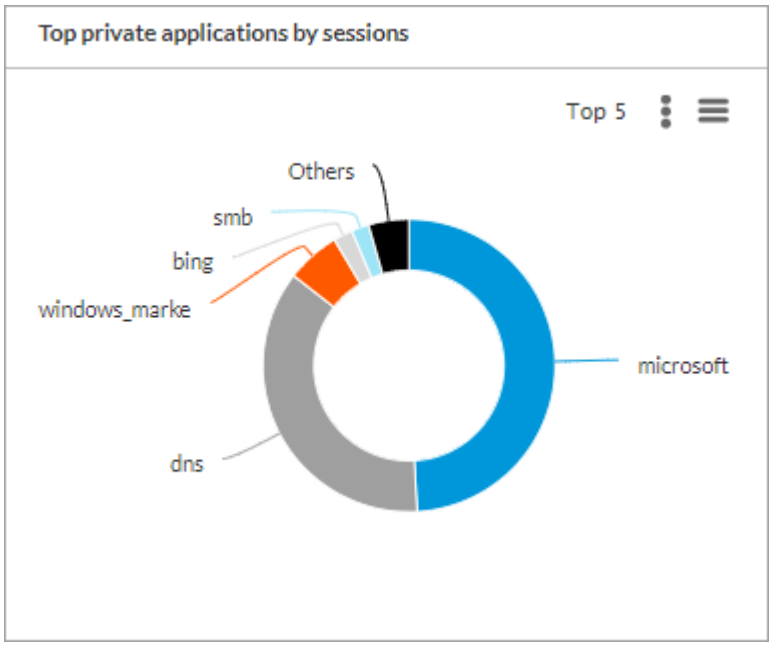
- Applications—Displays statistics for private applications by sessions (percentage and number of sessions), usage over time, usage data.
- Users—Displays statistics for private application users by usage of applications, usage over time, and usage data.

To display private applications information:

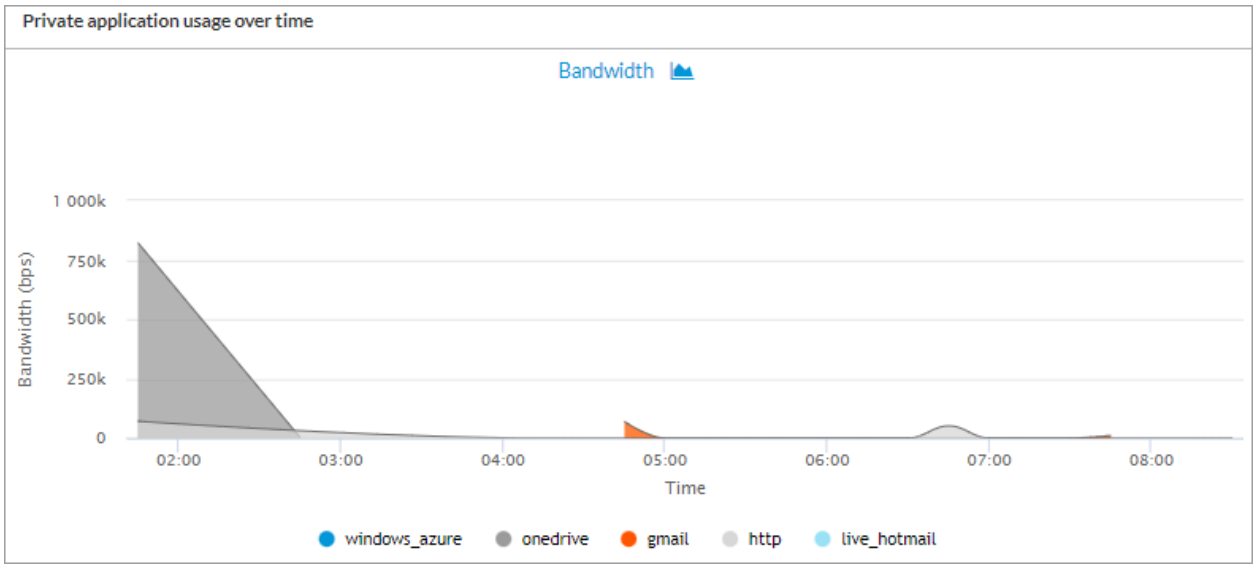
1. Select View in the left navigation pane and then select the Security tab.
2. Select Private App Protection > Applications.



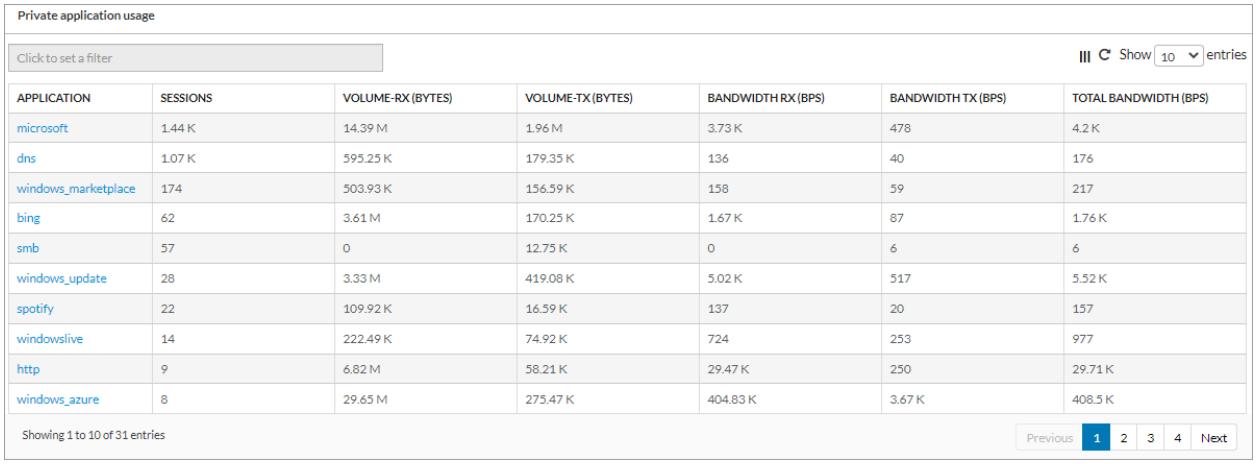
3. Select the Applications tab to view analytical statistics of applications. The Applications tab displays the following panes:
   - Top private applications by sessions. Click any application in the graph to view details.



   - Private application usage over time



- Private application usage (table)



Private application usage

Click to set a filter

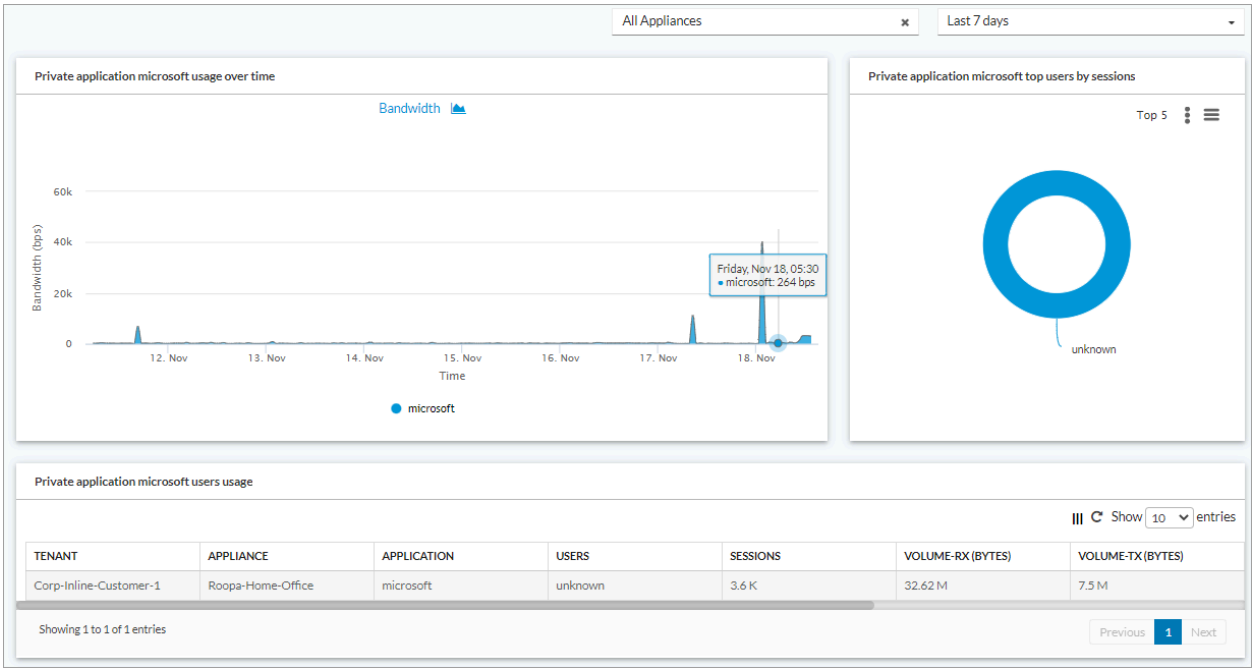
Show 10 entries

APPLICATION	SESSIONS	VOLUME-RX (BYTES)	VOLUME-TX (BYTES)	BANDWIDTH RX (BPS)	BANDWIDTH TX (BPS)	TOTAL BANDWIDTH (BPS)
microsoft	1.44 K	14.39 M	1.96 M	3.73 K	478	4.2 K
dns	1.07 K	595.25 K	179.35 K	136	40	176
windows_marketplace	174	503.93 K	156.59 K	158	59	217
bing	62	3.61 M	170.25 K	1.67 K	87	1.76 K
smb	57	0	12.75 K	0	6	6
windows_update	28	3.33 M	419.08 K	5.02 K	517	5.52 K
spotify	22	109.92 K	16.59 K	137	20	157
windowslive	14	222.49 K	74.92 K	724	253	977
http	9	6.82 M	58.21 K	29.47 K	250	29.71 K
windows_azure	8	29.65 M	275.47 K	404.83 K	3.67 K	408.5 K

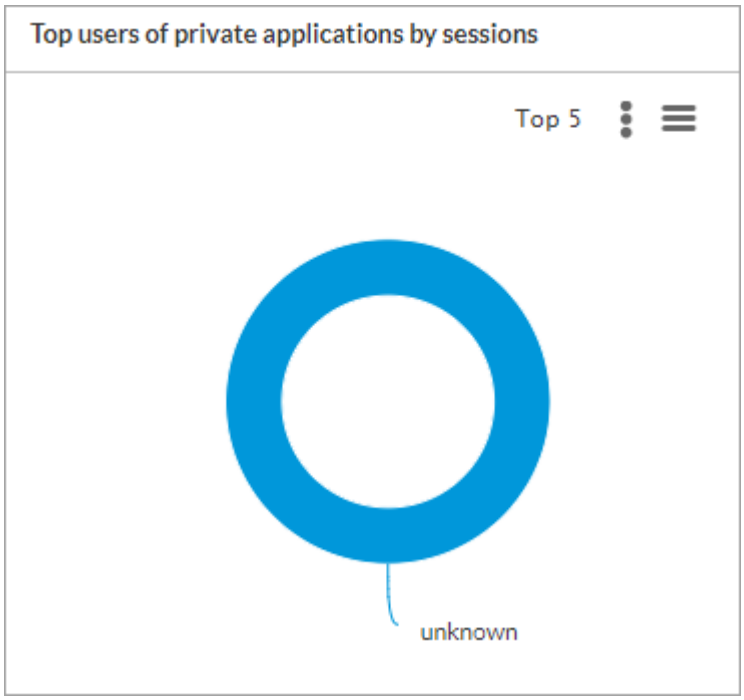
Showing 1 to 10 of 31 entries

Previous 1 2 3 4 Next

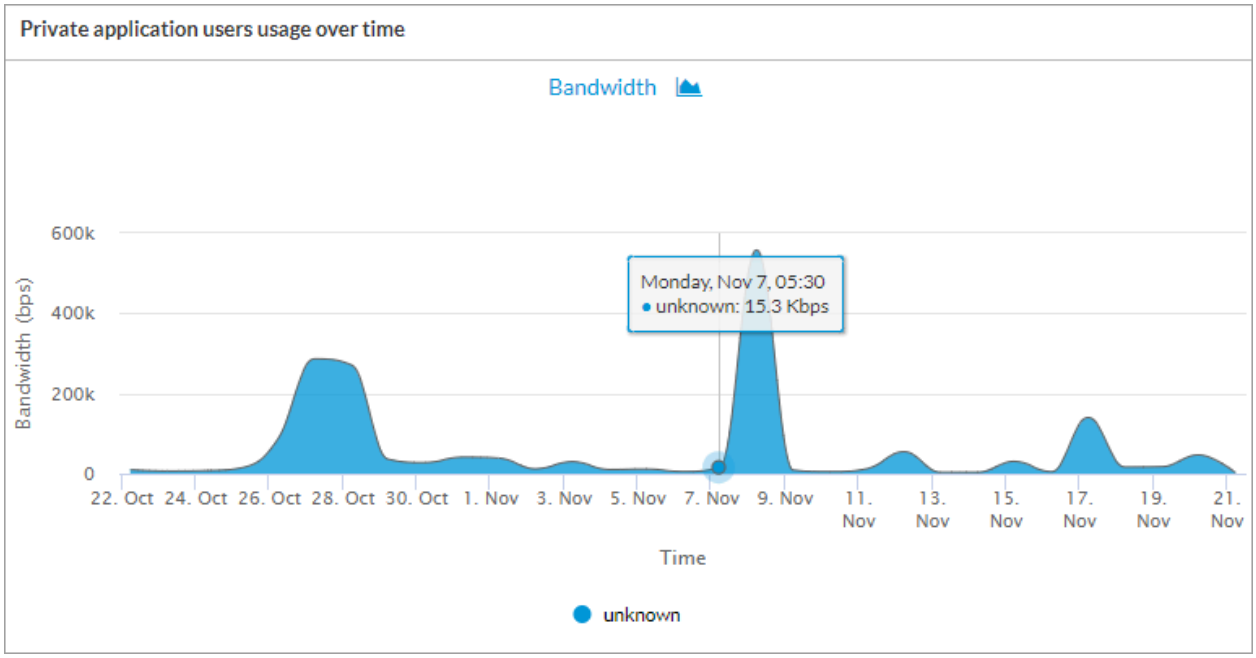
Click an application name in the table above or in the Top Private Applications by Sessions graph to view details of an application. For example:



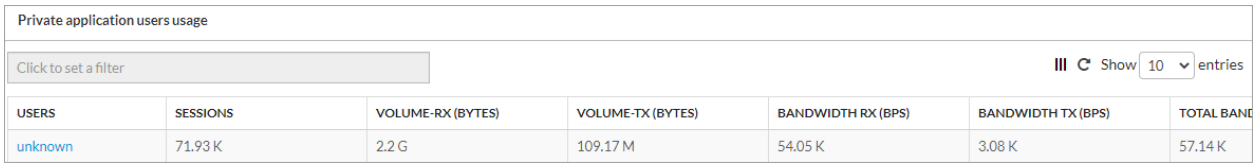
4. Select the Users tab to view analytical statistics of application usage by users. The Users tab displays the following panes:
   - Top users of private applications by sessions



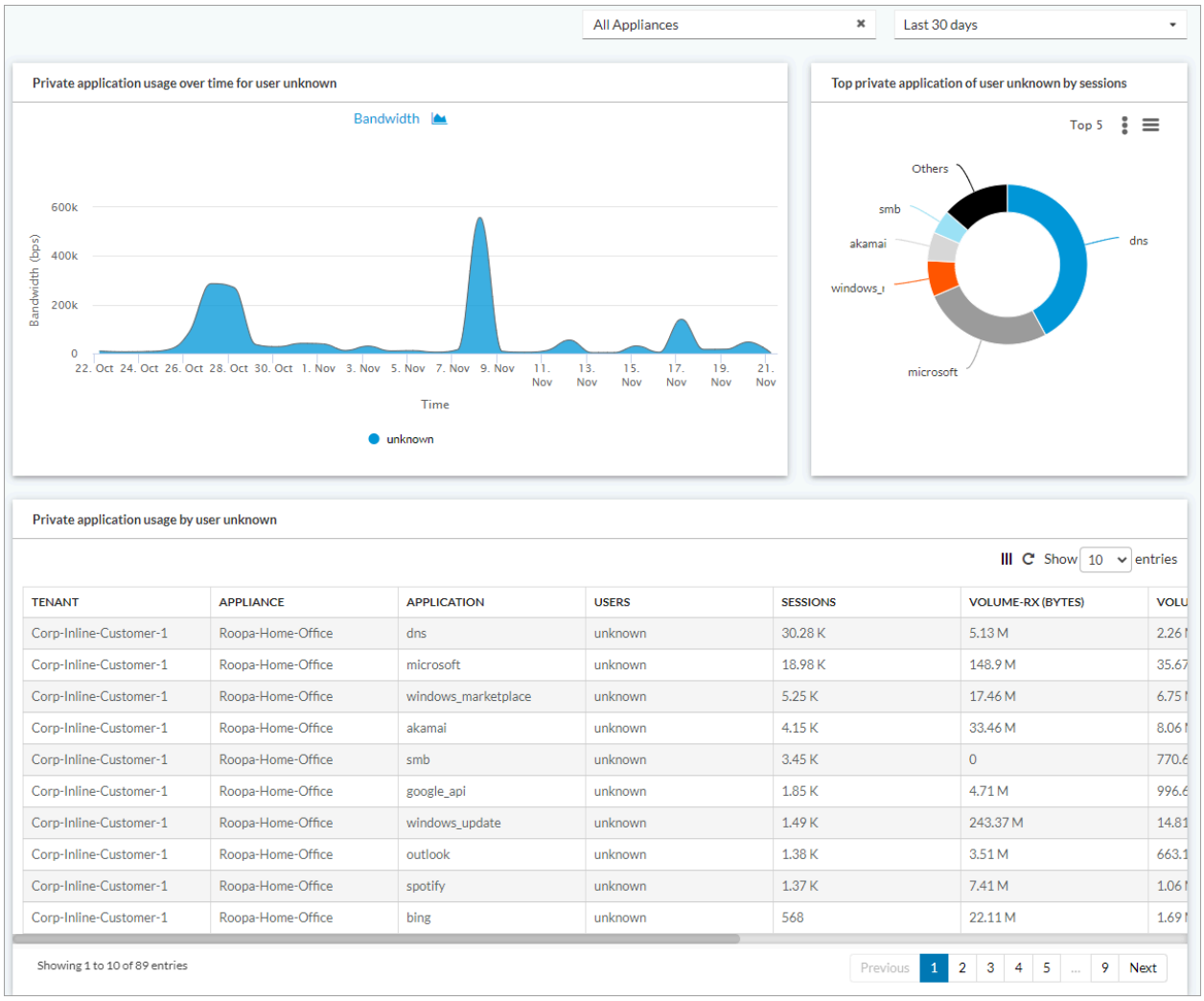
   - Private application users usage over time



- Private application users usage (table)



- Click an user name in the table above or in the Top Users of Private Applications by Sessions graph to view details of a user. For example:



View Private Application Protection Information Threat Detection Information

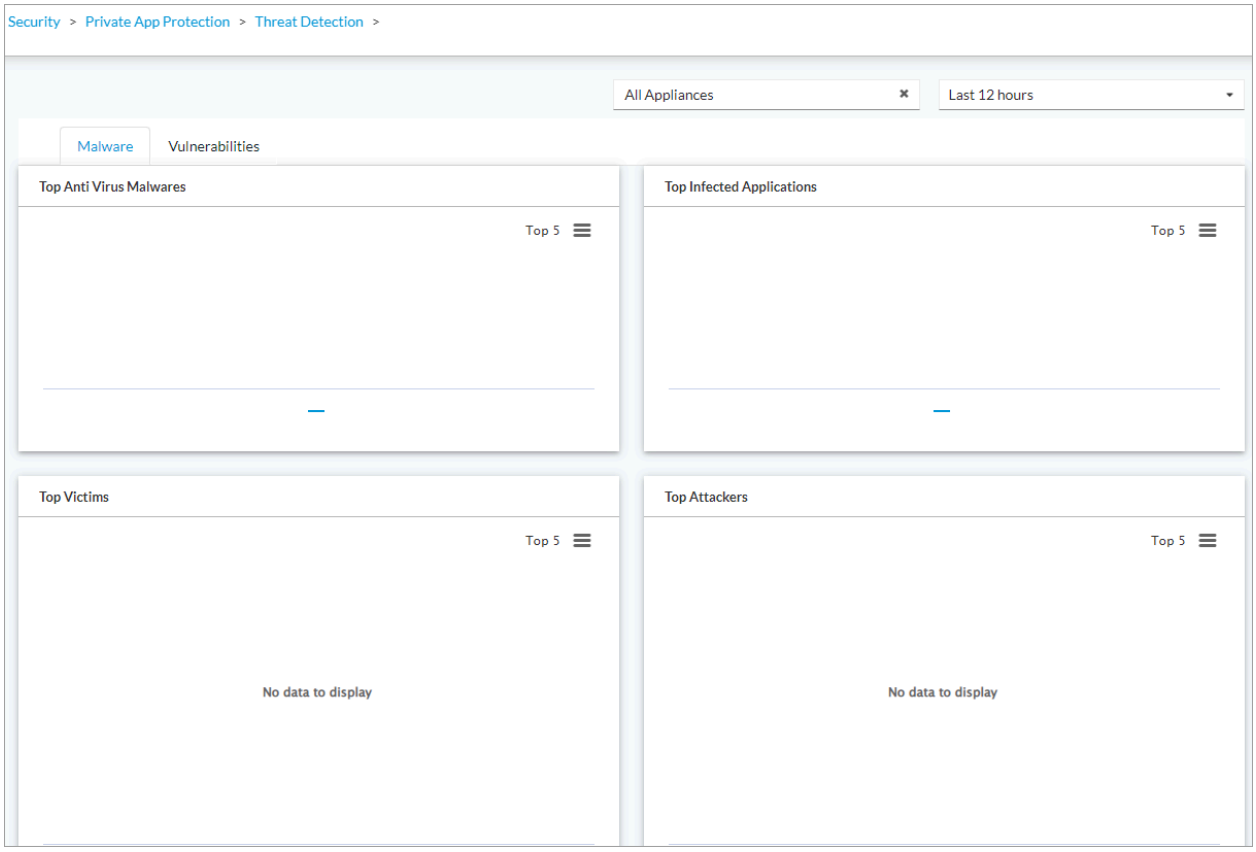
The private application protection threat detection screen displays the analytical statistics of malware and vulnerabilities of private applications:

- Malware—Displays analytical statistics for malware attack on applications.
- Vulnerabilities—Displays analytical statistics for vulnerabilities of applications.

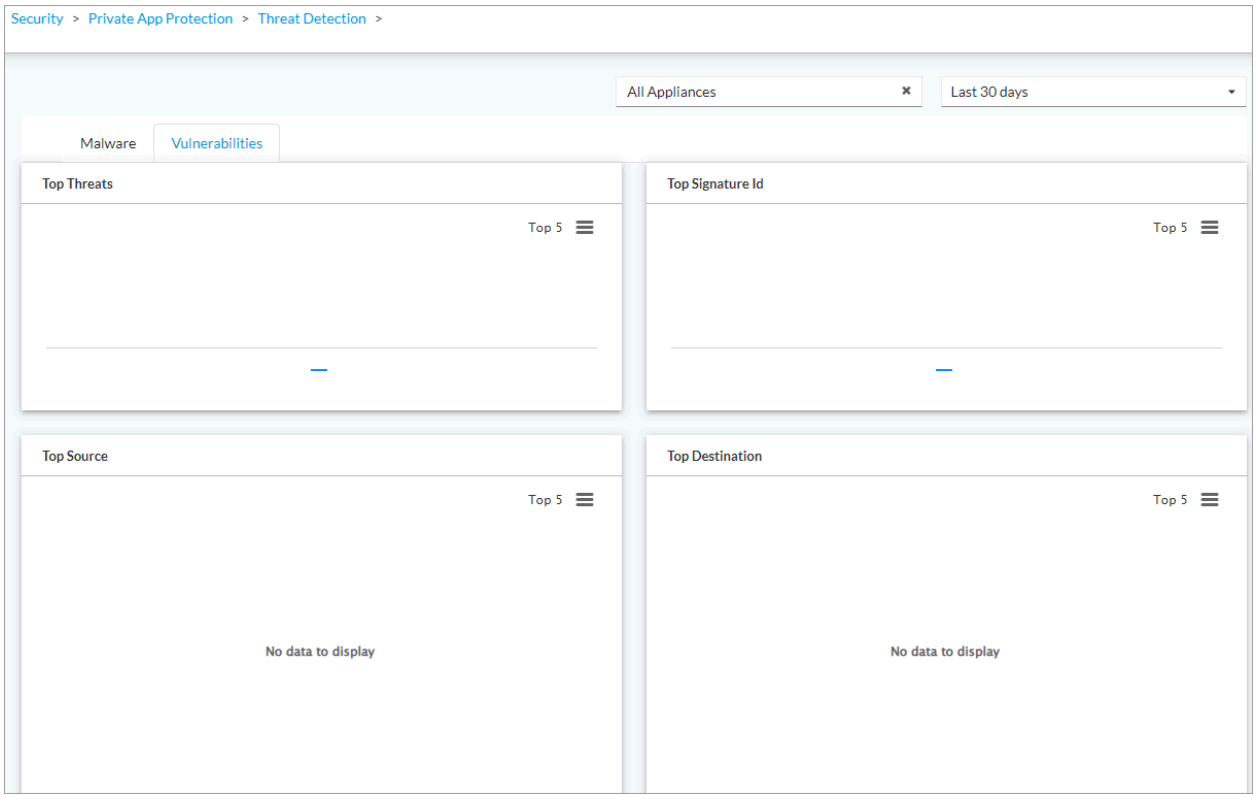
To display threat detection for private applications:

1. Select View in the left navigation pane and then select the Security tab.
2. Select Private App Protection > Threat Detection.
3. Select the Malware tab (default) to display information of infected applications. The Malware tab displays the following panes:
    - Top Antivirus Malware

- Top Infected Applications
- Top Victims
- Top Attackers



4. Select the Vulnerabilities tab to display vulnerability information of applications. The Vulnerabilities tab displays the following panes:
   - Top Threats
   - Top Signature ID
   - Top Source
   - Top Destination



View Secure SD-WAN Information

You can manage SD-WAN networks analytical statistics, build and manage reporting, and view device settings from the Secure SD-WAN menu under View.

