Cisco vAnalytics Version 2.5

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Overview and Onboarding

Cisco vAnalytics is a cloud-based service that offers insights into the performance of applications and the underlying SD-WAN network infrastructure.

Cisco vAnalytics offers the following insights:

- Multi-Layer Insights on Application Behavior
  - Application Quality of Experience (QoE)
  - Bandwidth usage
  - Distribution across sites, devices, tunnels, and carrier links

  Use this information to review usage of various applications over time in a given infrastructure, assess end-user experience with these applications, and correlate end-user experience with the underlying network performance.

- Contextual Network Visibility
  - Loss, latency, and jitter on the underlying network tunnels
  - Traffic distribution across sites, devices, tunnels and circuits

  - Availability information of circuits and devices
  - Top users and top flows

  Use this information to correlate application experience with the underlying network conditions.

- Aggregate-level assessment through views across Application Families and Classes
  - Application families are broad categories used to group together applications based on their use.
  - Application classes are broad categories used to group together applications based on their behavior and network performance requirements.

  Use this information to assess behavior of applications as a group to identify if there are broader systemic issues.

Cisco vAnalytics collects and stores metadata about traffic flows in its cloud storage and provides analytics based on the data for a maximum of four weeks. This service is available with a DNA Advantage or DNA Premier license.

Changes in Cisco vAnalytics Version 2.5

- Cisco vAnalytics provides analytics based on the collected and stored data up to the past four weeks.
- The Summary dashboard does not include a count of the SD-WAN tunnels.
- The Flow category provides analytics on only the top talkers. Analytics for top flows and top destinations are deprecated.

Onboarding Cisco vAnalytics

To onboard Cisco vAnalytics for your overlay for the first time, open a case with Cisco Support here: https://mycase.cloudapps.cisco.com/case. After your vAnalytics instance is created, enable data collection in your vManage configuration as described in the respective section below.

In a multitenant deployment, each tenant must onboard a Cisco vAnalytics instance for the tenant overlay network.

If you have an existing Cisco vAnalytics instance for your overlay and are upgrading your Cisco vManage to release 20.3 or later, you must perform an additional OTP configuration on Cisco vManage to allow for data collection by Cisco vAnalytics. Refer to the steps outlined in the *Enable Data Collection* sections below. If necessary, open a Cisco Support case to obtain your OTP.

Cisco vAnalytics leverages Okta Identity Provider (IDP) in the backend to authenticate users before giving users access to the Cisco vAnalytics portal. During initial onboarding, you will receive an e-mail from Okta (on behalf of Cisco) to activate the user account and set a password for accessing Cisco vAnalytics. After your user account is established, access Cisco vAnalytics using its URL.

Note The direct cross launch from Cisco vManage currently takes you to the previous version (version 1.0) of Cisco vAnalytics. The cross launch will be updated to take you to Cisco vAnalytics version 2.5 in a future release.

Request New Cisco vAnalytics Instance

Open a support case with Cisco, https://mycase.cloudapps.cisco.com/case, and provide the following information:

- Customer Name
- Org Name (as configured on Cisco vManage)
- License type (DNA license type)
- Approve metadata collection by vAnalytics: (Yes | No)
- Approval date
- Customer e-mail
- Cisco Contact
- Cisco vManage deployment (cloud-hosted | on-prem)
- Cisco vManage software version
- Cisco vManage Geographic location (Americas | Europe | Australia | country)
- Cisco vManage tenancy (Single-tenant | Multitenant)
- Migrating from v1? (Yes | No)

After receiving this information, Cisco takes approximately 24 to 48 hours to prepare and deploy the Cisco vAnalytics instance.

Cisco vAnalytics collects metadata about traffic flows, events, activity, and inventory in the Cisco SD-WAN overlay network to provide analytics about traffic flows, network conditions, and application experience. The metadata is exported from Cisco vManage to Cisco vAnalytics using secure API at periodic intervals of 30 minutes. The Cisco privacy data sheet describes how Cisco SD-WAN Cloud handles data.