Secure SD-WAN Overview Tab

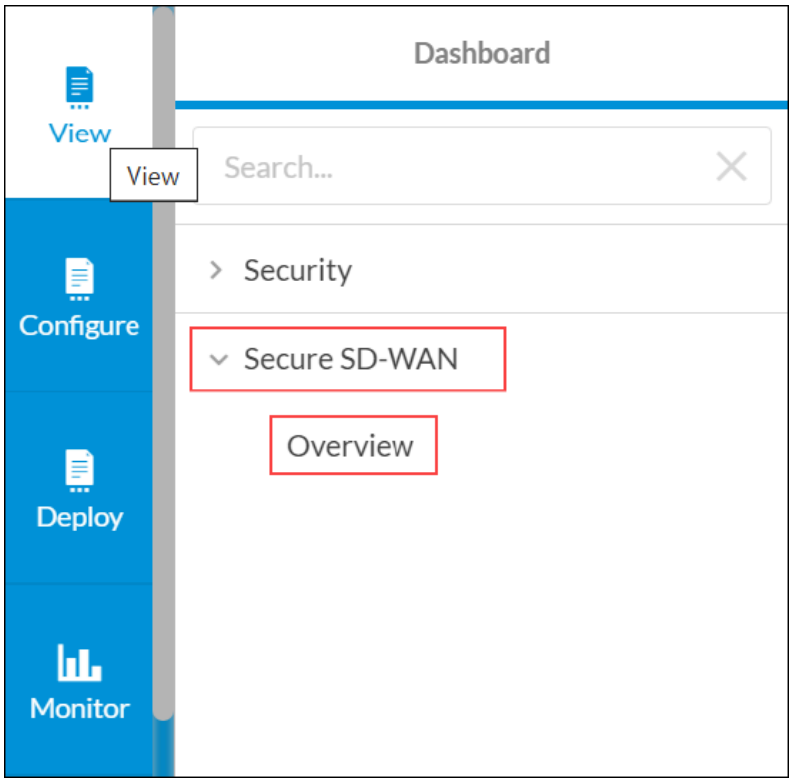
The Secure SD-WAN Overview tab displays the following real-time statistics of devices by default:

- Total number of devices in the tenant network
- Alarming devices with number of critical and major alarms
- Number of WAN links down
- Number of devices that are up and down
- Tenant health and asset summary
- Historical statistics of devices

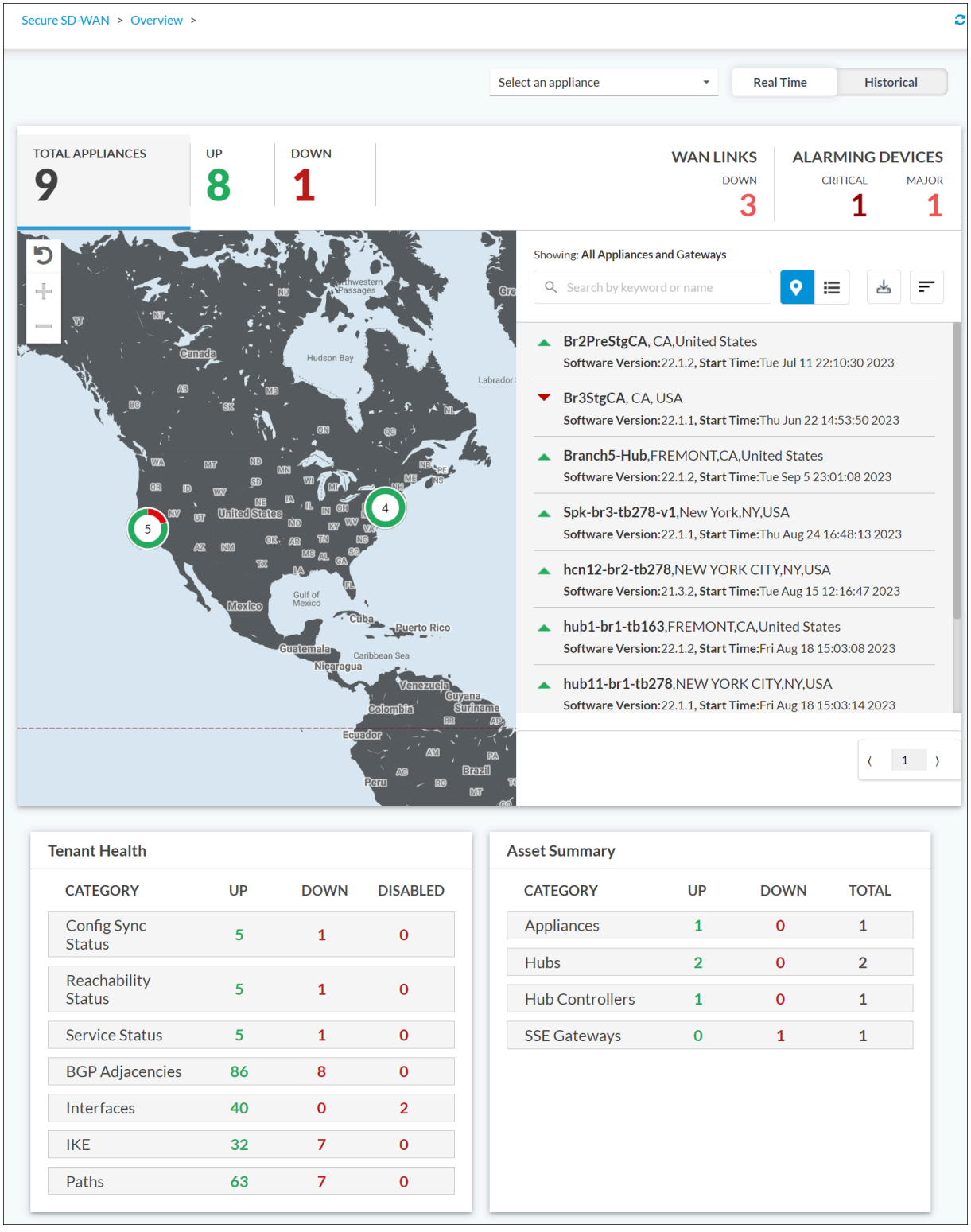
View Real-Time Information

To view real-time information about devices:

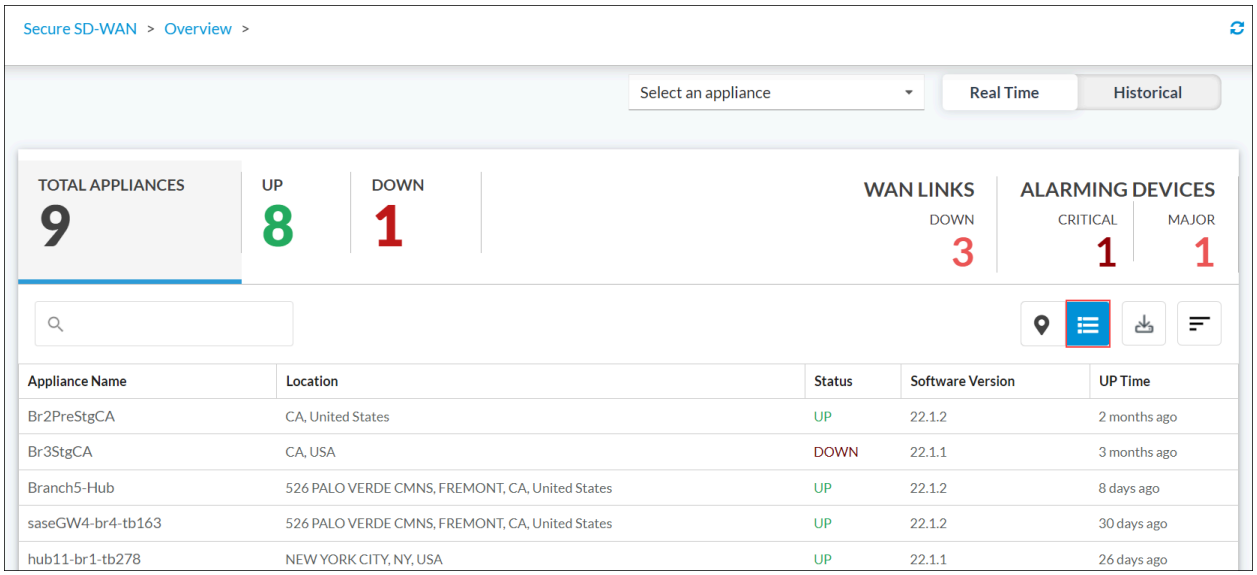
1. In Tenant view, go to the View lifecycle in the left menu bar.
2. Select Secure SD-WAN > Overview.



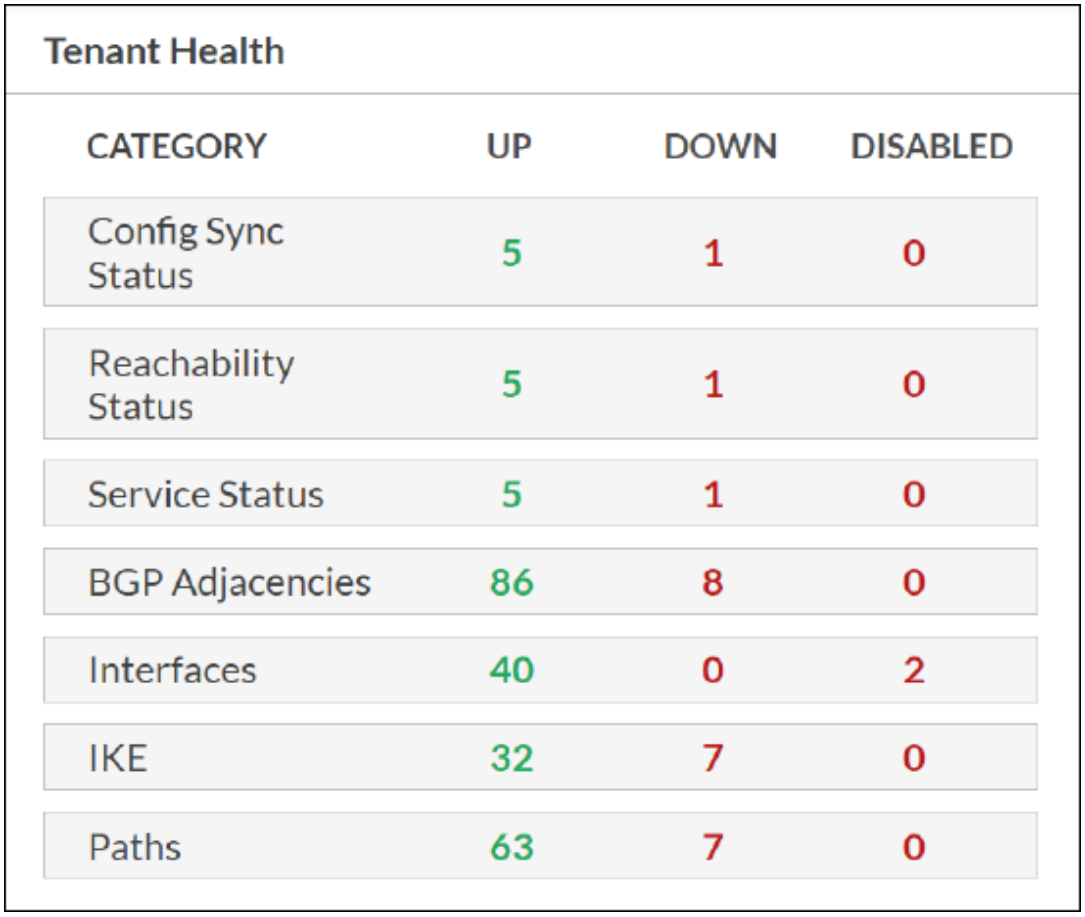
The Overview page displays the real-time statistics of devices with map view by default.



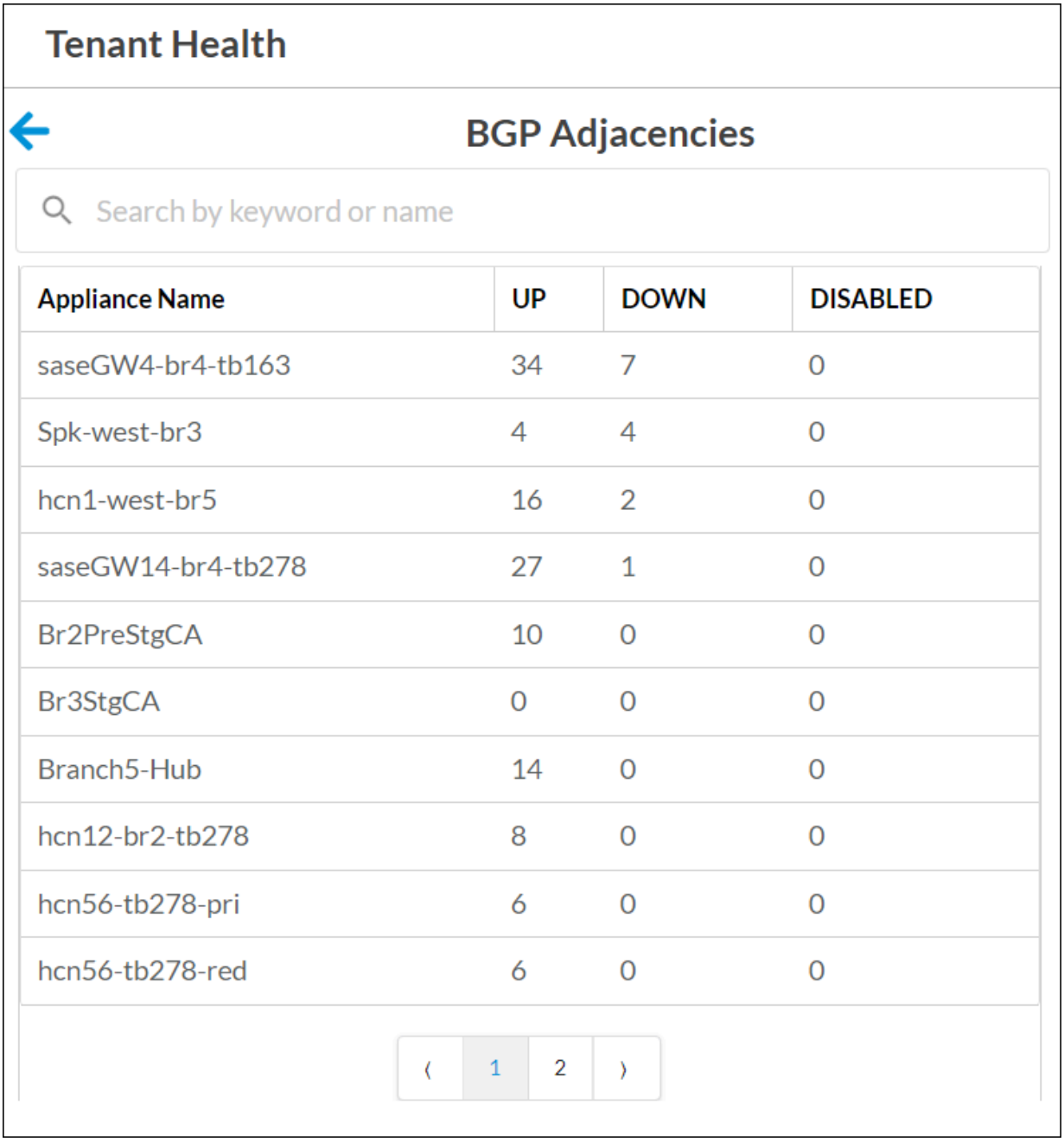
3. To display the devices in the network as a list, click List View.



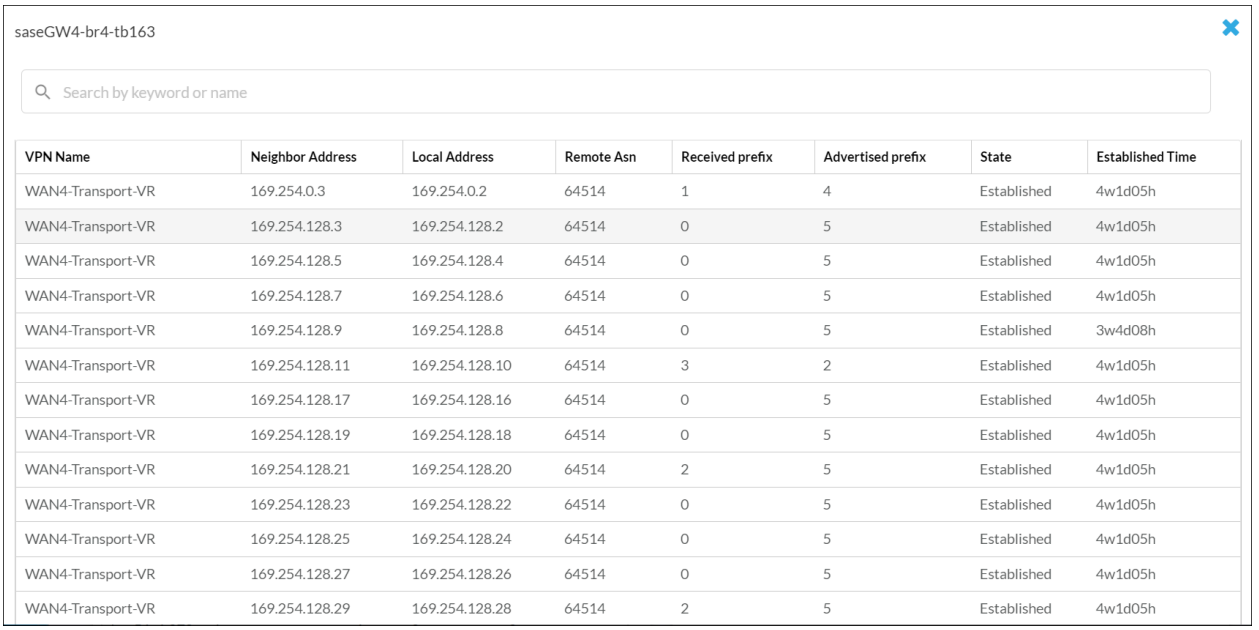
4. To download a file in CSV format containing the information about the devices and gateways, click the Download CSV icon .
5. In the Tenant Health section, click any category to view the service status.
   - Configuration Sync Status—Whether the configuration on the device is in sync with the configuration in the Concerto node's database
   - Reachability Status—Whether the device is reachable from the Concerto node
   - Service Status—Status of the services running on the device
   - BGP Adjacencies—Number of BGP peering sessions that are up (green), down (red), and disabled (red)
   - Interfaces—Number of interfaces that are up (green), down (red), and disabled (red)
   - IKE—Number of IKE connections that are up (green), down (red), and disabled (red)
   - Paths—Number of SD-WAN paths that are up (green), down (red), and disabled (red)



- The following screens display examples of tenant health status for various services and device information:
  - BGP Adjacencies

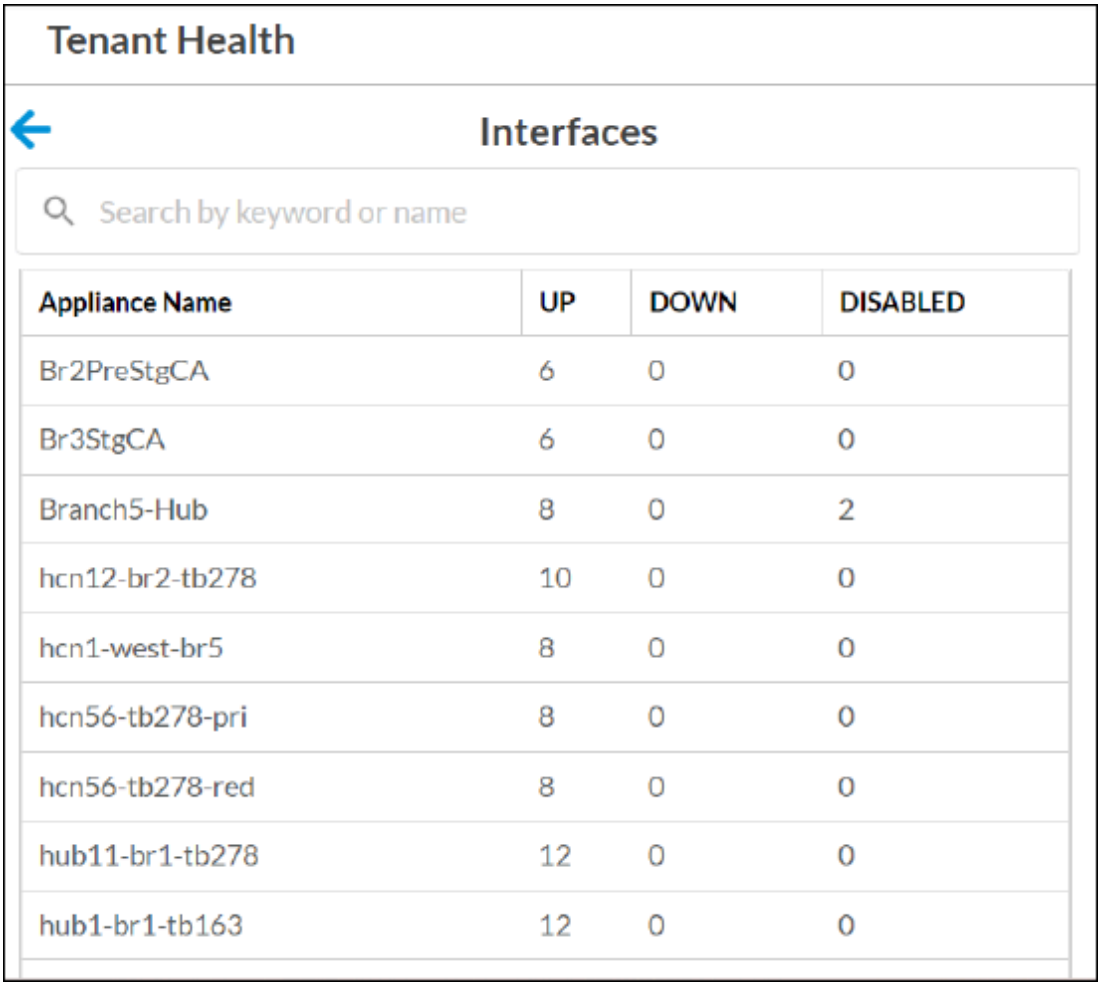


- To view the BGP adjacency information for a device, click the device name.

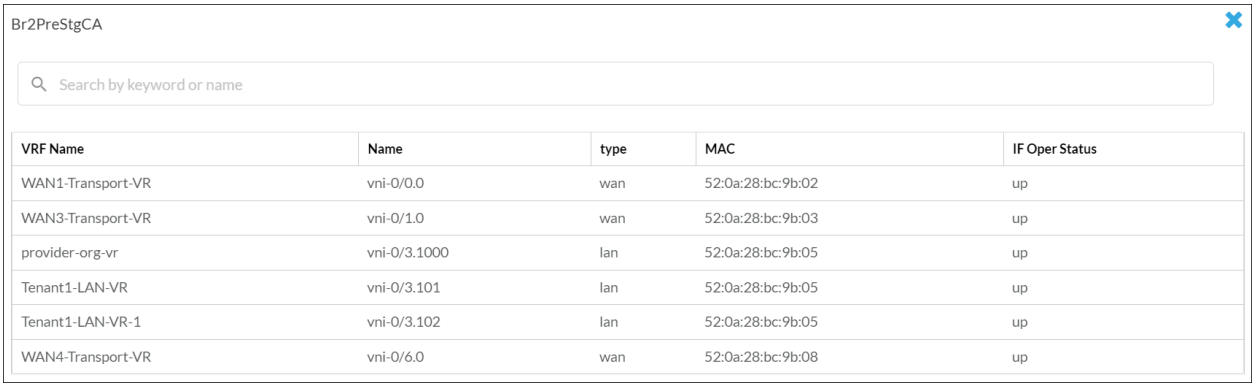


VPN Name	Neighbor Address	Local Address	Remote Asn	Received prefix	Advertised prefix	State	Established Time
WAN4-Transport-VR	169.254.0.3	169.254.0.2	64514	1	4	Established	4w1d05h
WAN4-Transport-VR	169.254.128.3	169.254.128.2	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.5	169.254.128.4	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.7	169.254.128.6	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.9	169.254.128.8	64514	0	5	Established	3w4d08h
WAN4-Transport-VR	169.254.128.11	169.254.128.10	64514	3	2	Established	4w1d05h
WAN4-Transport-VR	169.254.128.17	169.254.128.16	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.19	169.254.128.18	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.21	169.254.128.20	64514	2	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.23	169.254.128.22	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.25	169.254.128.24	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.27	169.254.128.26	64514	0	5	Established	4w1d05h
WAN4-Transport-VR	169.254.128.29	169.254.128.28	64514	2	5	Established	4w1d05h

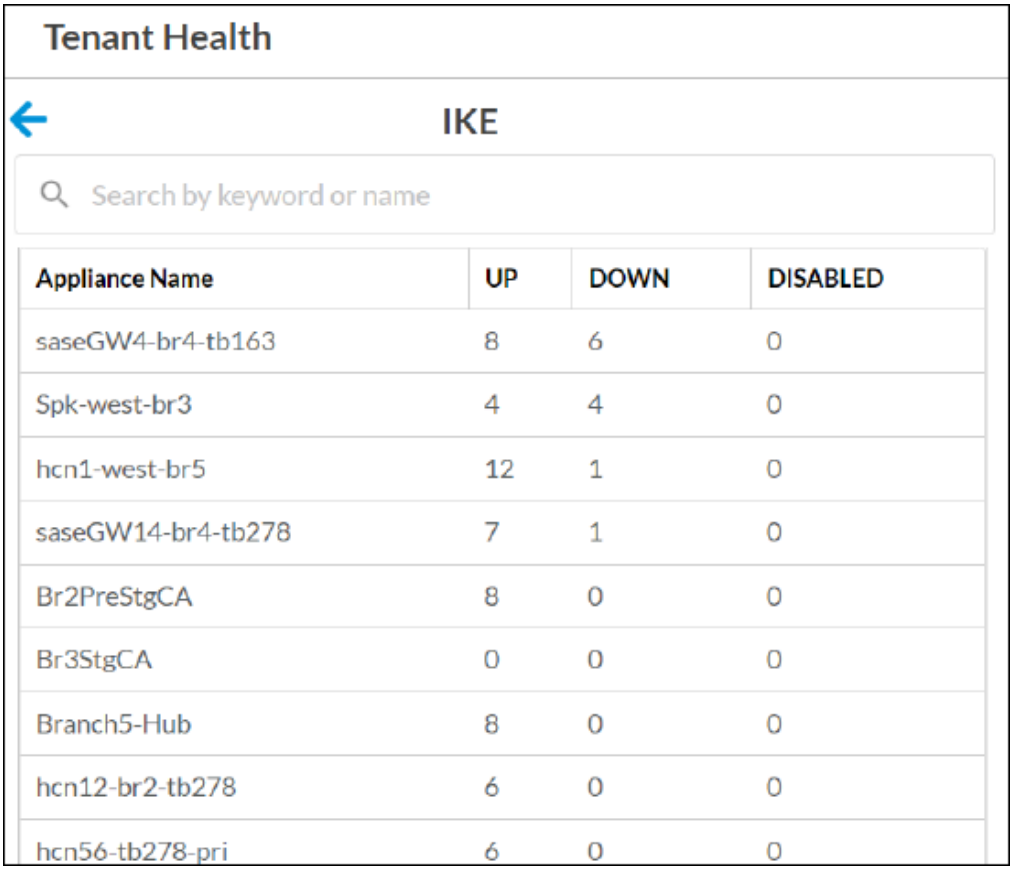
- Interfaces



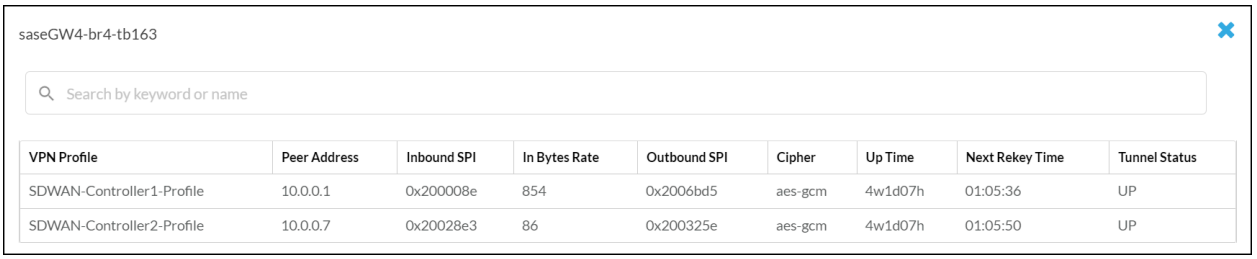
- To view interface information for a device, click the device name.



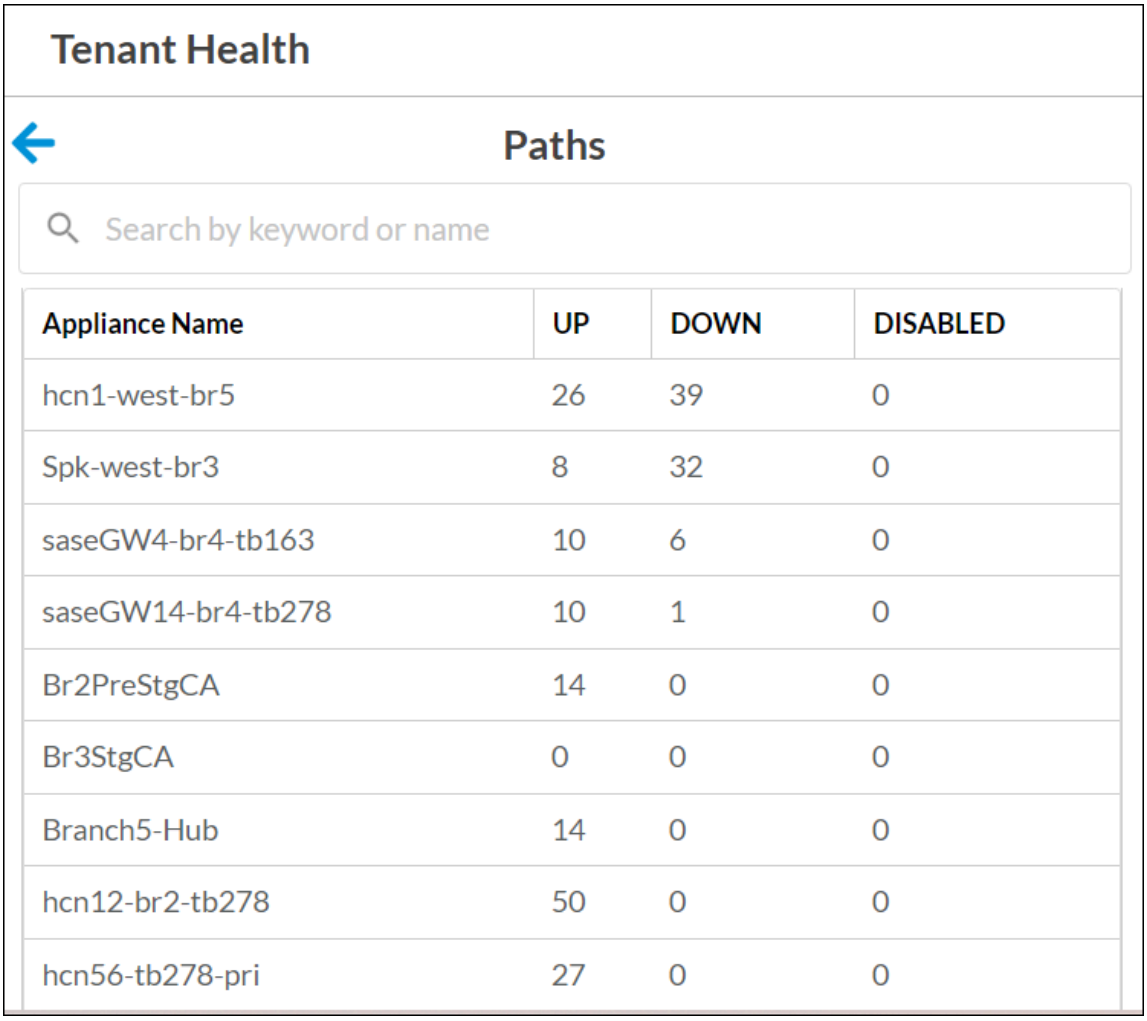
- IKE



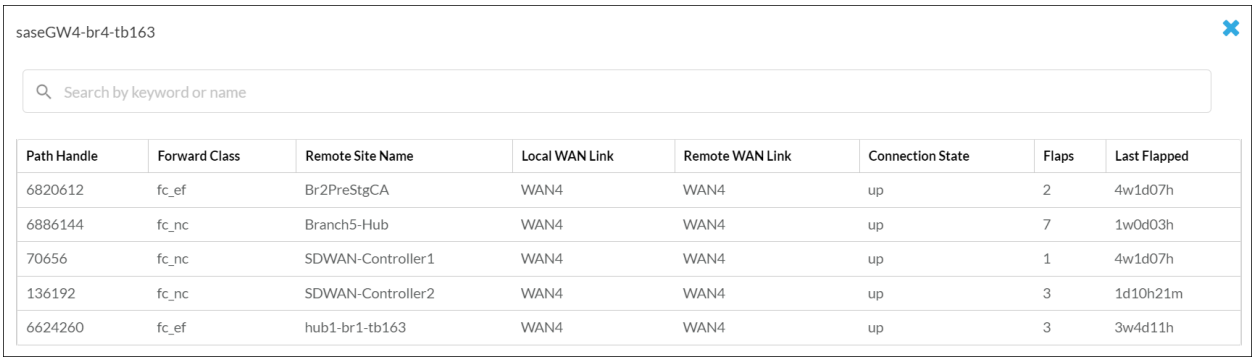
- To view the IKE information for a device, click the device name.



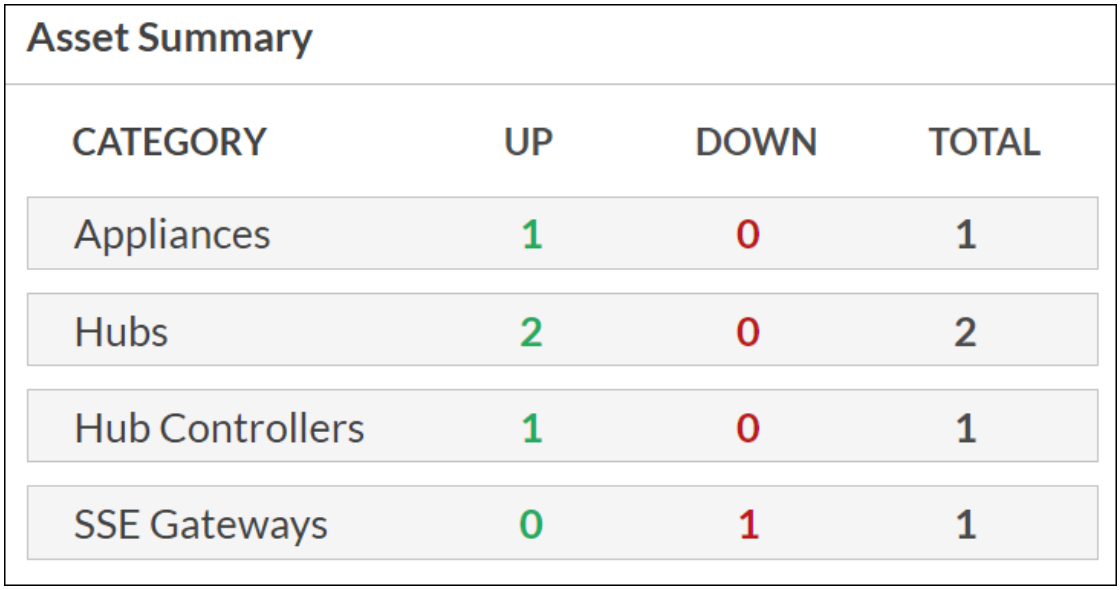
- Paths



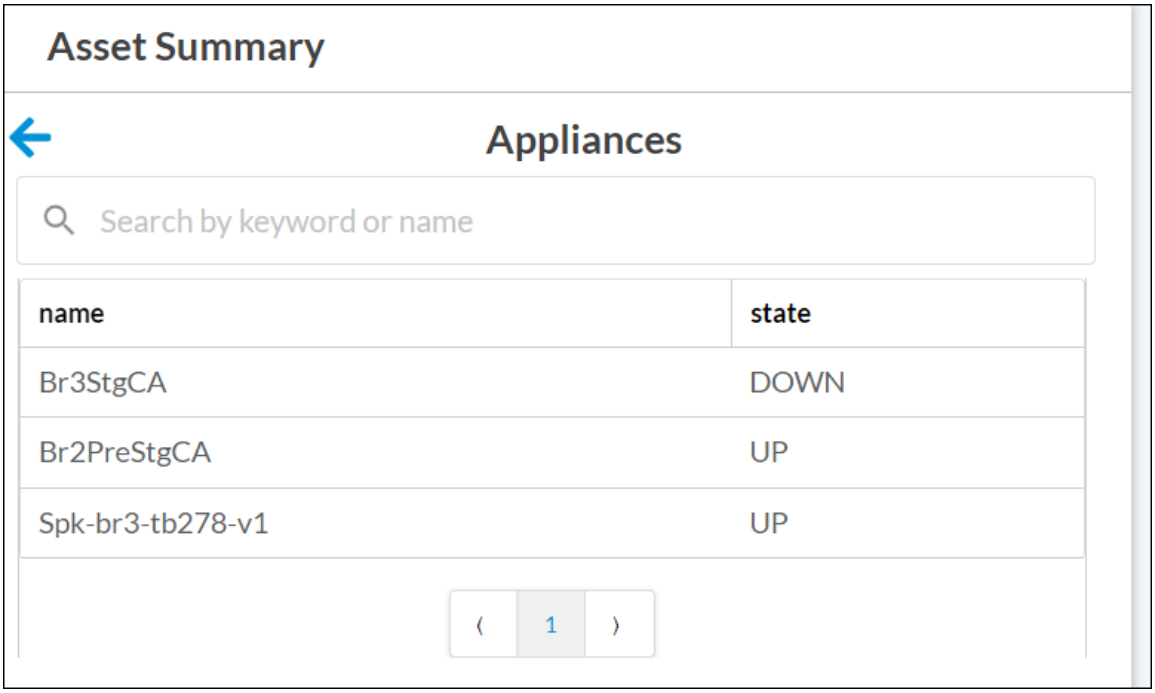
- To view path information for a device, click the device name.



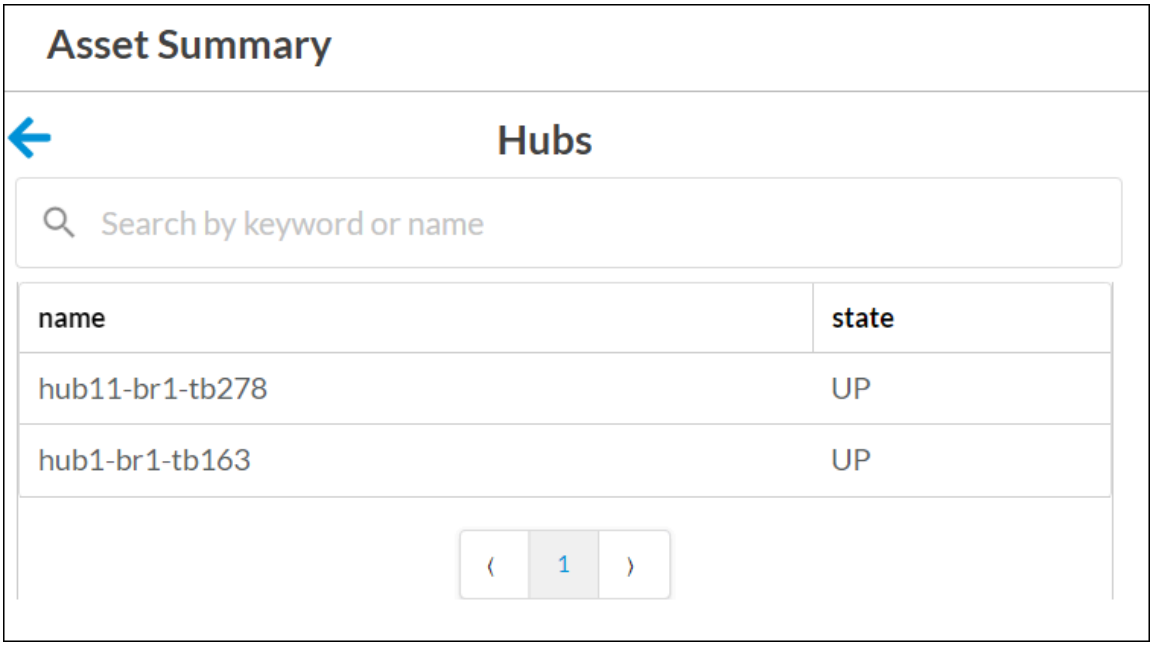
6. In the Asset Summary section, click the Appliance, Hubs, Hub–Controllers, or SSE Gateways category to view the device status up (green) or down (red).



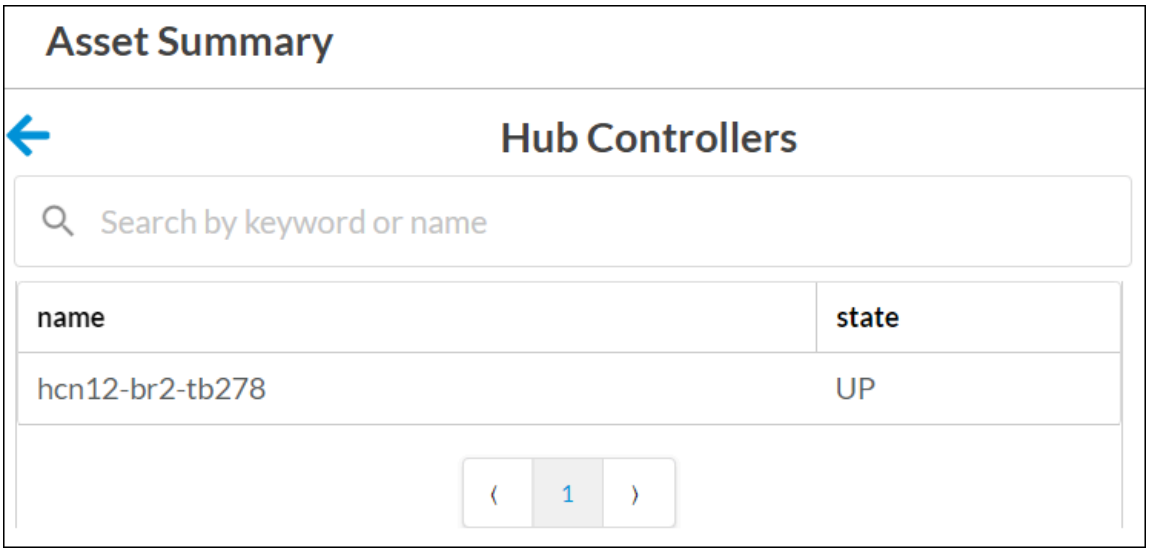
- The following screens display asset summary of devices:
  - Asset summary of devices



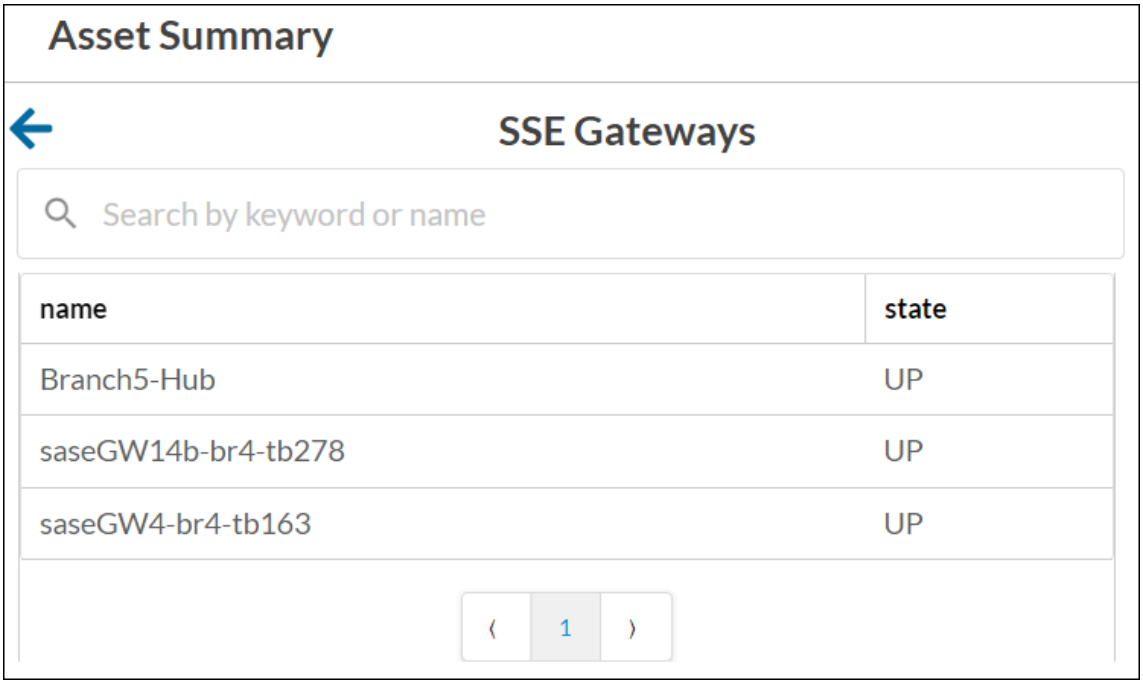
  - Asset summary of hubs



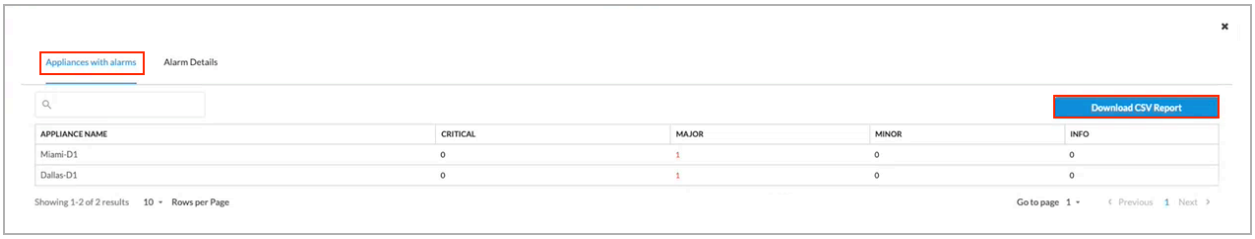
- Asset summary of hub–controllers



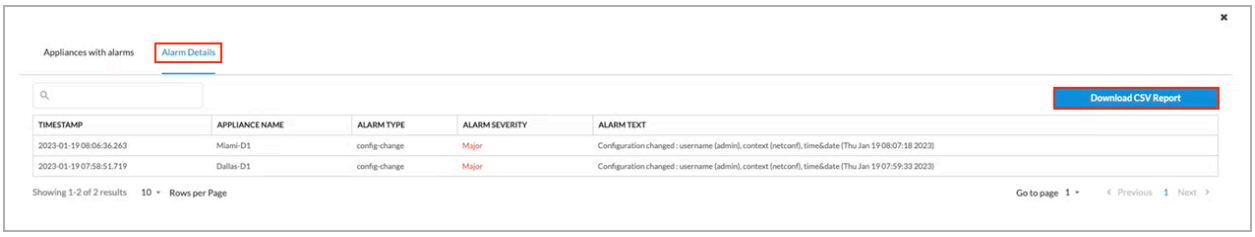
- Asset summary of SSE gateways



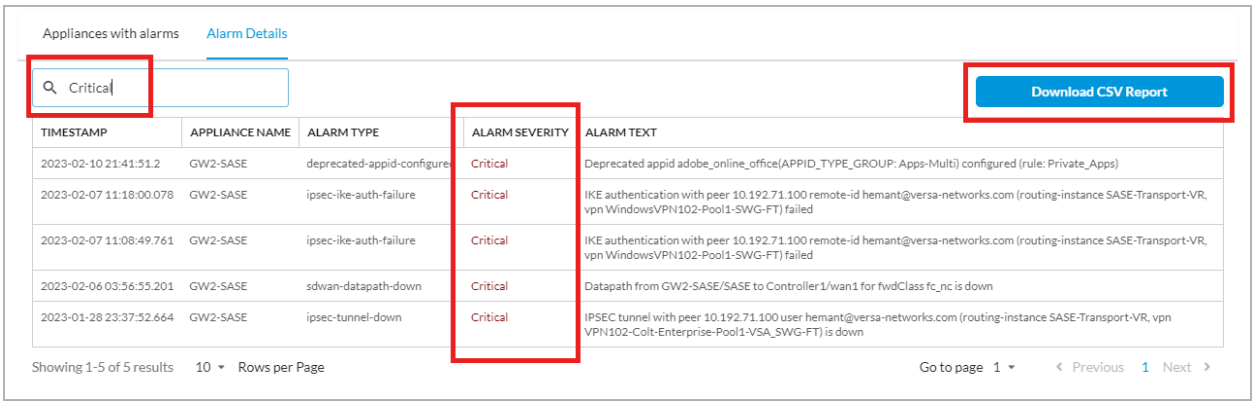
7. (For Releases 11.3.2 and later.) In Alarming Devices, click the number below Critical and Major to view details about the alarms. The screen displays two tabs, with the Appliances with alarms tab selected by default.
   a. To download a file in CSV format containing the information about the devices with alarms, click Download CSV Report.