The following are some groups of metadata exported from Cisco vManage to Cisco vAnalytics:

- Device configurations
- Device statistics
- Interface statistics
- Alarm statistics
- Audit logs
- SD-WAN Application Intelligence Engine (SAIE) flow statistics

  Note In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

- AppRoute statistics
- SpeedTest results

- URL/AMP filtering data

Enable Data Collection (Cisco vManage Release 20.3 or later)

Note In a multitenant deployment, a provider **admin** user must enable cloud services in the provider view.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Find **Cloud Services** and click **Edit**.
3. For the **Cloud Services** field, click **Enabled**.
4. Enter the **OTP**.

   Cisco shares the OTP after creating the Cisco vAnalytics instance.

   If both the Cisco vManage and Cisco vAnalytics instances are being newly created, Cisco enables Cloud Services and enters the OTP while configuring the Cisco vManage instance.

   If you have an existing Cisco vAnalytics instance for your overlay and are upgrading your Cisco vManage to software release 20.3 or later, open a case with Cisco TAC support to request OTP.
5. Check the **vAnalytics** check box.
6. Check the **I agree...** check box.
7. Click **Save**.
8. Access Cisco vAnalytics using one of the following URLs based on the location of your Cisco vAnalytics instance:
   - Americas — https://us01.analytics.sdwan.cisco.com/
   - Americas (East) — https://us02.analytics.sdwan.cisco.com/
   - Europe — https://eu01.analytics.sdwan.cisco.com/
   - Australia — https://au01.analytics.sdwan.cisco.com

Enable Data Collection (Cisco vManage Release 20.1 or earlier)

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Find **vAnalytics** and click **Edit**
3. For the **Enable vAnalytics** field, click **Enabled**.
4. Enter **SSO Username** and **SSO Password**.

   The username and password are not used while collecting data. Enter a dummy username and a password of your choice.
5. Check the **I agree...** check box.
6. Click **Save**.

7. Access Cisco vAnalytics using one of the following URLs based on the location of your Cisco vAnalytics instance:

   - Americas — https://us01.analytics.sdwan.cisco.com/
   - Americas (East) — https://us02.analytics.sdwan.cisco.com/
   - Europe — https://eu01.analytics.sdwan.cisco.com/

Additional Step for Enabling Data Collection on an On-Premises Cisco vManage Instance

Configure the local firewall to allow outbound communication from Cisco vManage (interface VPN 0) on port 443 to the destinations in the following table. Choose the appropriate set of destinations based on the geographic location of your Cisco vAnalytics instance.

Location	Destinations
Americas	https://us-west.dcs.viptela.net (Cisco vManage Release 20.1 or earlier) https://us01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3 or later)
Americas (East)	https://us-east.dcs.viptela.net (Cisco vManage Release 20.1 or earlier) https://us02.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3 or later)
Europe	https://europe.dcs.viptela.net (Cisco vManage Release 20.1 or earlier) https://eu01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3 or later)
Australia	https://au01.datagateway.analytics.sdwan.cisco.com (Cisco vManage Release 20.3 or later) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage Release 20.3 or later)

You can use the cURL -k command from your Cisco vManage CLI to verify reachability to these destinations.

Access Cisco vAnalytics

Access Cisco vAnalytics using one of the following URLs based on the location of your Cisco vAnalytics instance:

- Americas — https://us01.analytics.sdwan.cisco.com/
- Americas (East) — https://us02.analytics.sdwan.cisco.com/

- Europe — https://eu01.analytics.sdwan.cisco.com/
- Australia — https://au01.analytics.sdwan.cisco.com

The portal presents analytics in the following categories:

- Dashboard – Summary view of the SD-WAN network and application performance
- Applications – Analytics on application usage and behavior
- Network – Analytics on SD-WAN network fabric performance
- Flows – Analytics on top talkers

Note

- Cisco vAnalytics does not include Direct Internet Access (DIA) statistics at this time.
- Cisco vAnalytics accounts for only the egress traffic. So, you may notice variations between application usage statistics reported by Cisco vManage and the statistics reported by Cisco vAnalytics.