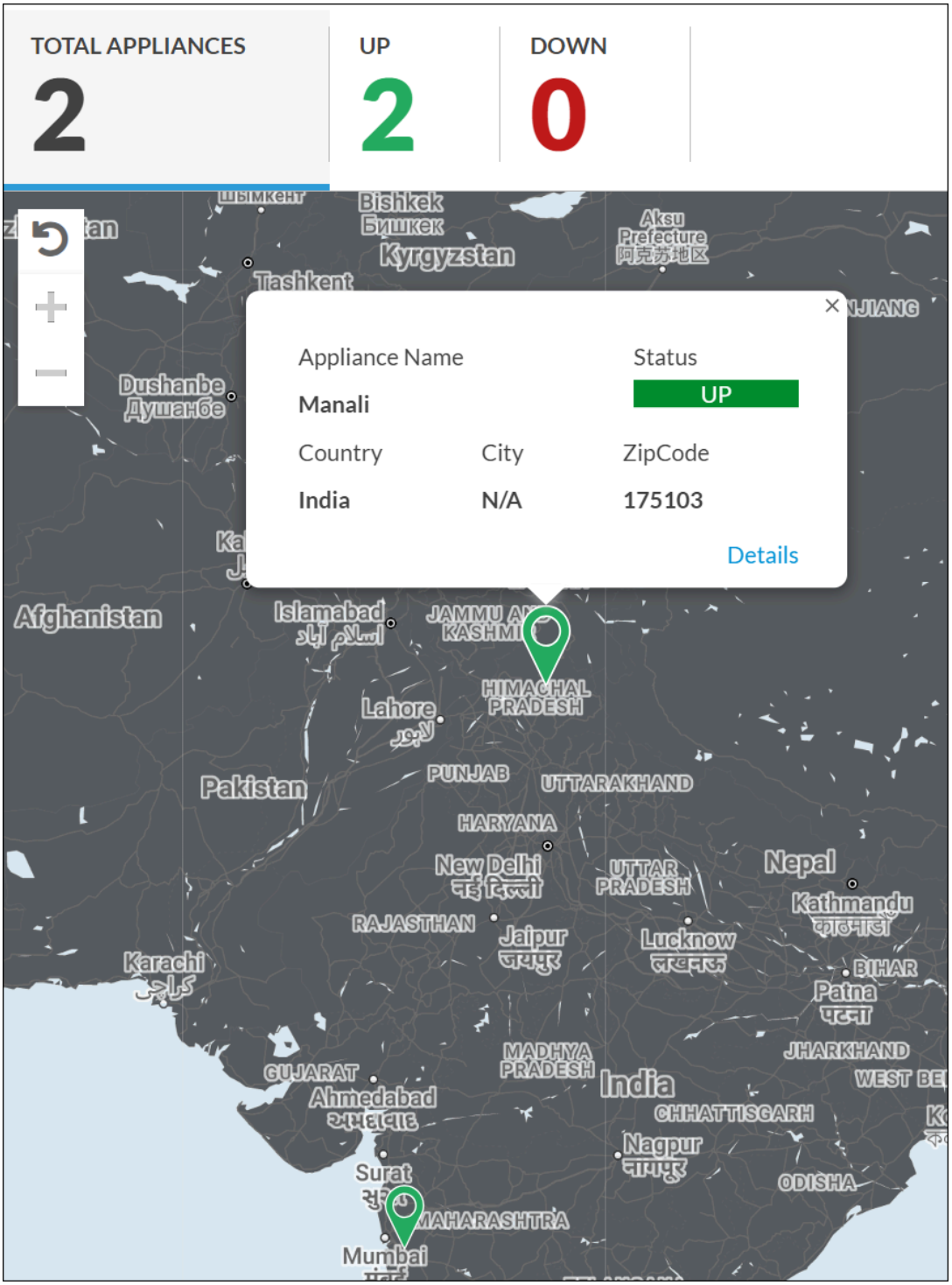
   b. To view details for each alarm, select the Alarm Details tab.
   c. To download a file in CSV format containing the details for each alarm, click Download CSV Report.



   d. To filter the results that display, use the Search bar. For example, you can search for and display all alarms that are Critical, as follows:



8. Click a device on the map or in the list to view details. Then click Details to view detailed information. For example:



9. In the horizontal menu bar, select a device, and then select the time interval for which to display information:
   - Last 5 minutes
   - Last 15 minutes
   - Last 30 minutes

- Last hour
- Last 12 hours
- Last day
- Last 7 days
- Last 30 days
- Custom range

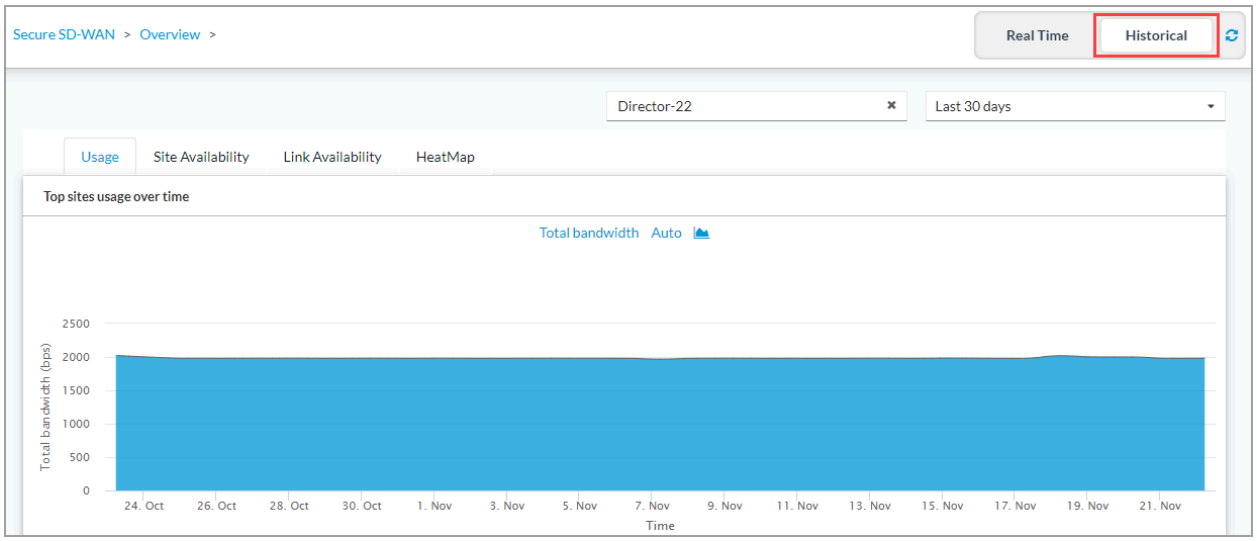
View Historical Information

The historical view of SD-WAN information displays site details by the following:

- Usage
- Site availability
- Link availability
- Heat map

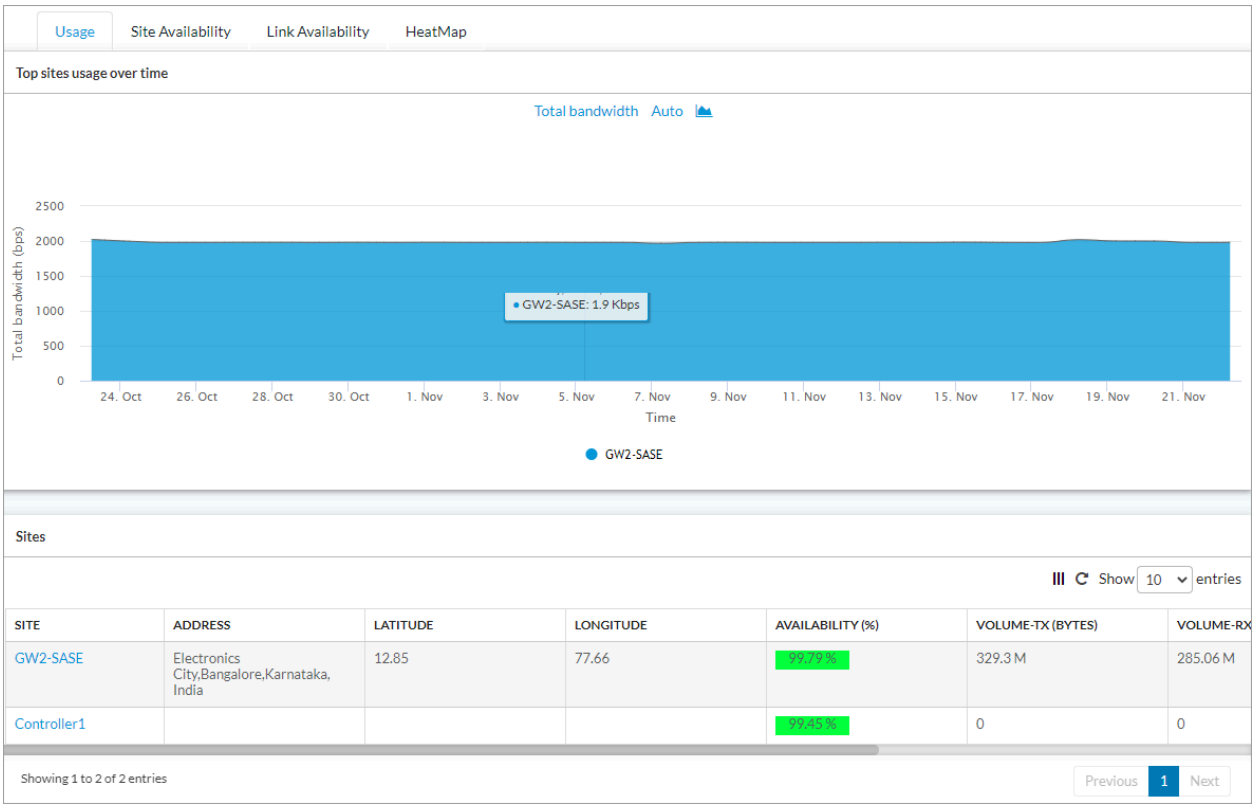
To view historical information SD-WAN devices:

1. In the SD-WAN Overview page, click Historical. The Usage tab displays by default.

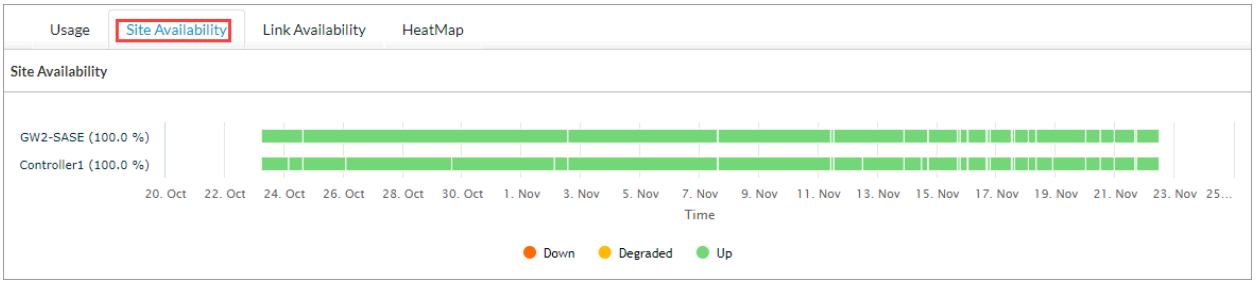


The Usage tab display top site usage over time. To sort the information, use the drop-down menus at the top of the screen. To view the sites as a list, go to the Sites section. To view detailed information about a site, click the site name in the Sites table.

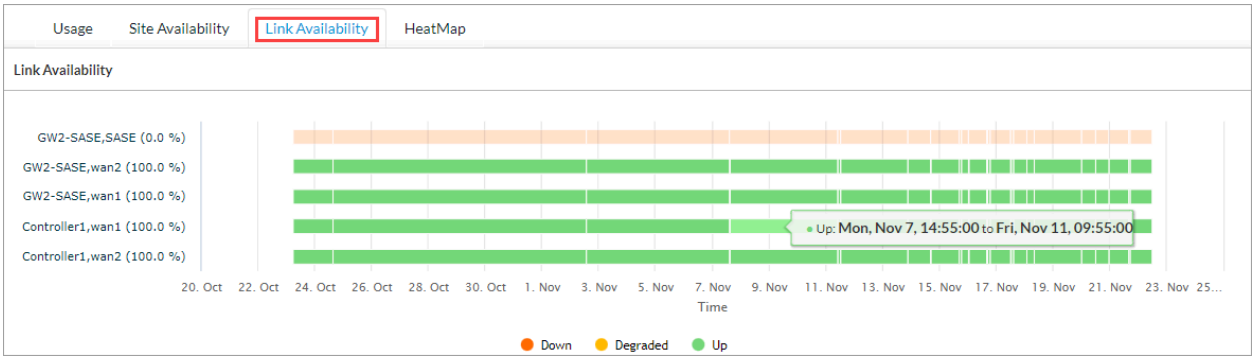
Updated: Wed, 23 Oct 2024 08:54:28 GMT



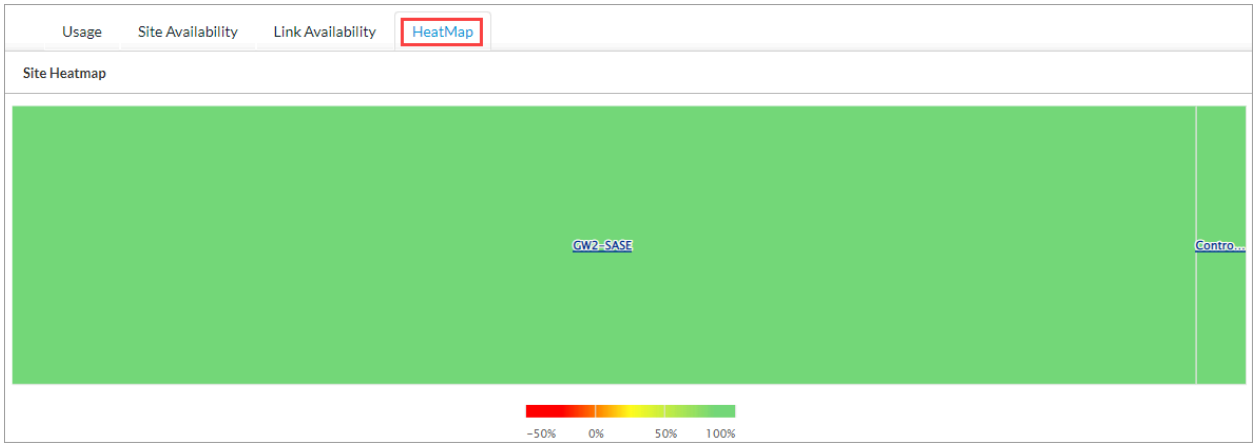
2. To view top site availability over time, select the Site Availability tab . The Site Availability graph shows site status as degraded performance, Down, and Up.



3. To view the status of site links, select the Link Availability tab.



4. To view how much attention a site is receiving, select the Heat Map tab. Hover over sections in the heat map to view site name, availability, and number of sessions.

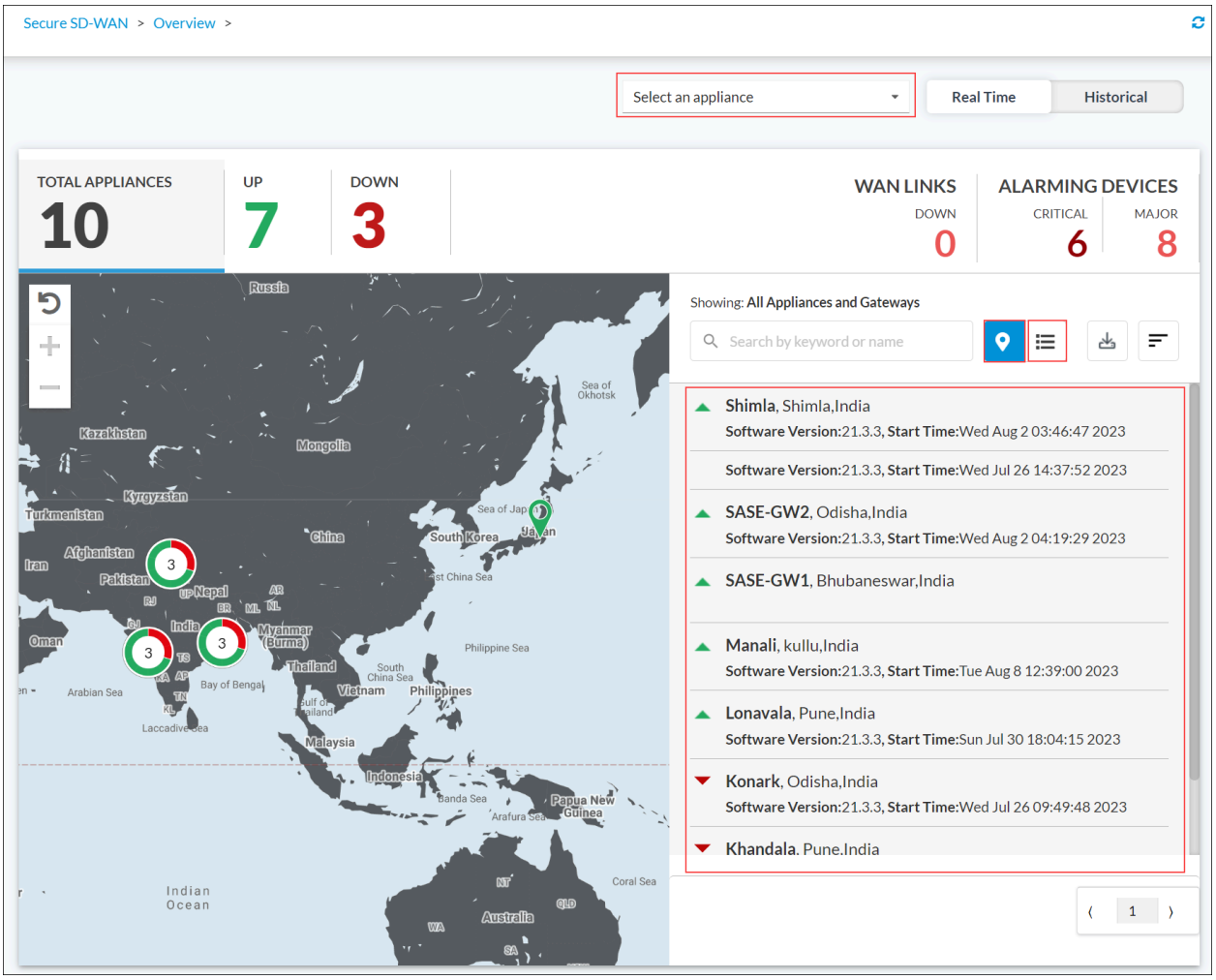


View Device Availability Information

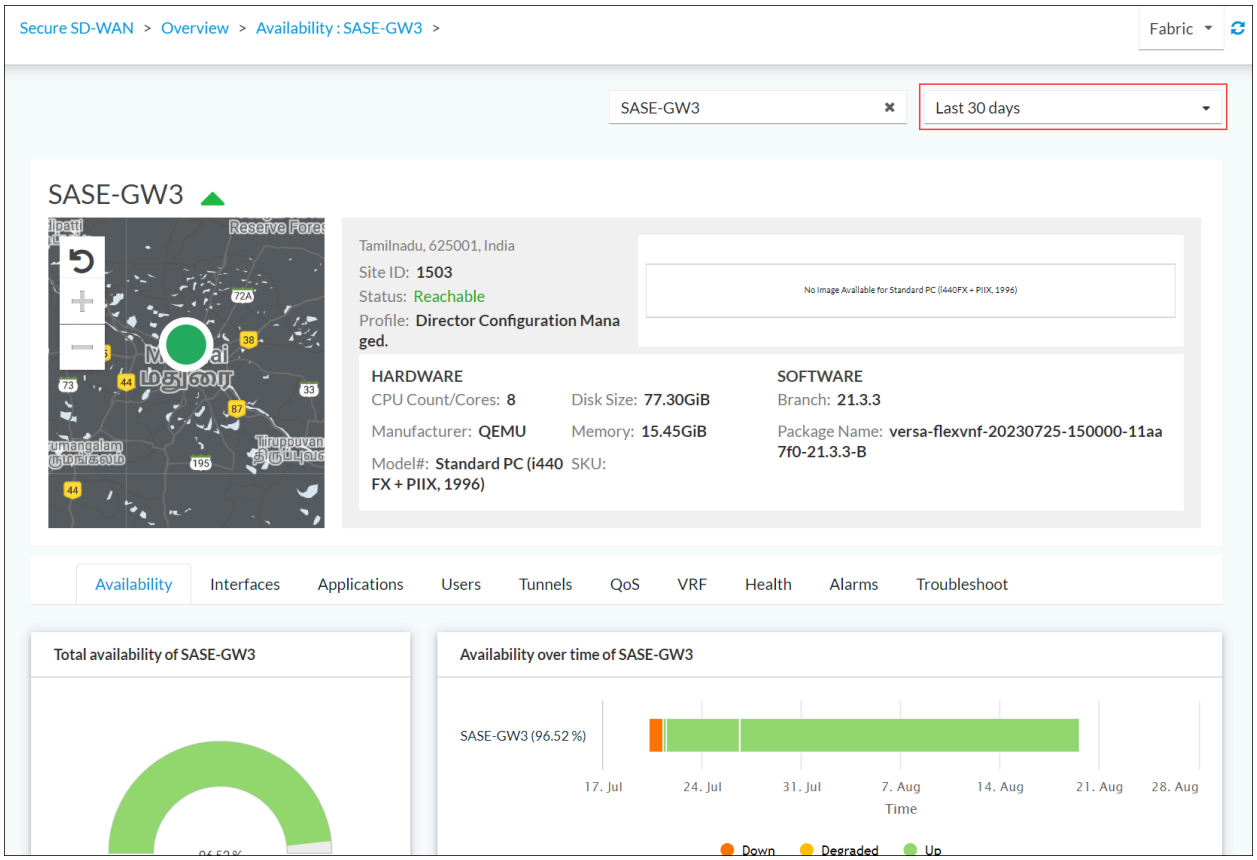
For Releases 11.4.1 and later.

To view the availability information about a device:

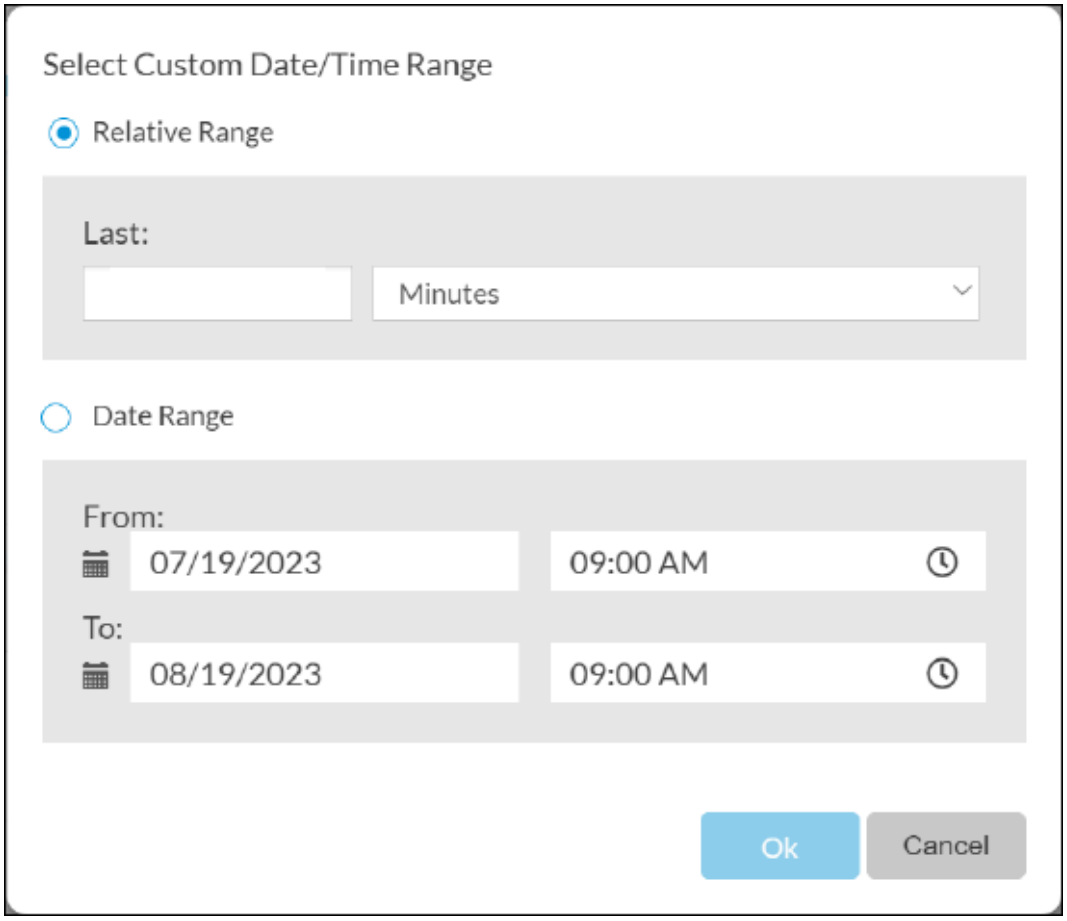
1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View. The green Up arrow icon indicates that the device is reachable, and the red Down arrow indicates that the device is unreachable.



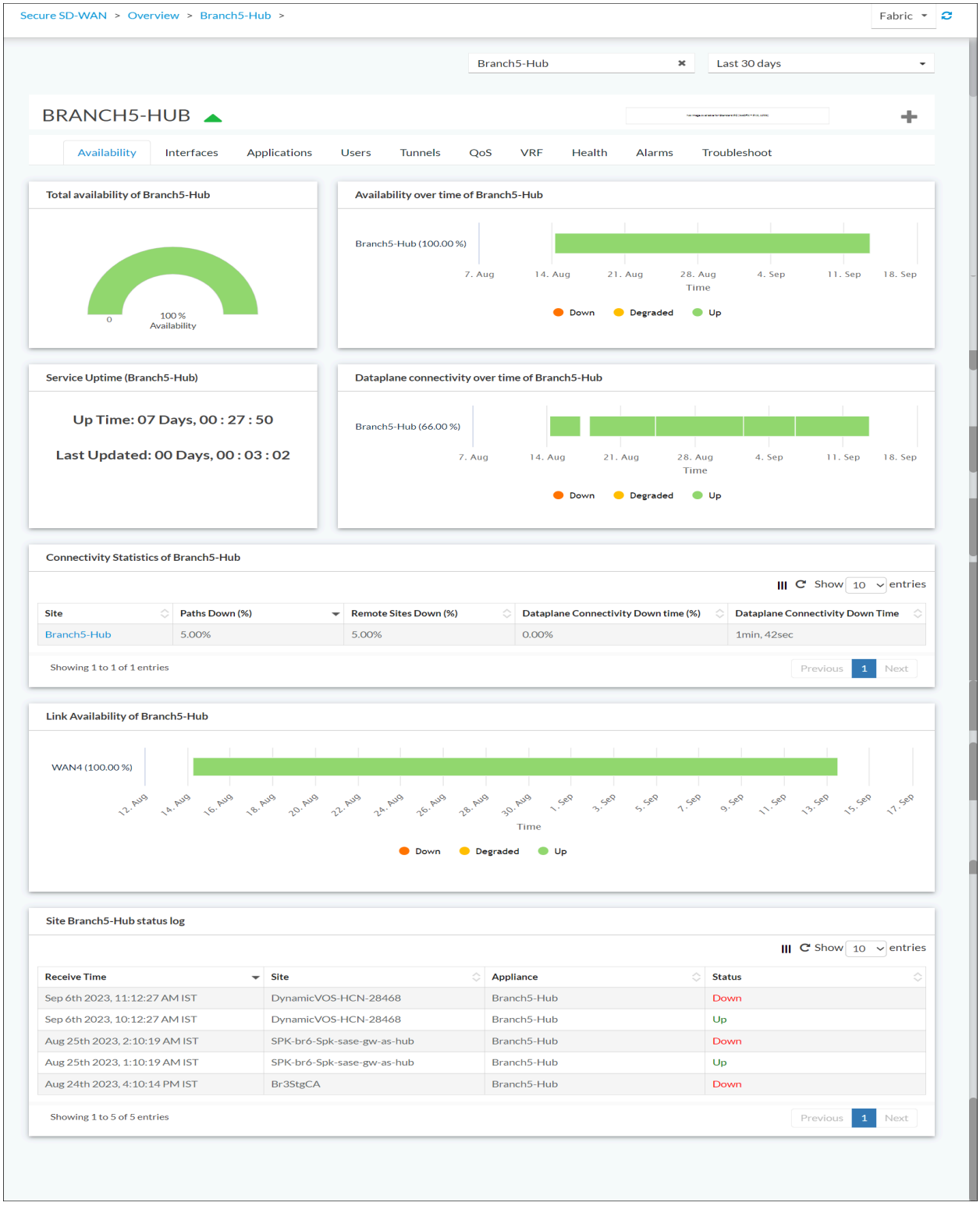
2. Select the time interval for which to display information.



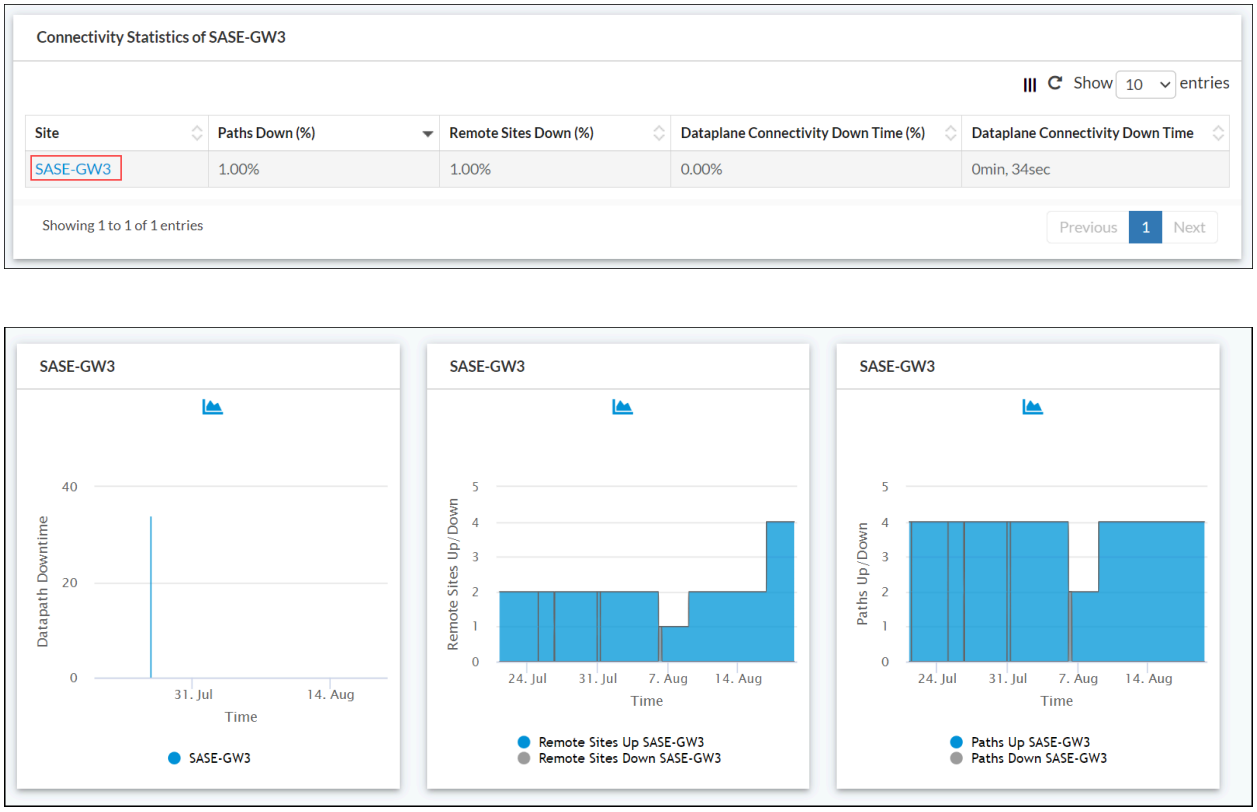
- Last 5 minutes
- Last 15 minutes
- Last 30 minutes
- Last hour
- Last 12 hours
- Last day
- Last 7 days
- Last 30 days
- Custom range. Select the range, and then click OK.



3. Select the Availability tab to displays the following information for the selected device:
   - Total availability
   - Availability over time
   - Service uptime
   - Data plane connectivity over time
   - Connectivity statistics
   - Link availability
   - Site status log



4. To view the graphical representation of connectivity statistics, click site name in the Connectivity Statistics pane.



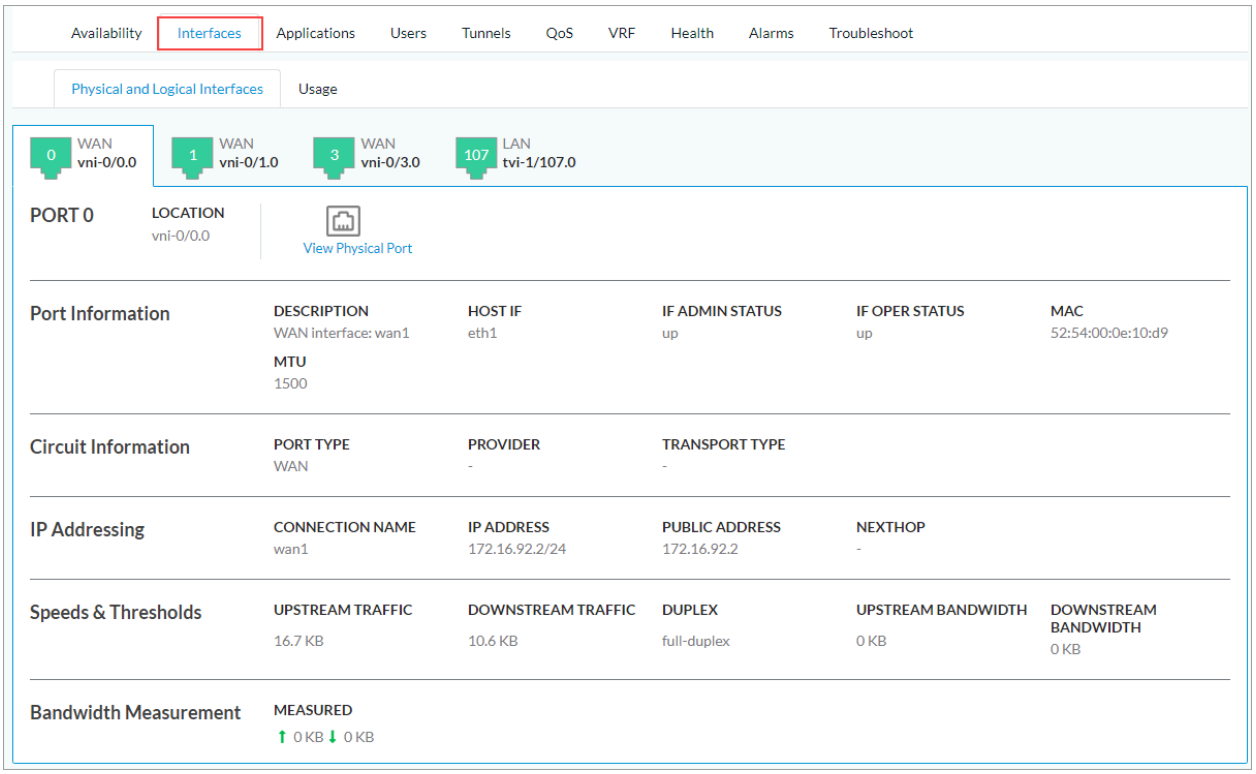
5. To change the graphical representation of data, click the Chart Menu icon to select the current graphical data representation. The format can be Area, Column, Line, Scatter, or Stacked Column.

Monitor Device Interfaces

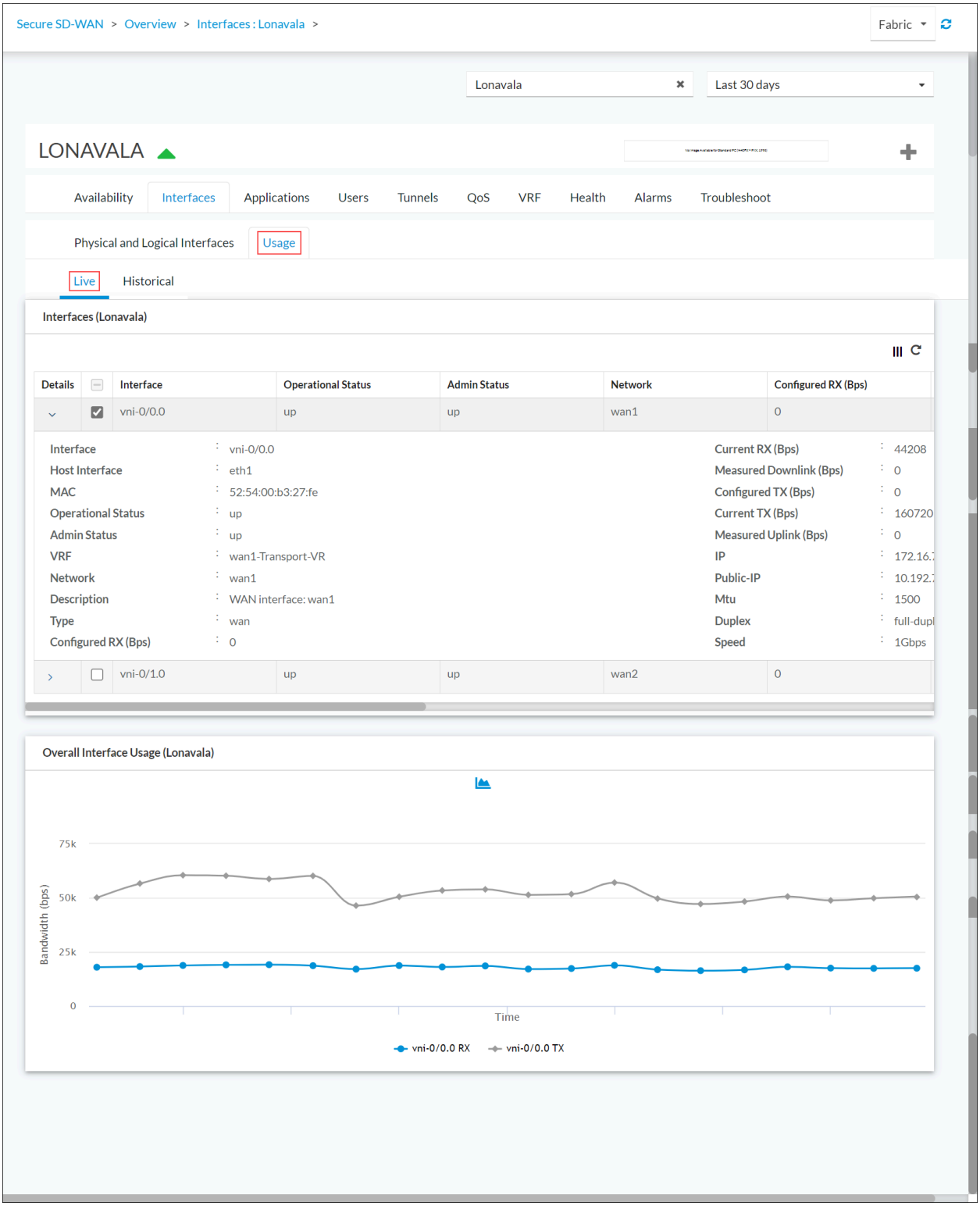
The Interfaces screens displays information about the device's CPE interfaces and the traffic transiting them.

To monitor device interfaces:

1. Click View > Secure SD-WAN > Overview, and and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Select the Interfaces tab.
3. Select the Physical and Logical Interfaces to display information about the interfaces.



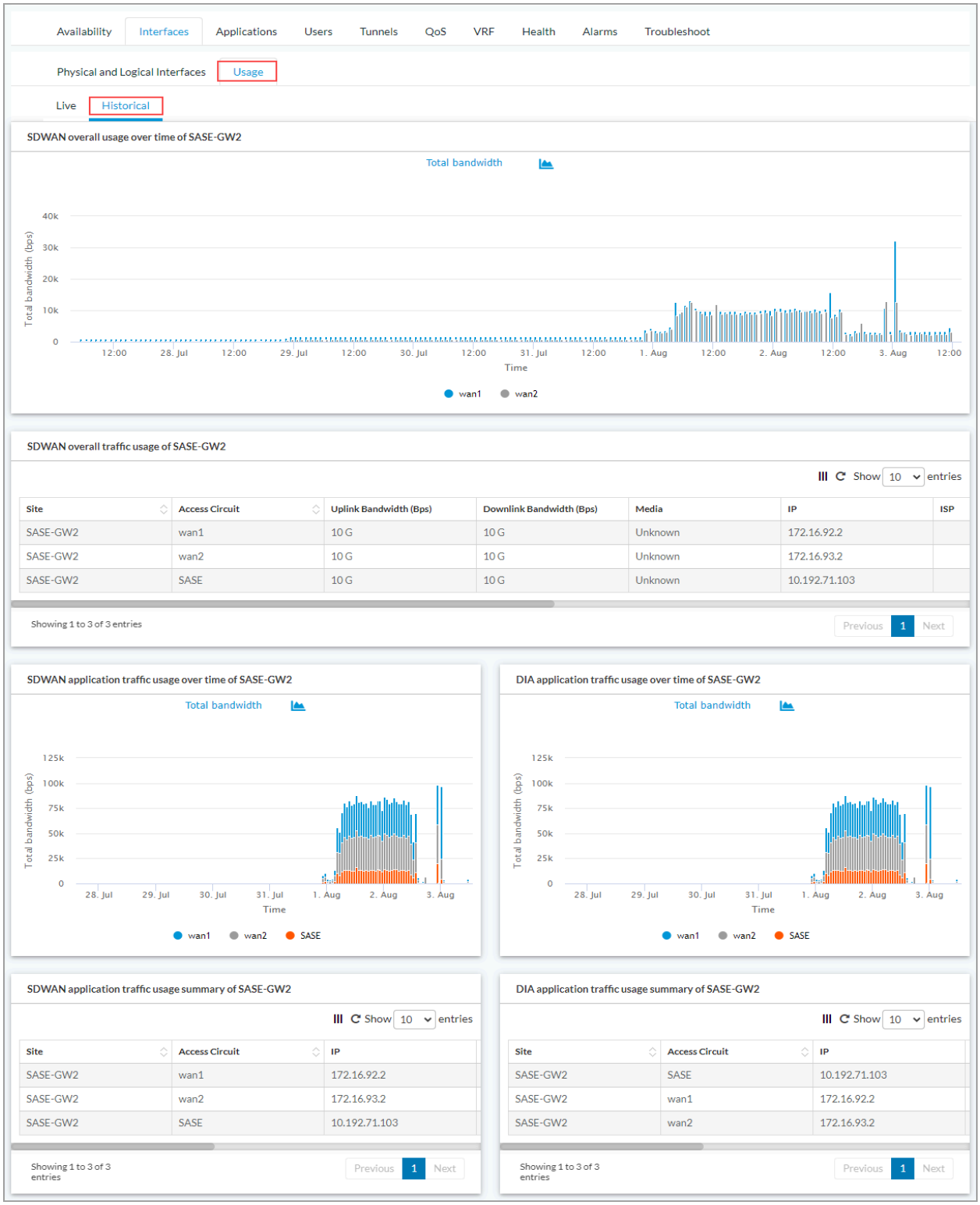
4. Select the Usage tab to display live and historical information of interfaces.
5. To display real-time information about interfaces, select the Live tab.
    a. To view more information, click the down arrow in the Details column.
    b. To view the Overall Interface Usage graph, which displays real-time transmission data, click the checkbox next to down arrow.



c. To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.

6. To display past usage information about interfaces, select the Historical tab. The Historical tab displays the following panes:

- SD-WAN Overall Usage over Time
- SD-WAN Overall Traffic Usage
- SD-WAN Application Traffic Usage over Time
- DIA Application Traffic Usage over Time
- SD-WAN Application Traffic Usage Summary (for Releases 11.4.1 and later)
- DIA application traffic Usage Summary (for Releases 11.4.1 and later)



You can change the view type to any one of the following:

- Bandwidth received and transmitted (TX RX)
- Total bandwidth

- Volume received (RX)
- Volume transmitted (TX)
- Volume received and transmitted (TX RX)

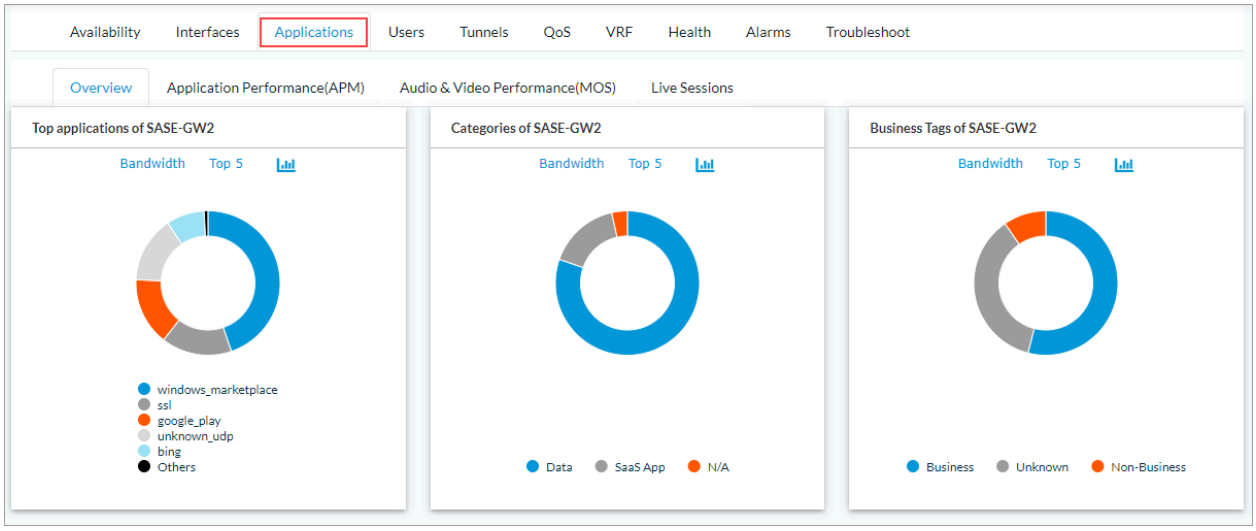
To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.

View Application Information for a Device

The Applications tab displays information about application performance, audio and video performance, and application live data for a device.

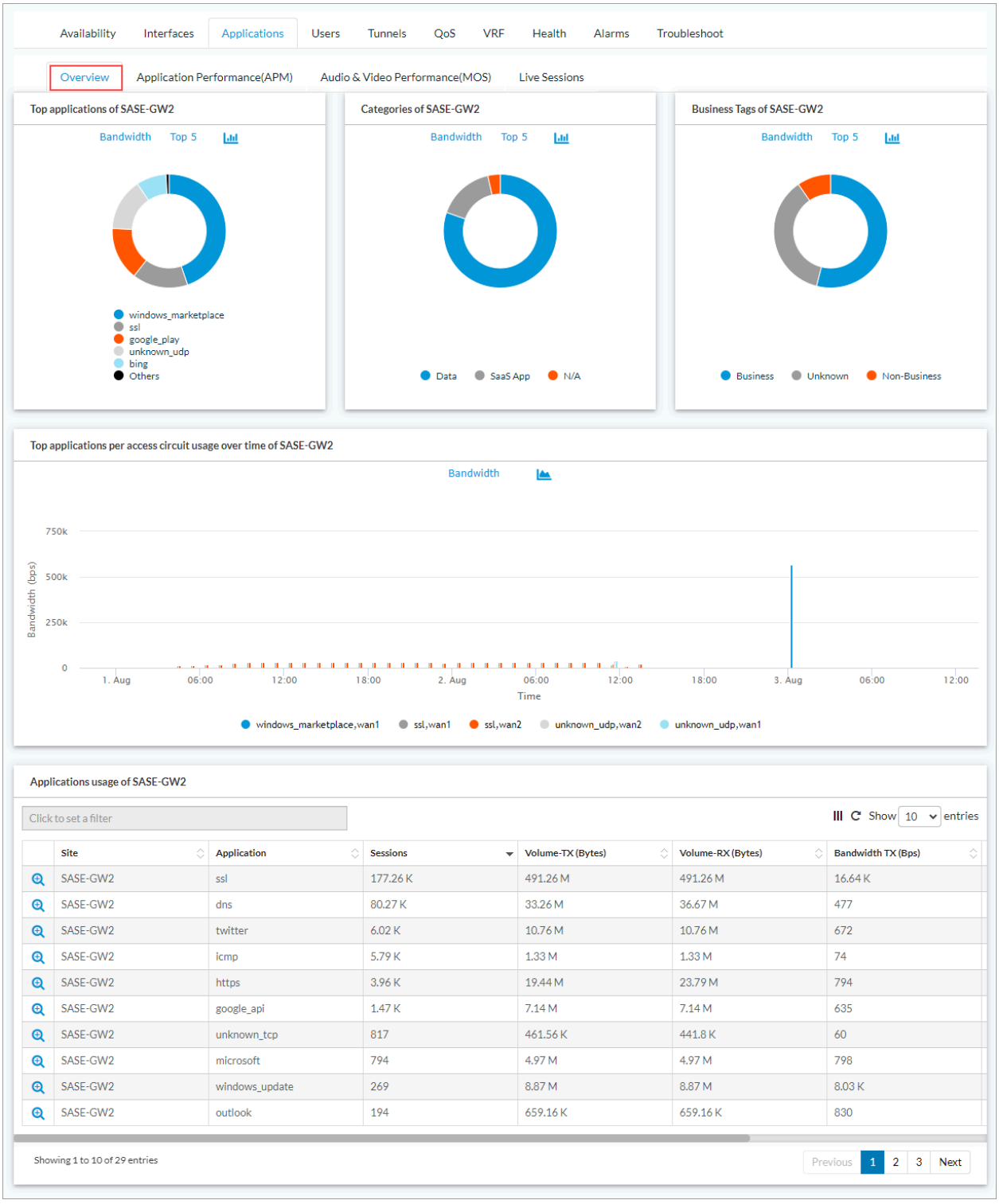
To view application information for a device:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Select Applications tab. The Applications tab displays the following tabs:
   - Overview (default)
   - Application Performance (APM)
   - Audio & Video Performance (MOS)
   - Live Sessions



3. Select the Overview tab. This tab displays the following panes:
   - Top Applications (for device or circuit) (chart)
     - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
   - Categories (for device or circuit) (chart)
     - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx

    - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
- Business Tags (for device or circuit) (chart)
    - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
    - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
- Top Applications per Access Circuit Ssage over Time (for device or circuit) (chart)
    - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
    - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
- Applications Usage (table)
    - To view user statistics for each device, click the  Zoom icon.

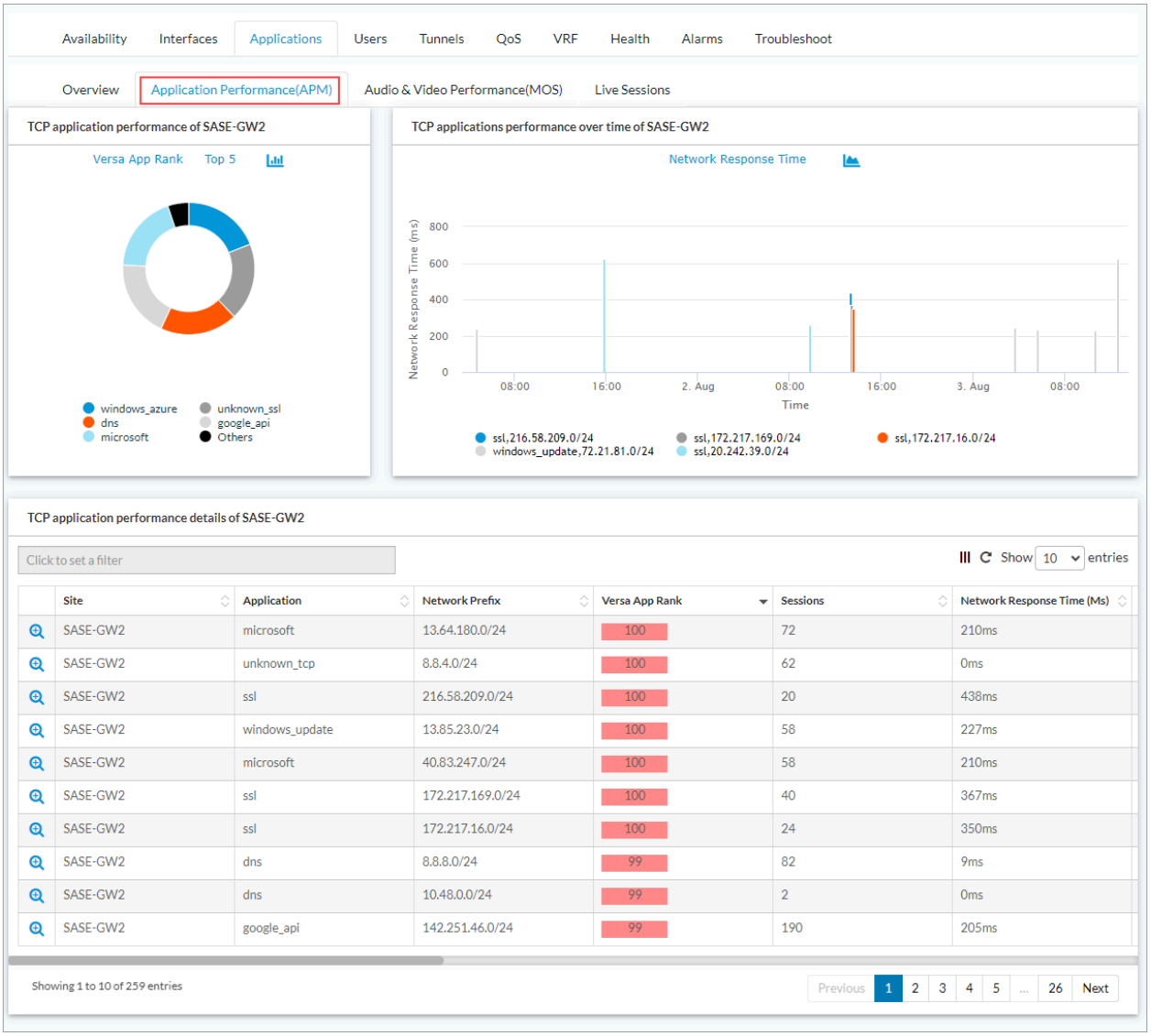


4. To view application information, select the Application Performance (APM) tab. This tab displays the following pane:
   - TCP Application Performance (device or circuit) (chart)
     - By Aborted and Refused, Average SAA and SSA, Network Response Time, Retransmit Fwd and Rev,

Versa App Rank

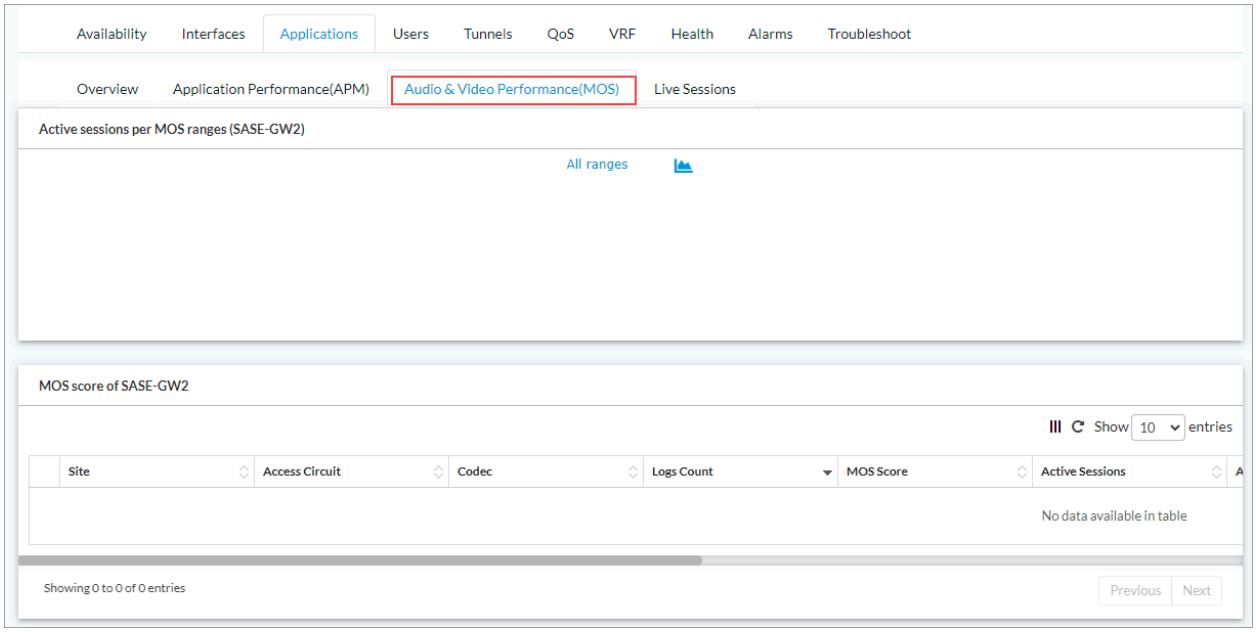
- To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.