Authentication and Authorization

Authentication

Cisco vAnalytics users can log in using one of the following IDs:

- Cisco CCO ID: The ID that they use to log in to Cisco Software Central.
- My Organization ID: The ID defined in and authenticated by their organization's identity provider (IdP).

  Note The organization IdP must support the SAML 2.0 or the OIDC protocol to interoperate with Cisco vAnalytics.

- Existing Okta ID: The Cisco-assigned Okta ID.

  Note Support for the Okta IdP will be deprecated in the months to come. The option to use the Okta IdP for authentication is a temporary measure to allow existing users to transition to either the Cisco IdP or their organization's IdP. If you are using Okta IDs, we recommend that you switch to a supported IdP at the earliest.

Authorization

You can authorize Cisco vAnalytics users to have access to select overlays and operations.

Authorization with Cisco CCO ID

You can manage user access and operational privileges through Cisco Software Central. Each overlay is associated with a Virtual Account. To allow a user to access Cisco vAnalytics for a particular overlay, add the user to the Virtual Account in one of the following capacities:

- Virtual Account Administrator: The user can access all Cisco vAnalytics screens for the overlay. In addition, the user can configure the IdP to be used for user authentication for the overlay.
- Virtual Account User: The user can access all Cisco vAnalytics screens for the overlay.

Alternatively, you can add a user to a Smart Account. Doing so allows the user to access Cisco vAnalytics for every overlay that is associated with a Virtual Account belonging to the Smart Account. This option of adding a user at the Smart Account level is especially useful for managed service providers (MSPs) and enterprises managing multiple overlays. You can add a user to a Smart Account in one of the following capacities:

- Smart Account Administrator: The user can access all Cisco vAnalytics screens for all the overlays. In addition, the user can configure the IdP to be used for all the overlays or configure the use of an organization IdP for a particular overlay.
- Smart Account User: The user can access all the Cisco vAnalytics screens, except the Microsoft 365 Cloud OnRamp screens, for all the overlays.

Note A Smart Account Approver has the same privileges as a Smart Account User.

Authorization with Organization ID

When authenticated by their organization's IdP, users are granted access to overlays and operations based on the role assigned to them using the `authzCiscovAnalytics` attribute on the IdP or the default role assigned to users while defining organization IdP on Cisco vAnalytics.

A user can be assigned the following roles:

- The `basic` role allows a user to access all the Cisco vAnalytics screens for the overlay except the Microsoft 365 Cloud OnRamp screens.
- The `o365` role allows a user to access the Microsoft 365 Cloud OnRamp screens.

  You can assign both the `basic` and `o365` roles to an user to enable the user to access all the Cisco vAnalytics screens for the overlay.
- The `admin` role allows a user to access all the Cisco vAnalytics screens for the overlay. In addition, the user can also define an IdP for the overlay.

Use the following syntax to specify the default role or a value for the `authzCiscovAnalytics` attribute:

```
<syntax-version>;<overlay-1>:<role1>[,<role2>][;<overlay-2>:<role1>[,<role2>]]...
```

Currently, only one version of the syntax is supported and you must specify the syntax version as `v1`.

You can specify an overlay name and the user privileges for the overlay in the format: `<overlay-1>:<role1>[,<role2>]`.

- To assign the same privileges to the user for all the overlays, specify the overlay name as `*`. Further, if a set of overlays share a part of their name, you can specify the set of the overlays using a combination of the shared part of the name and the wildcard character `*`.

  If you're configuring the IdP for a single overlay, specify the overlay name as `*`.

First Login to Cisco vAnalytics

After a Cisco vAnalytics instance is created for your overlay network, the administrator must log in to Cisco vAnalytics with their CCO ID. On logging in, the administrator sees either the **Smart Accounts** or the **Dashboard** screen.