- TCP Application Performance over Time (device or circuit) (chart)
  - By Aborted and Refused, Average SAA and SSA, Network Response Time, Retransmit Fwd and Rev, Versa App Rank
  - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
- TCP Application Performance Details (device or circuit) (table)
  - To view user statistics for each device, click the Zoom icon.

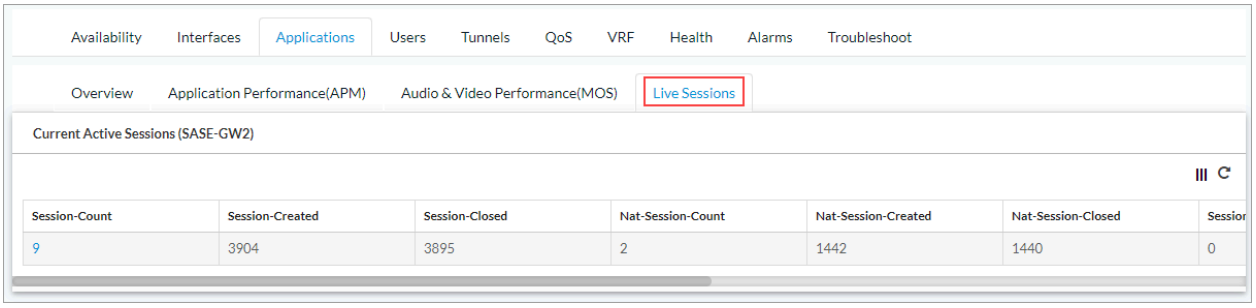


5. To view the mean opinion score (MOS) information for applications, select the Audio and Video Performance (MOS) tab. This tab displays the following panes:

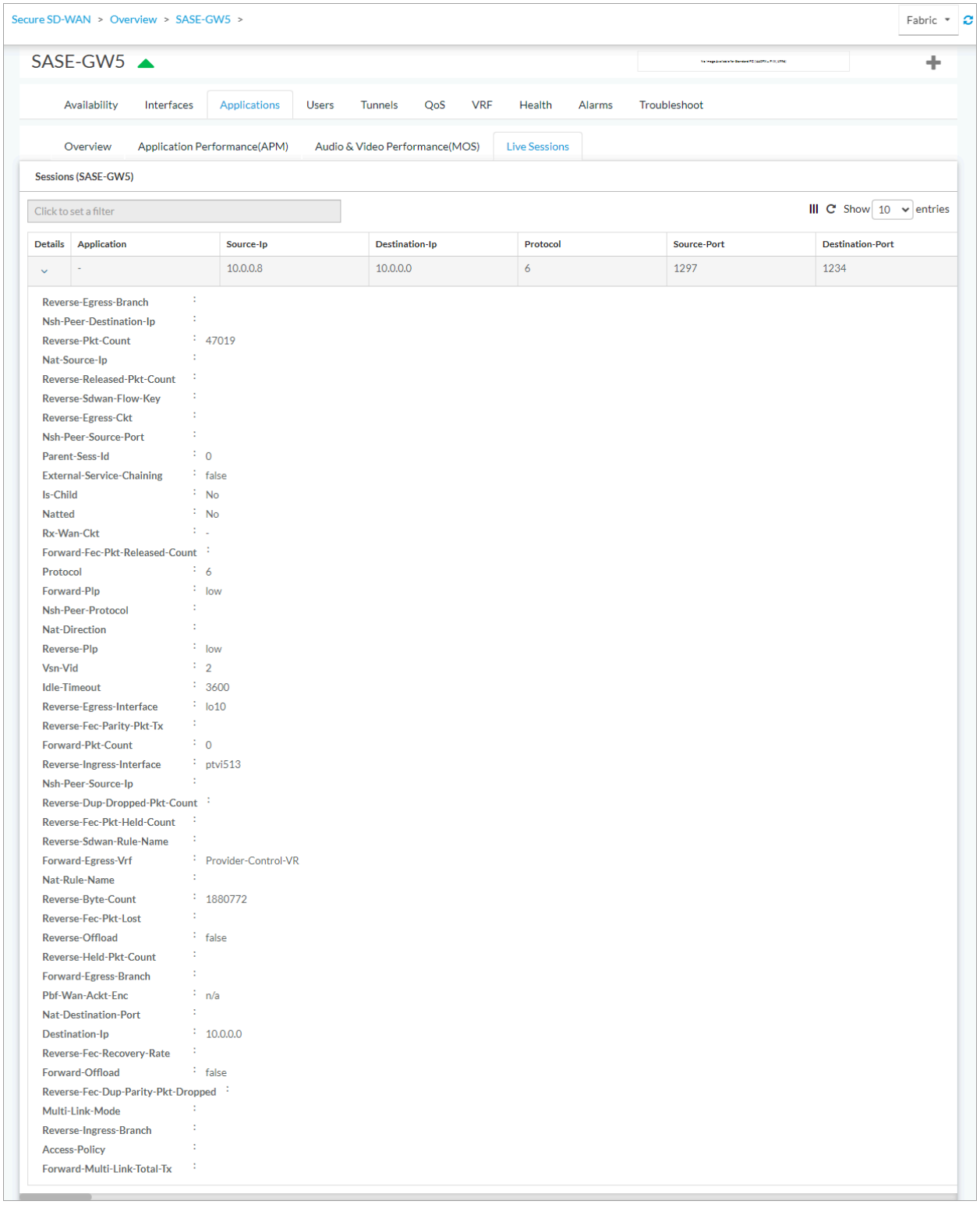
- Active Sessions per MOS Range (device or circuit) (chart)
  - By All Ranges, Sessions MOS 1-2, Sessions MOS 2-3, Sessions MOS 3-3.5, Sessions MOS 3.5-4, Sessions MOS 4-5
  - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
- MOS Score (device) (table)



6. To view the current active sessions for the tenant, Select the Live Sessions tab.



7. To view session statistics, click Session Count, and then click the down arrow in the Details column to view more information.



Updated: Wed, 23 Oct 2024 08:54:28 GMT

View User Information

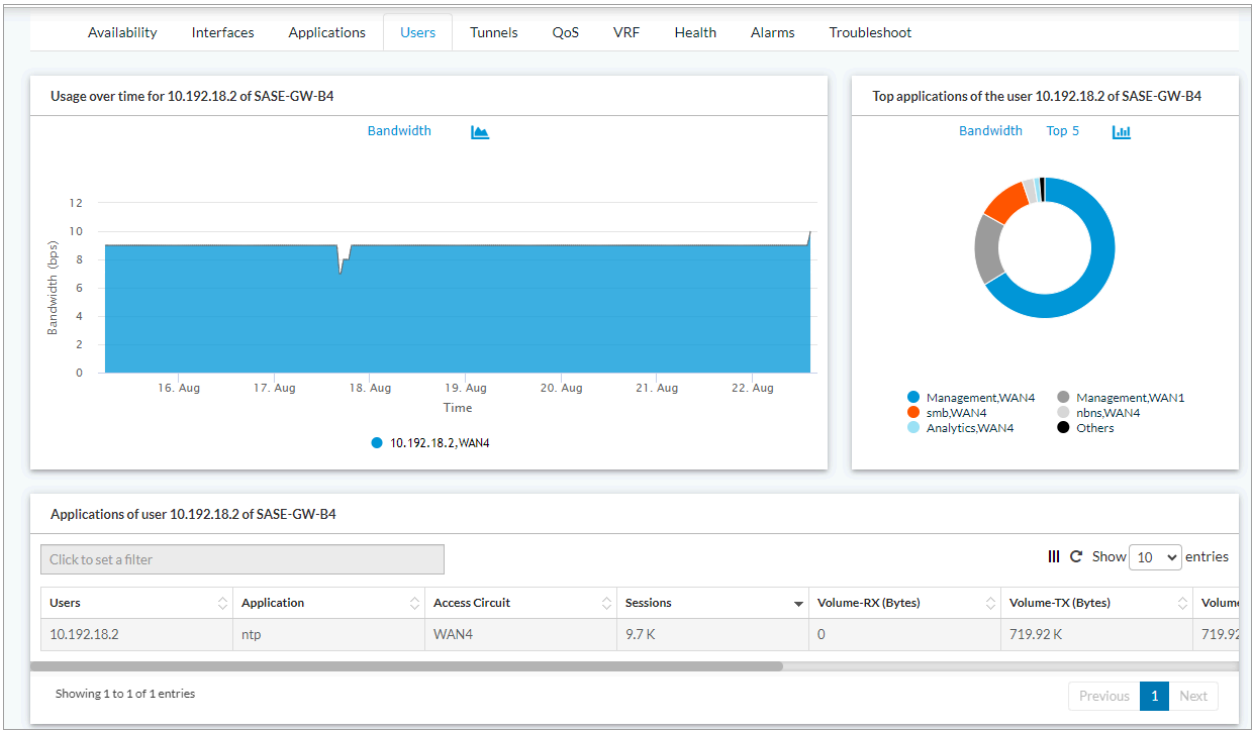
For Release 11.4.1 and later.

The Users tab displays information about a tenant's SD-WAN users.

To view user information:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Click Users tab. This tab displays the following pages:
    - Top Users
        - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
        - To change the graphical representation of data, click the Chart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
    - Top Users per Access Circuit over Time
        - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
        - To change the graphical representation of data, click the Chart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
    - Users table

3. To view user statistics for each device, click the Zoom icon.



View Tunnel Information

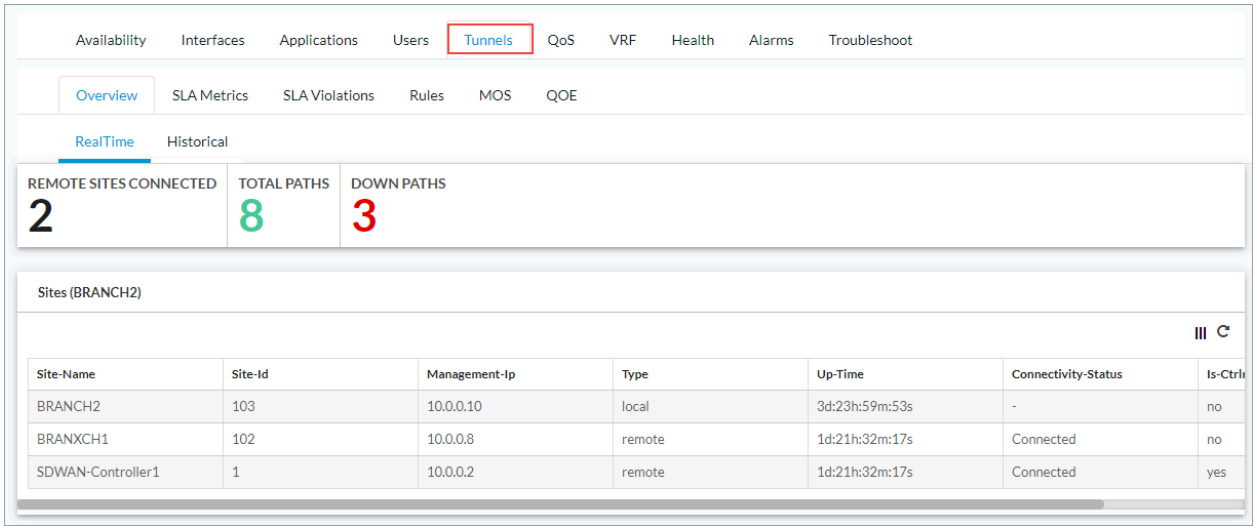
For Release 11.4.1 and later.

The Tunnels tab displays the following information about site-to-site tunnels:

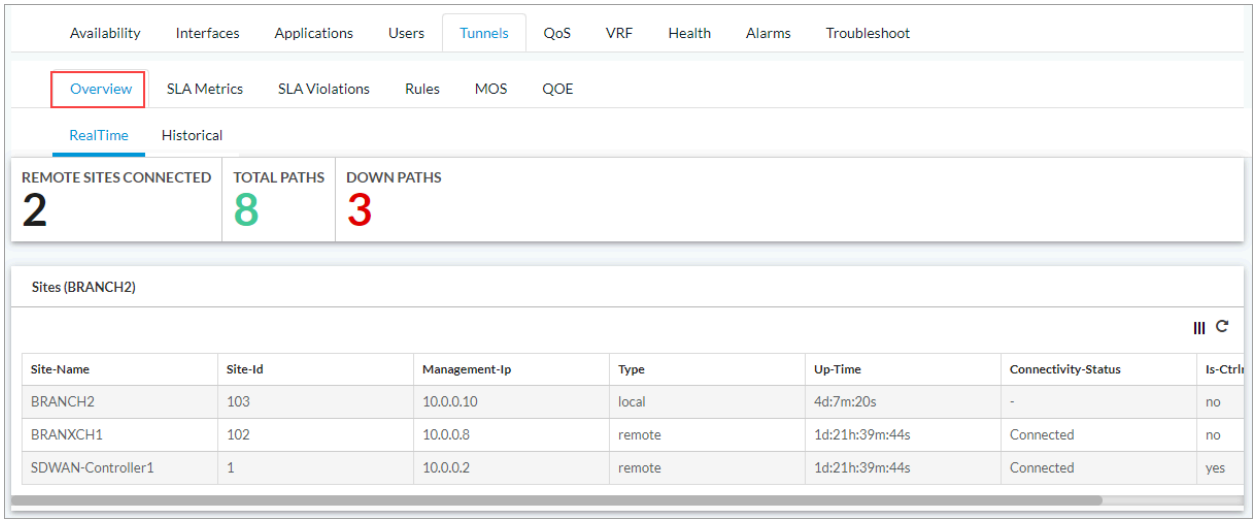
- Overview
- SLA metrics
- SLA violations
- Rules
- MOS
- QoE

To view tunnel information:

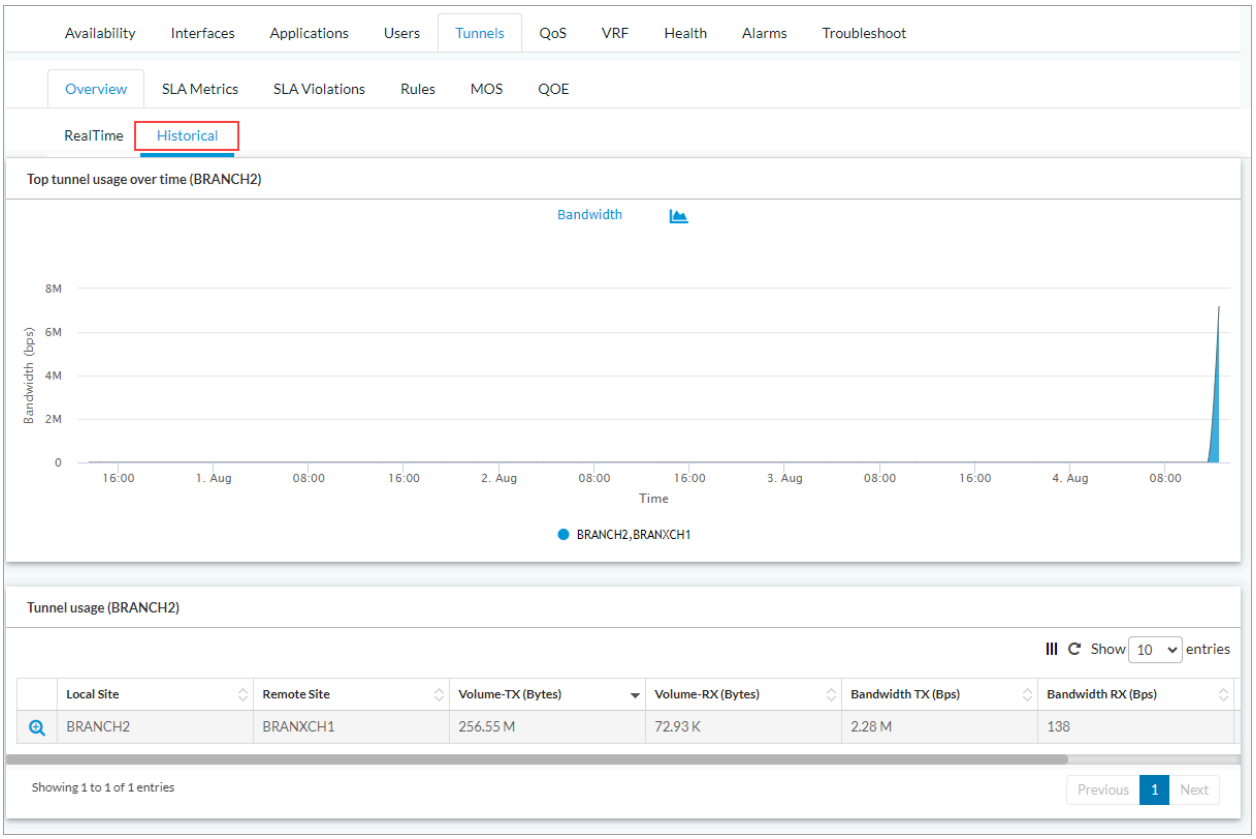
1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Select the Tunnels tab, and then select he Overview tab.



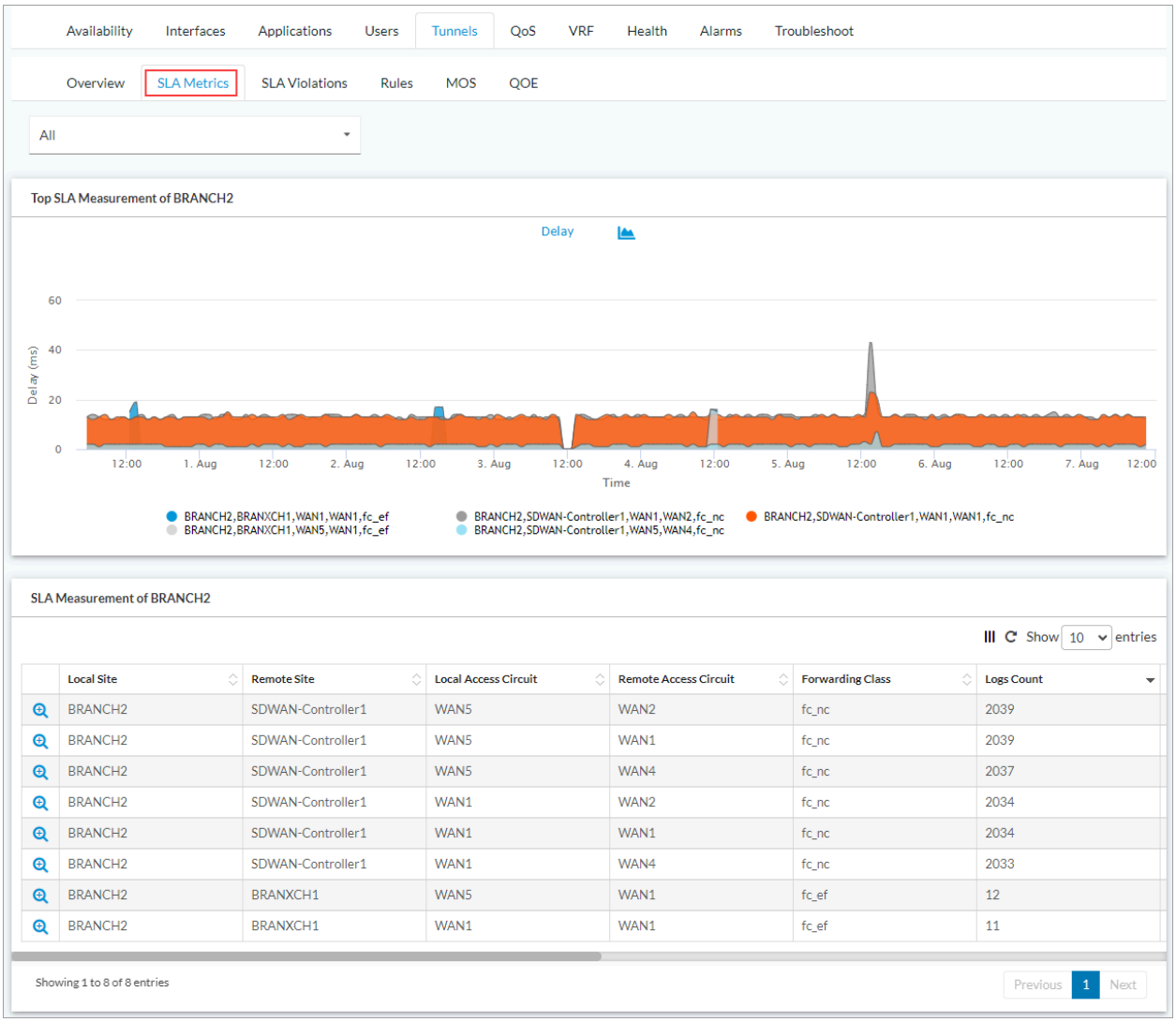
3. To view the number of connected remote sites, total paths, down paths, and real-time information about the sites, select the Real-Time tab.



4. Select the Historical tab. The Historical tab displays the following panes:
   - Top Tunnel Usage over Time
     - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
   - Tunnel Usage
     - To view the path usage from the local site to the remote site, click the Zoom icon.

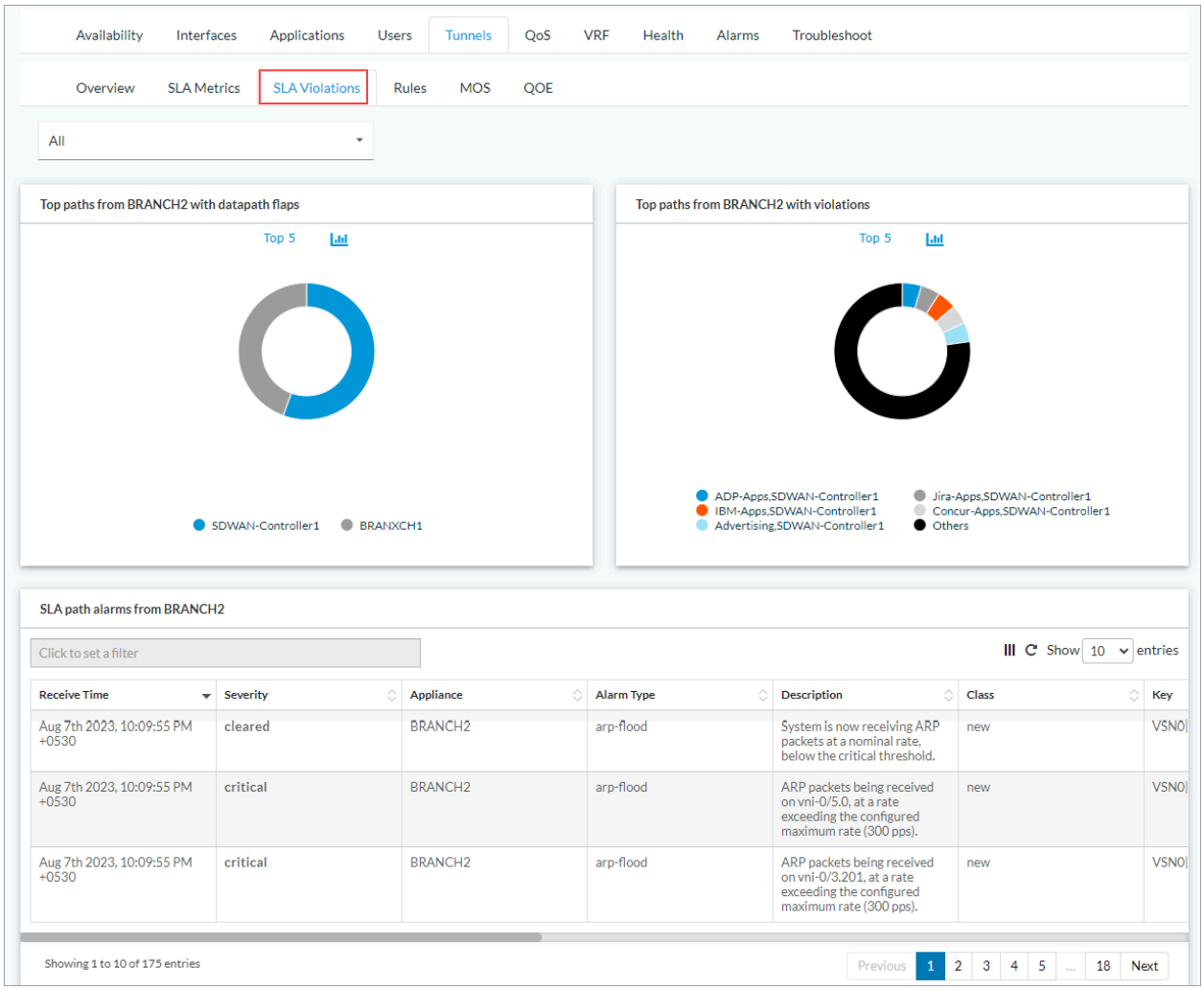


5. To view information about changes in the SLA status that occurred on a path between sites, select the SLA Metrics tab. The SLA Metrics tab displays the following panes:
   - Top SLA Measurement
     - By Delay, Forward Delay Var, Forward Loss Ratio, PDU Loss Ratio, Reverse Delay Variation, Reverse Loss Ratio
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
   - SLA Measurement
     - To view the SLA delay metrics, SLA loss ratio, and SLA logs from local site to remote site, click the Zoom icon.

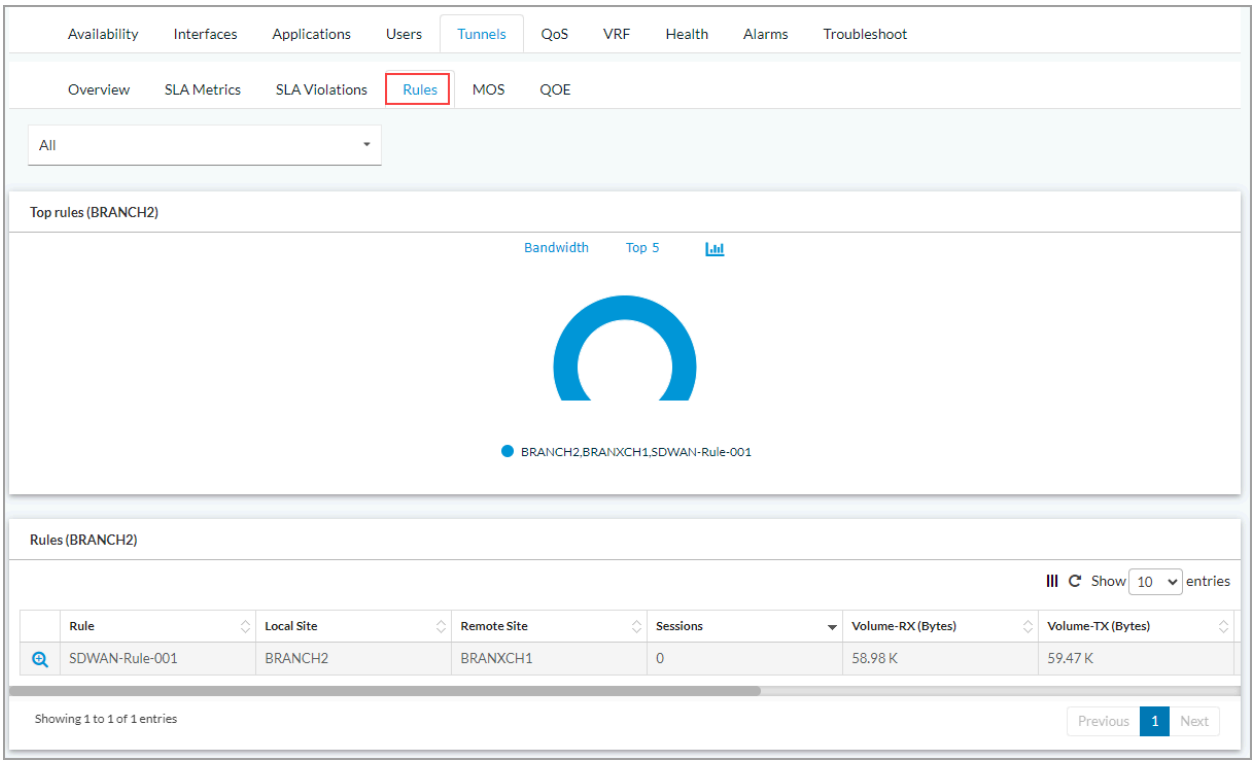


6. To view information about SLA violation events that occurred on a path between sites, select the SLA Violations tab. The SLA Violations tab displays the following panes:
   - Top Paths with Data Path Flaps
     - To change the graphical representation of data, click the Chart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
   - Top Paths with Violations
     - To change the graphical representation of data, click the Chart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
   - SLA Path Alarms

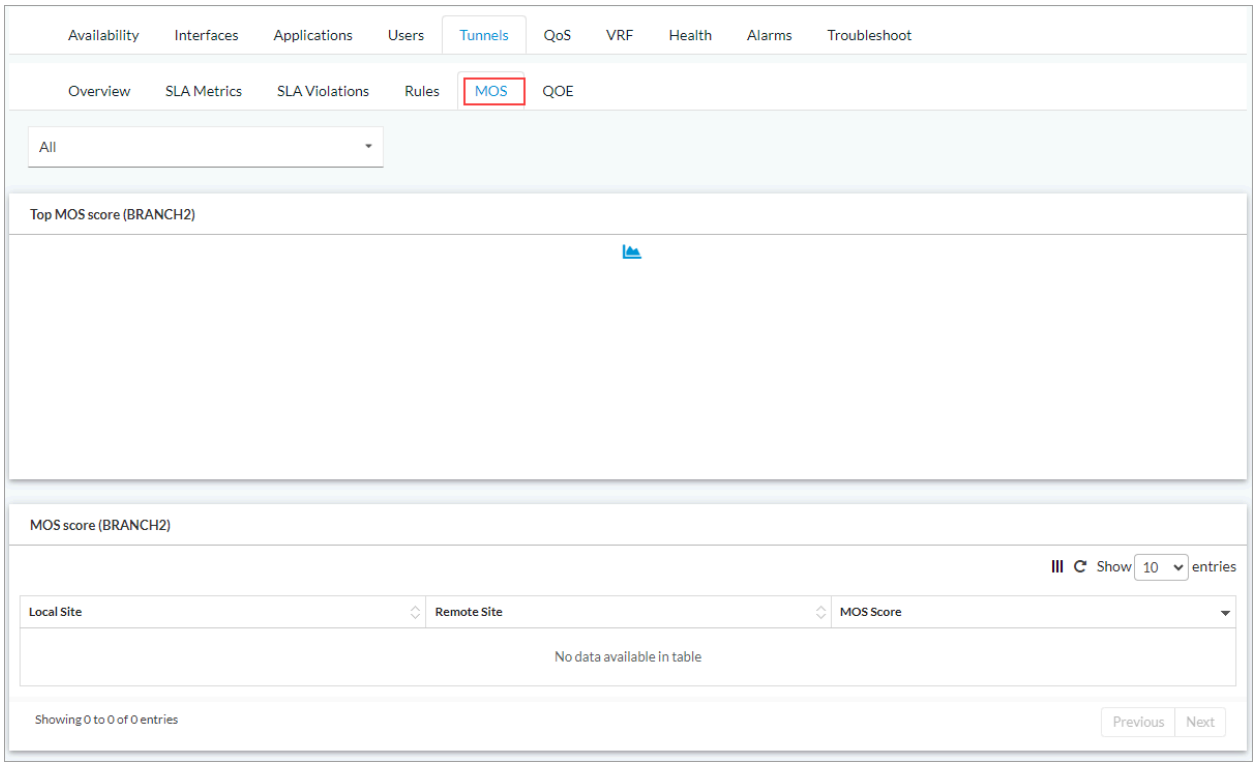
Updated: Wed, 23 Oct 2024 08:54:28 GMT



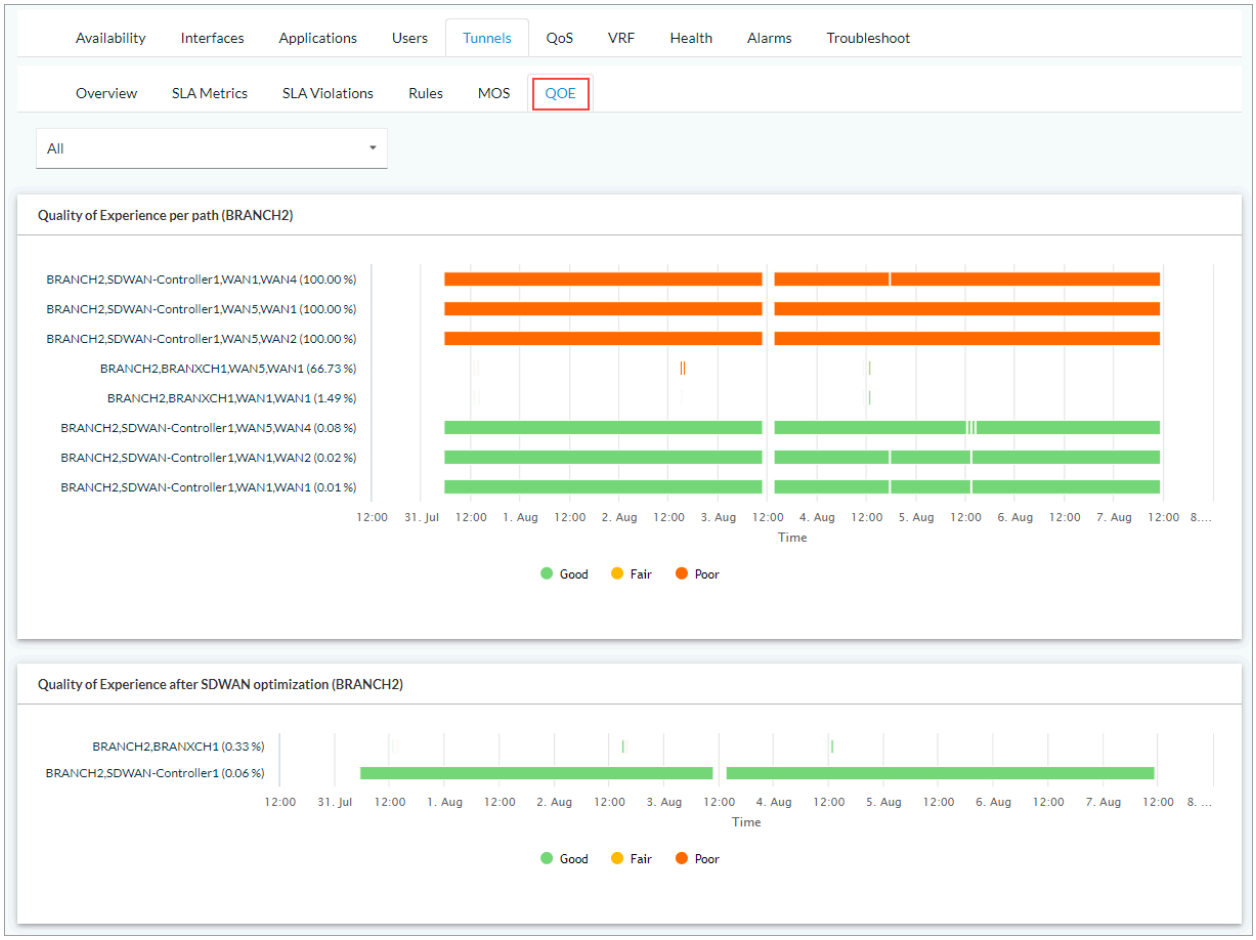
7. To view information about the site-to-site tunnel policy rules, select the Rules tab. The Rules tab displays the following panes:
   - Top rules (chart)
     - By Bandwidth, Bandwidth Tx Rx, Sessions, Volume Rx, Volume Tx, Volume Tx Rx
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Bar, Column, Line, or Pie.
   - Rules (table)
     - To view details about the rules, click the Zoom icon.



8. To display the MOS score in a user profile, select the MOS tab. The MOS score is a measure of the quality of voice data traffic. When the traffic quality falls below the defined MOS score value. The MOS tab displays the following panes:
   - Top MOS Score (chart)
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
   - MOS Score (table)



9. To view information about QoE per path and QoE after WAN optimization between sites, select the QoE tab. The QOE tab displays the following panes:
   - Quality of Experience per Path
   - Quality of Experience after SD-WAN Optimization



View QoS Information

For Release 11.4.1 and later.

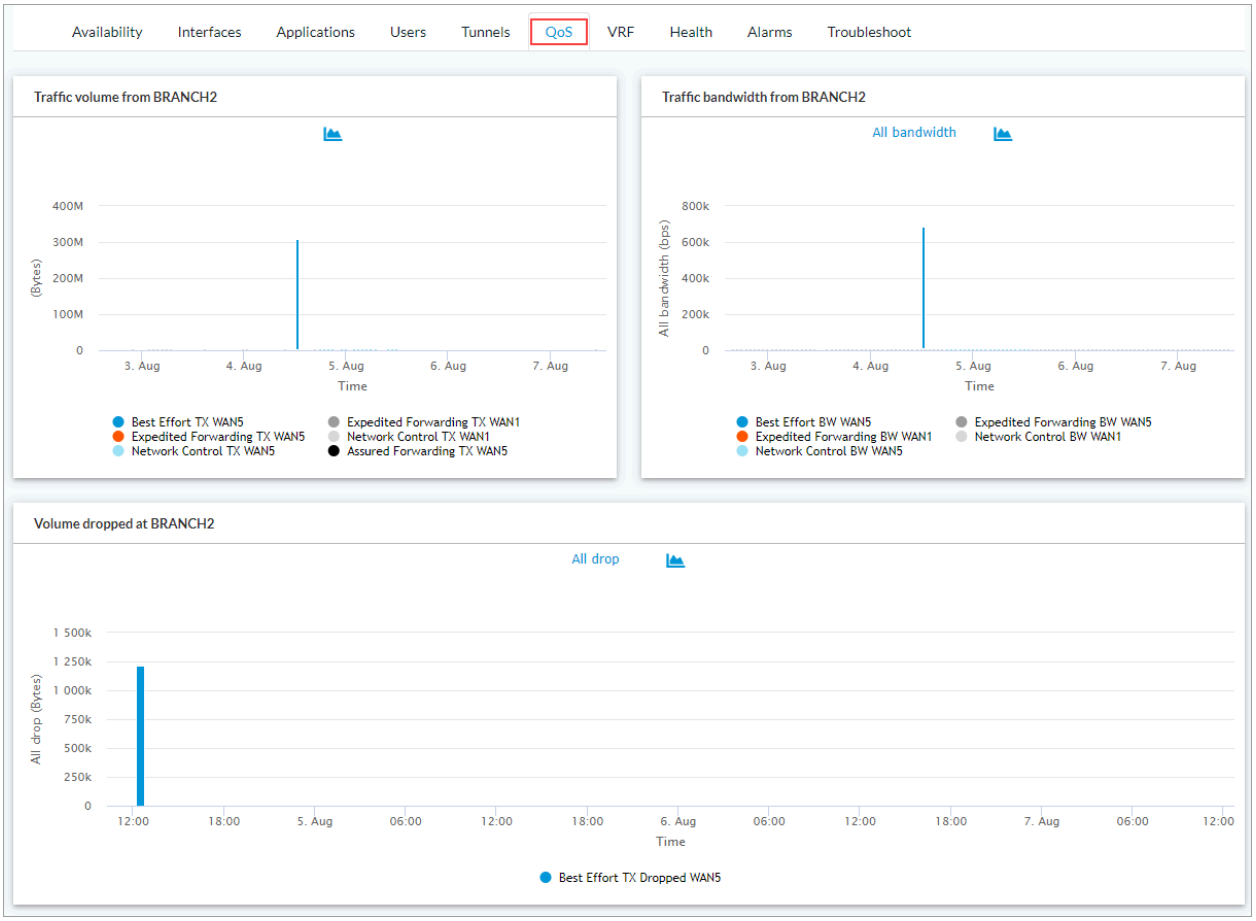
The QoS tab displays information about the QoS traffic and packet drops.

To view QoS information:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Click QoS tab. The QoS tab displays the following panes:
   - Traffic Volume (chart)
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.
   - Traffic Bandwidth (chart)
     - By All Bandwidth, Assured Forwarding, Best Effort, Expedited Forwarding, Network Control
     - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.

Updated: Wed, 23 Oct 2024 08:54:28 GMT

- Volume Dropped (chart)
  - By All Drop, Assured Forwarding, Best Effort, Expedited Forwarding, Network Control
  - To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.



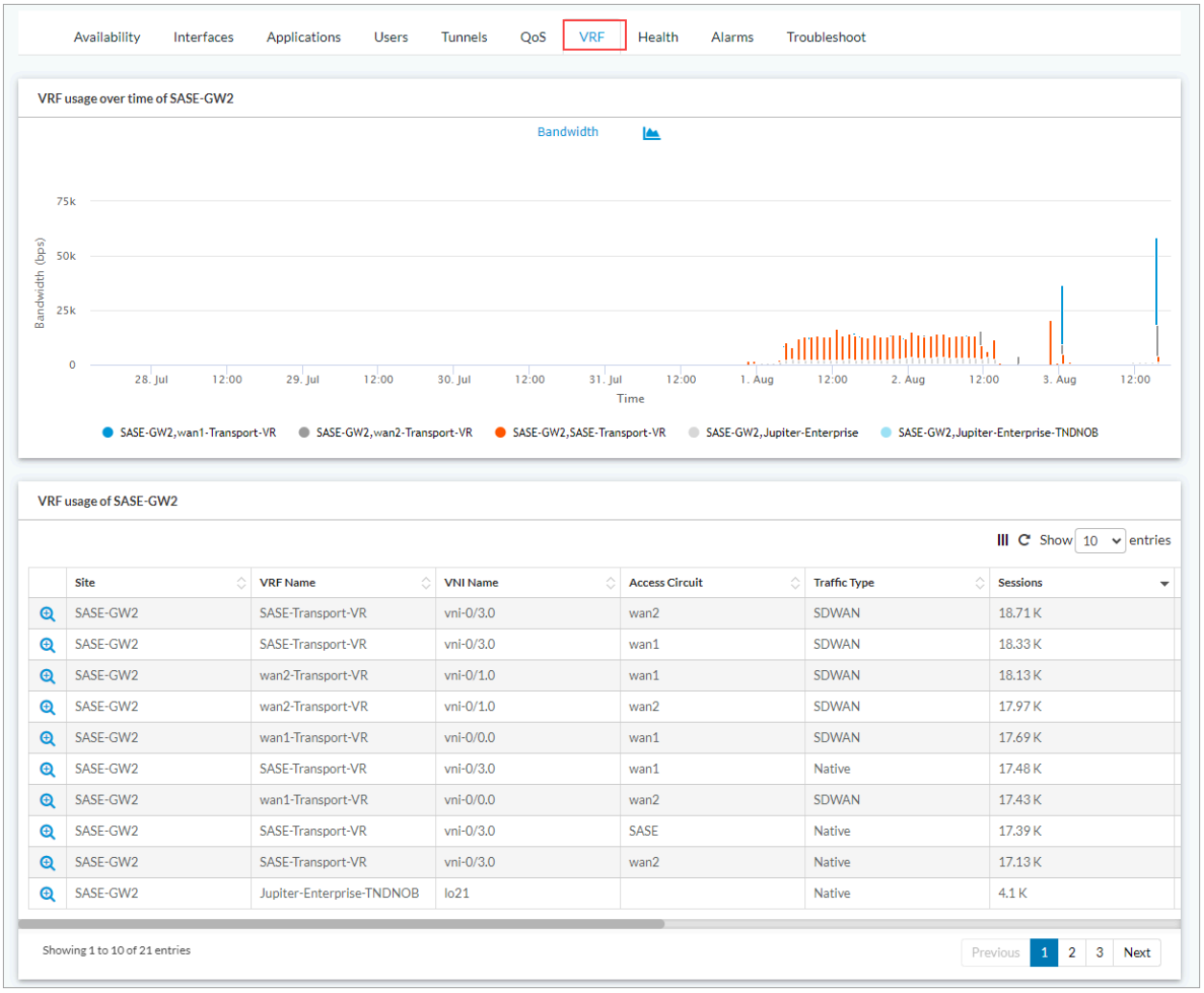
View VRF Information

For Release 11.4.1 and later.

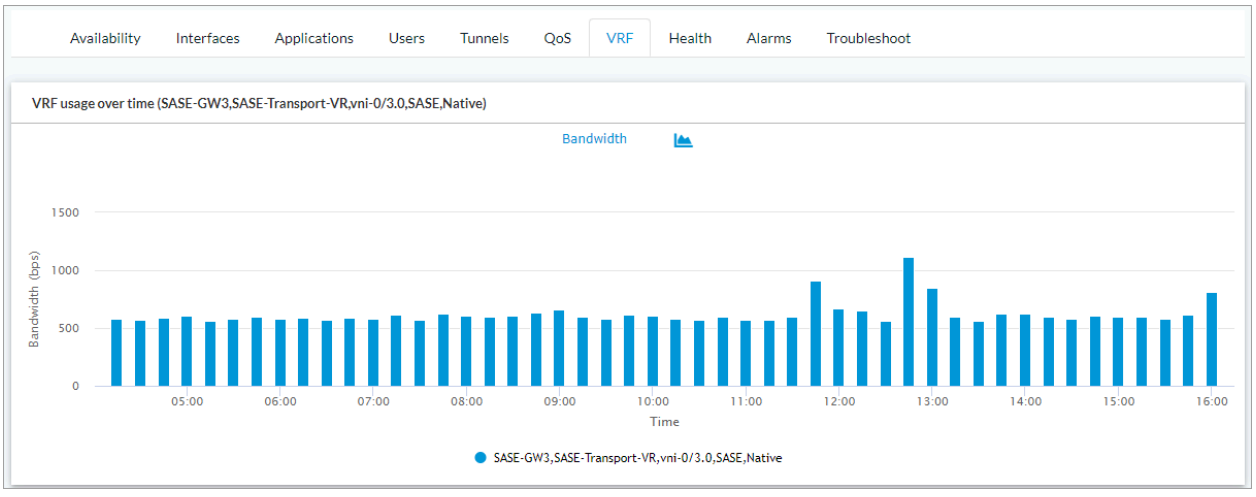
The VRF tab displays information about virtual routing and forwarding.

To view VRF information:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. To view the VRF usage information, select the VRF tab.



3. To view the VRF usage for each device, click the Zoom icon.



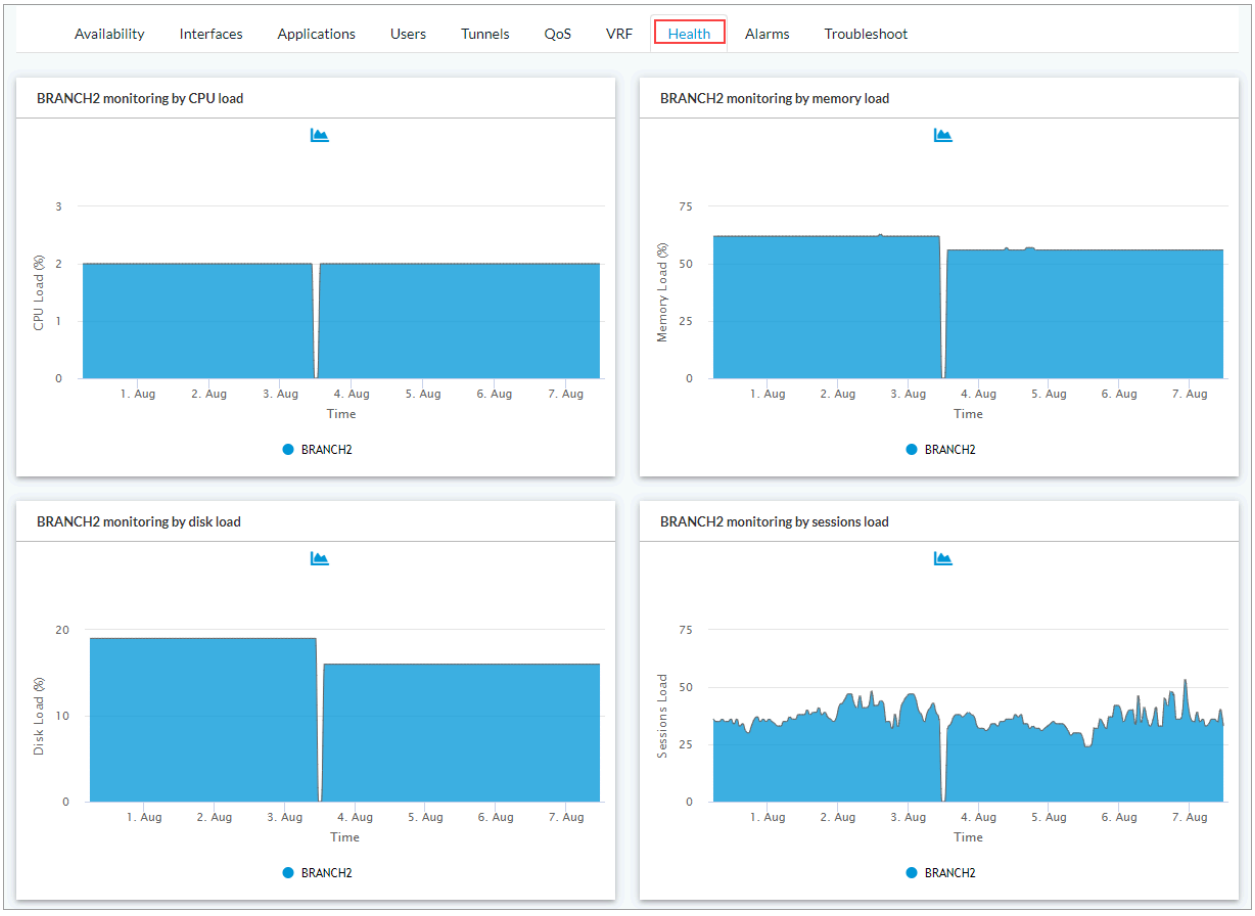
View Device Health Information

For Release 11.4.1 and later.

The Health tab displays current system load information for a device, including real-time CPU, system memory, disk, and sessions usage.

To view health information:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Click Health tab. The Health tab displays the following panes:
   - Device monitoring by CPU load
   - Device monitoring by memory load
   - Device monitoring by disk load
   - Device monitoring by sessions load



3. To change the graphical representation of data, click theChart Menu icon, and then select the graphical data representation format. The format can be Area, Column, Line, Scatter, or Stacked Column.

Updated: Wed, 23 Oct 2024 08:54:28 GMT

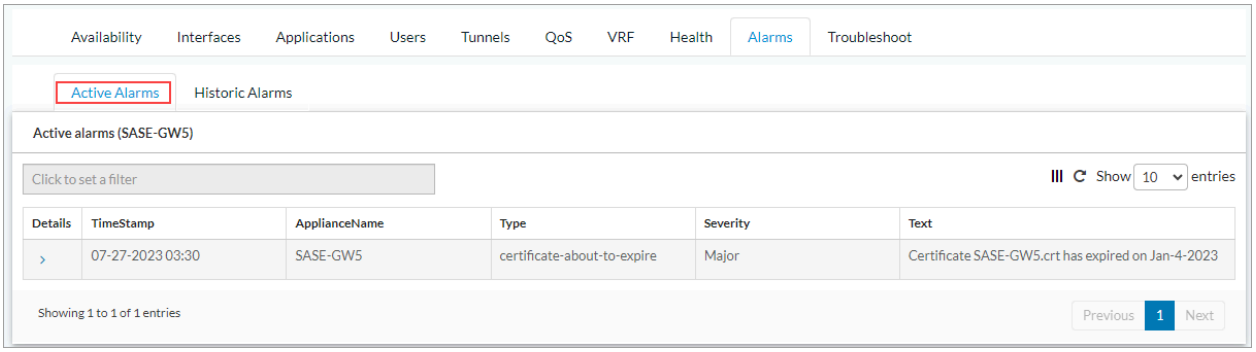
View Alarm Information

For Release 11.4.1 and later.

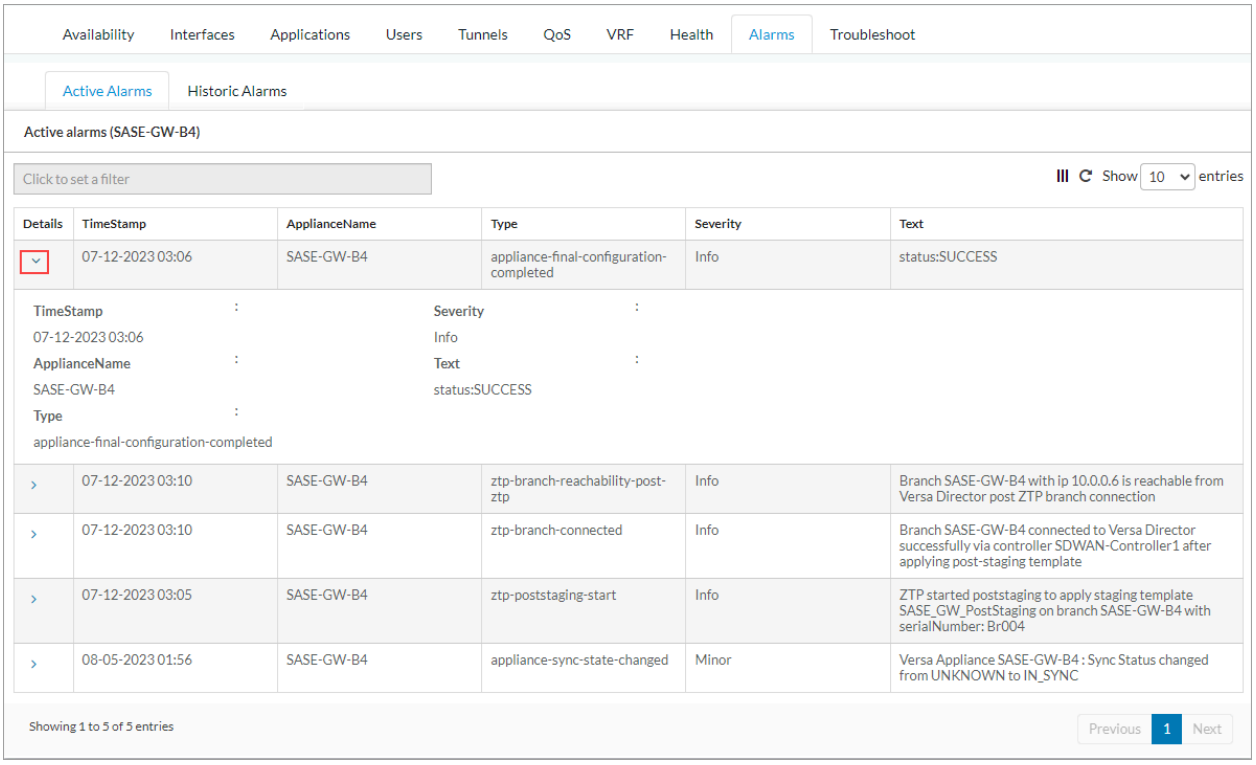
The Alarms tab displays information about the active and historic alarms.

To view alarm information:

1. Click View > Secure SD-WAN > Overview, and then select a device in the Select an Appliance field in the horizontal menu bar or in the device list in Map View or List View.
2. Select the Alarms tab, and then click Active Alarms tab to view the active alarms.

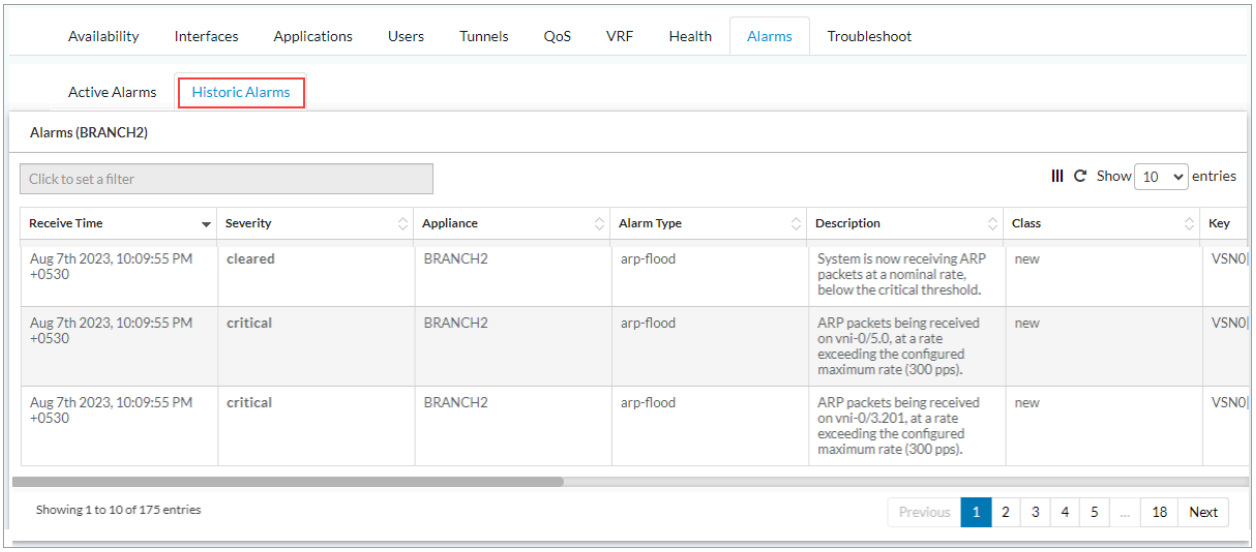


3. To view alarm details, click the arrow in the Details column.



4. To view historic alarms, select the Historic Alarms tab.

Updated: Wed, 23 Oct 2024 08:54:28 GMT

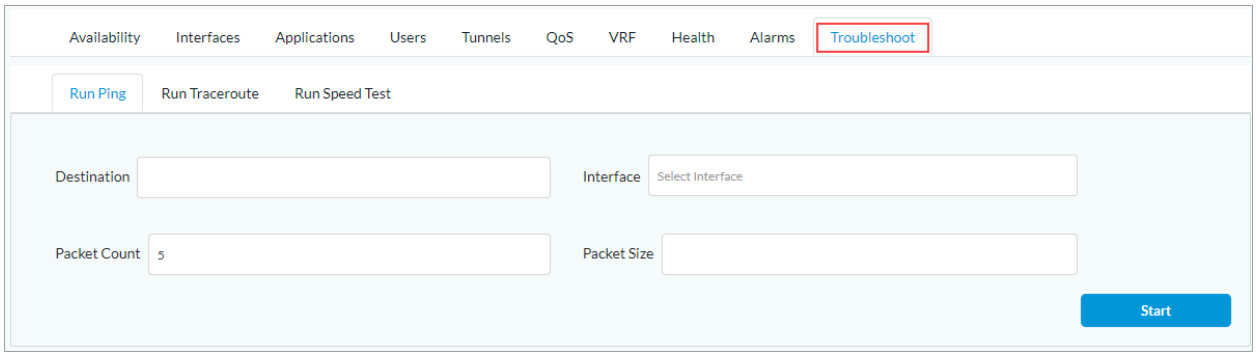


Access Monitoring Tools

You can monitor the network using the ping, tcpdump, and traceroute commands, and you can run a speed test.

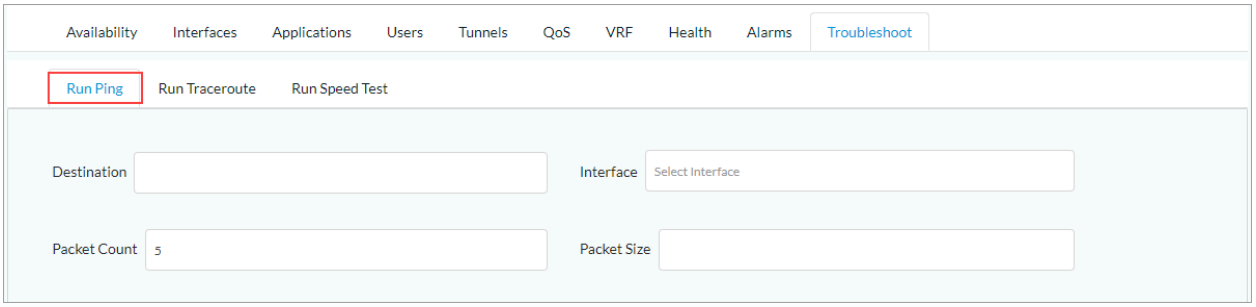
To access tools to monitor devices in the network:

1. In the SD-WAN Overview screen, select a device from Map View or List View.
2. Select Troubleshoot tab. The Troubleshoot tab has the following tabs:
   - Run Ping
   - Run Traceroute
   - Run Speed Test



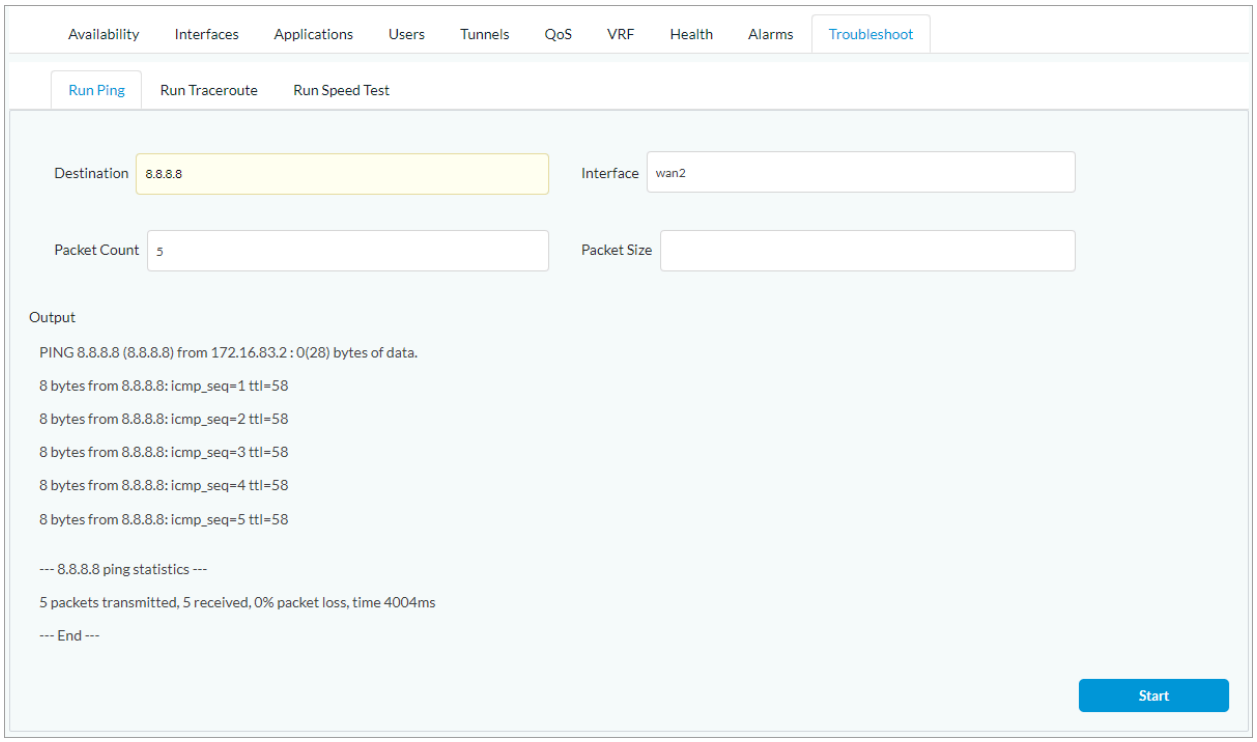
Run a Ping Test

1. In the Troubleshoot tab, select the Run Ping tab, and then enter information for the following fields.



Field	Description
Destination	Enter the IP address of destination to which the packets are sent.
Interface	Select the interface to use as the source address. Optionally, enter the packet size, in bytes. *Range:* 0 thorugh 65535 bytes *Default:* None
Packet Count	Enter the number of packets to send. *Range*: 1 through 25 *Default*: 5
Packet Size	Enter the packet size, in bytes. *Range:* 0 through 65535 bytes *Default:* None

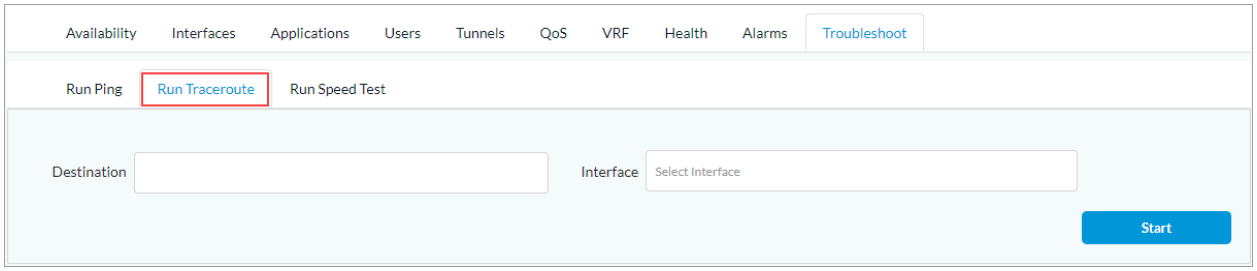
2. Click Start. After the ping diagnostic test completes, a screen similar to the following displays.



Run Traceroute

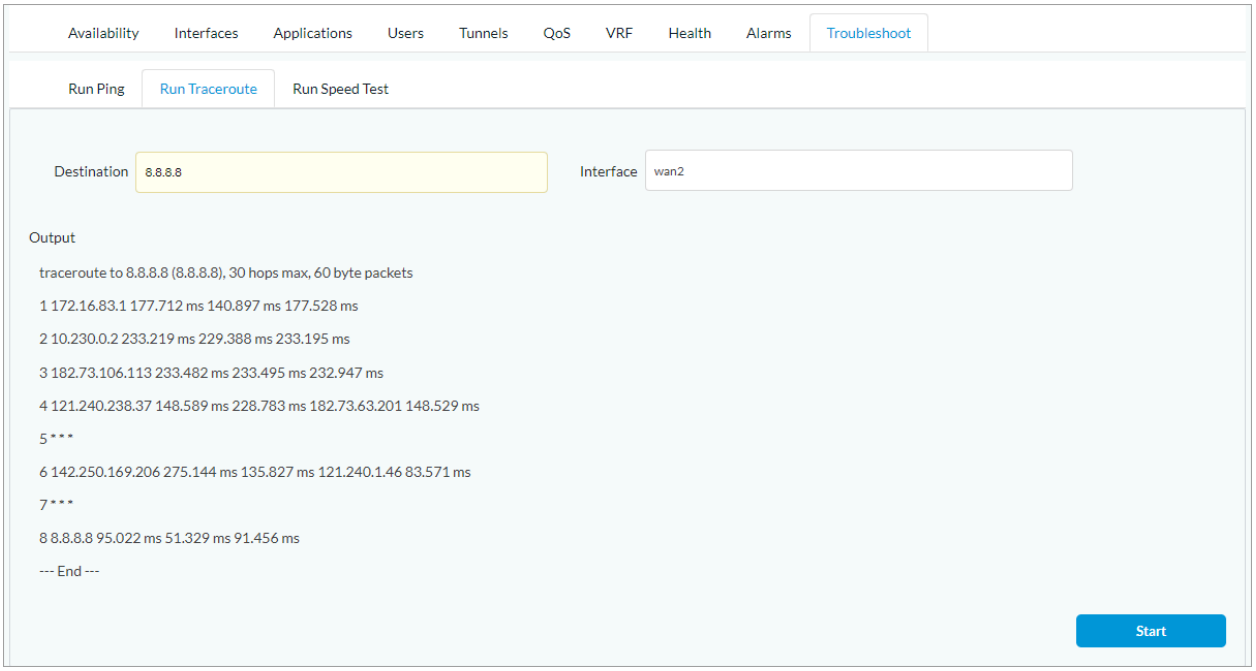
To trace a route:

1. In the Troubleshoot tab, select the Run Traceroute tab, and then enter information for the following fields.



Field	Description
Destination	Enter the IP address or FQDN of the target host.
Interface	Select the interface that initiates the traceroute.

2. Click Start. After a traceroute diagnostic test completes, a screen similar to the following displays.



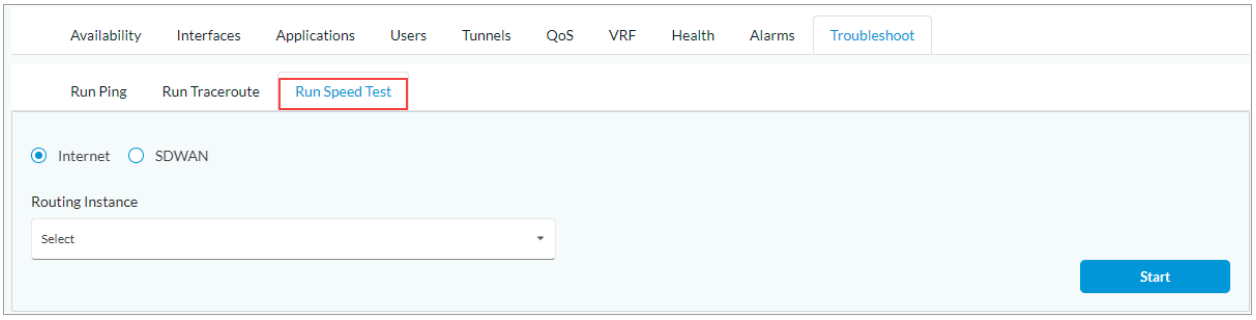
Run Speed Test

You can run two types of speed tests: Internet speed tests and Versa speed tests:

- Internet speed test—You run internet speed tests from Versa Operating System™ (VOS™) devices using predeployed internet speed-test servers. To run an internet speed test, the VOS device must have an internet connection over a WAN link. The internet speed test chooses the nearest predeployed speed-test server. You do not need to deploy an independent speed-test server.
- Versa speed test—You use a WAN interface that has been configured as a Versa speed-test server.

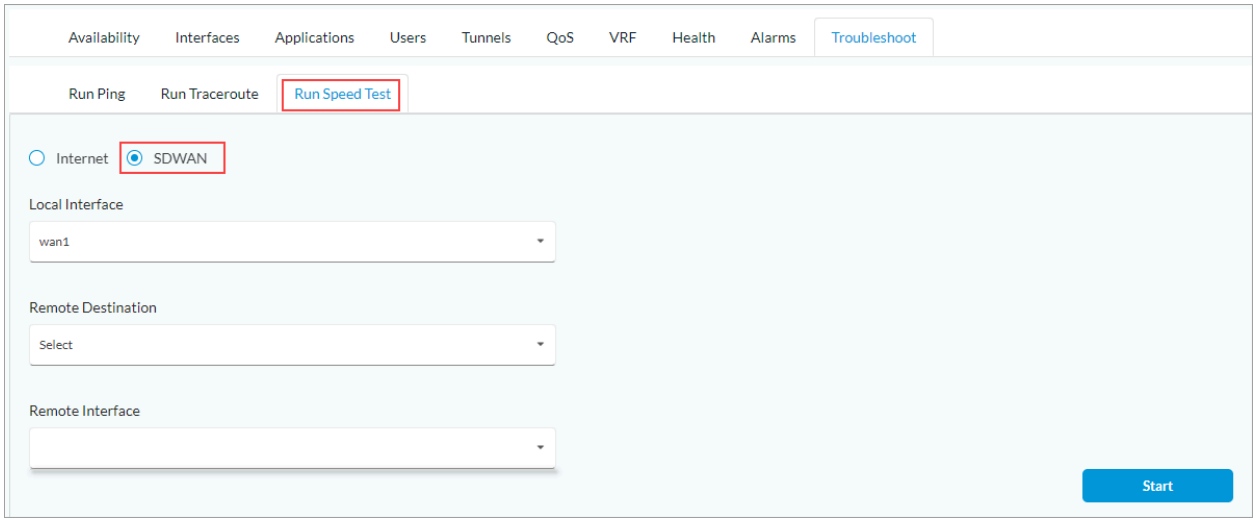
To run a speed test:

1. in the Troubleshoot tab, select Run Traceroute.
2. To run an internet speed test, select Internet.



   a. Select the routing instance to use to connect to the predeployed internet speed-test server.
   b. Click Start.

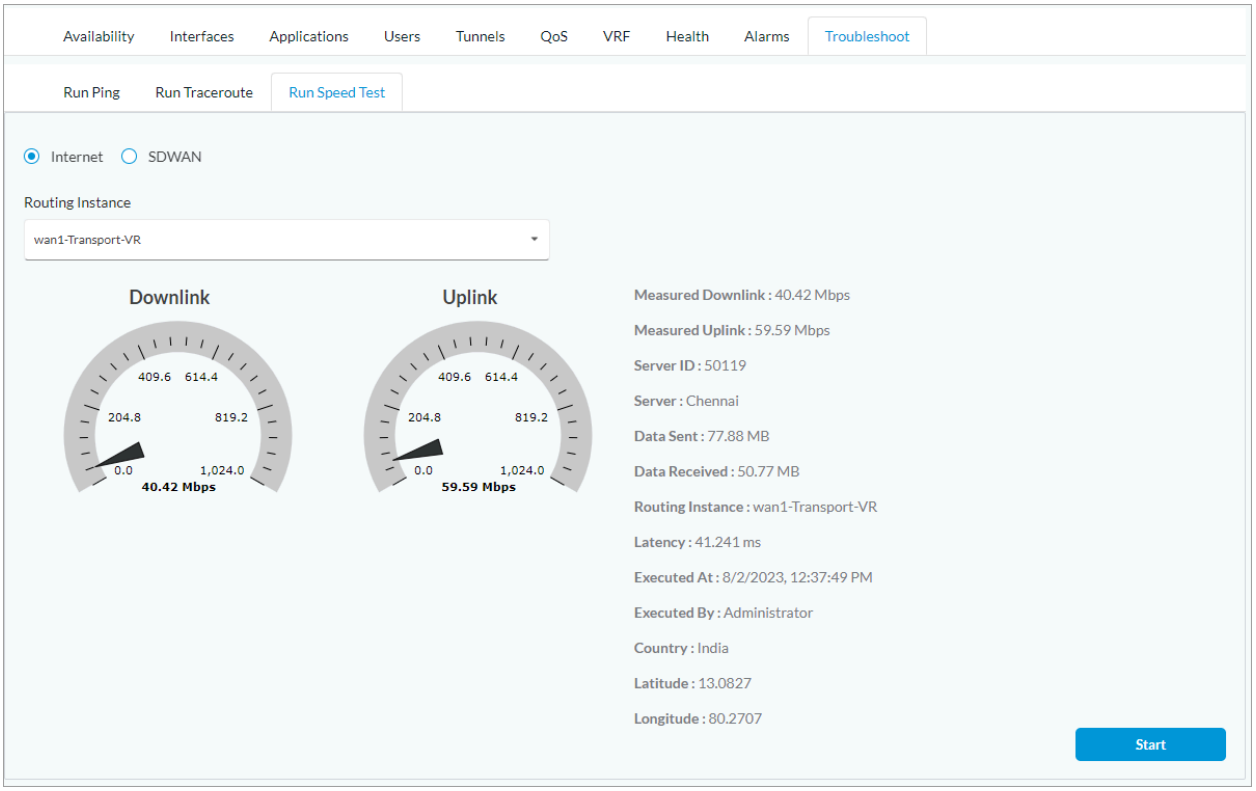
3. To run a SD-WAN speed test, select SD-WAN, and then enter information for the following fields.



Field	Description
Destination	Enter the IP address of destination to which the packets are sent.
Local Interface	Select the local interface to use for the speed test.
Remote Destination	Select the remote destination to use for the speed test.
Remote Interface	Select the remote interface to use for the speed test.

4. Click Start. After the speed test diagnostic test completes, a screen similar to the following displays.

Updated: Wed, 23 Oct 2024 08:54:28 GMT



Supported Software Information

Releases 11.3.1 and later support all content described in this article, except:

- Release 11.3.2 adds support for downloading CSV files showing information about alarms on SD-WAN devices.
- Release 11.4.1 adds Availability, Users, Tunnels, QoS, VRF, Health, and Alarms tabs in Monitor Device Interfaces.
- Release 12.1.1 adds support for Digital Experience.

Additional Information

Concerto Analytics
Monitor Concerto Orchestrator