If the administrator belongs to more than one Virtual Account, Smart Account, or both, the administrator sees the **Smart Accounts** screen. The **Smart Accounts** screen lists the Smart Accounts and Virtual Accounts to which the administrator is subscribed. Each Virtual Account represents an overlay network.

The administrator sees the **Dashboard** if the administrator belongs to only one Virtual Account and Smart Account, and therefore, has access to only one overlay. From the **Dashboard**, you can access the **Smart Accounts** screen by clicking **View all overlays**.

For an overlay, if a Cisco vAnalytics instance has been onboarded, the entry under **vAnalytics Status** reads **Activated**; if a Cisco vAnalytics instance is not onboarded, the entry reads **New**. If a Cisco vAnalytics instance is available for an overlay, you can launch the **Dashboard** for overlay by clicking on the overlay or Virtual Account name.

Note If the **vAnalytics Status** for an instance reads **New**, but you are aware that the instance has been onboarded, verify whether you have logged in using the correct Cisco vAnalytics URL.

The entry under **IDP Server** indicates whether your organization's IdP is configured to be used with the overlay or not (**Not Defined**).

To configure an IdP for an overlay for which Cisco vAnalytics has been activated, click **...** under **Actions**, and click **Define IDP**. For more information on defining the IdP, see Define Organization IdP for Overlays.

Define Organization IdP for Overlays

As an administrator for a Smart Account, you can configure your organization's IdP to be used for authenticating Cisco vAnalytics users for all or some of the overlays. As an administrator for a Virtual Account or an overlay, you can configure your organization's IdP to be used for authenticating Cisco vAnalytics users for the overlay.

1. Log in to Cisco vAnalytics.

   Note If this is your first login to the Cisco vAnalytics instance created for your overlay, log in with the Cisco CC ID. The organization IdP you define for the overlay authenticates and authorizes users in subsequent log-i attempts.

2. If you see the **Dashboard**, click **View all overlays** to go to the **Smart Accounts** screen.
3. Configure your organization's IdP for a Smart Account or the overlay associated with a Virtual Account:
   1. To configure your organization's IdP for a Smart Account, click **Define IDP**.
   2. To configure your organization's IdP for an overlay, hover the mouse pointer over **...** under **Actions**. Then, click **Define IDP**.
4. In the **Define IDP** dialog box, click **OIDC IDP** or **SAML IDP**.
   1. For an SAML 2.0 IdP, do the following:

Table 1: SAML IdP Properties

IDP Metadata	Click browse file and upload the SAML 2.0 metadata file to Cisco vAnalytics. Cisco vAnalytics reads the SAML 2.0 file and displays the following details: • **IDP Issuer URL** • **IDP Single Sign-on URL** • **IDP Signature Certificate Expiry (days)**
Default User Role	Configure a default role for Cisco vAnalytics users. The default role is used if a role is not assigned to a user on the IdP. **Note** In addition to specifying a default role while defining an IDP, you can manage user access and operational privileges by defining a `authzCiscovAnalytics` attribute for users on your organization's IdP. For more information on the available roles and the syntax to be used for specifying the roles, see Authorization with Organization ID.
Domain Identifier	Specify the domain identifier contained by every user ID. For example, if user IDs defined on your organization's IdP have the format `userID@example.com`, the common domain identifier is `example.com`.

b. For an OIDC IdP, do the following:

Table 2: OIDC IdP Properties

IDP Metadata	Enter the following OIDC properties for your organization's IdP: • **Client ID** • **Client Secret** • **Issuer** • **Authorization Endpoint** • **Token Endpoint** • **JWKS Endpoint** • **Userinfo Endpoint**

Default User Role	Configure a default role for Cisco vAnalytics users. The default role is used if a role is not assigned to a user on the IdP. **Note** In addition to specifying a default role while defining an IDP, you can manage user access and operational privileges by defining a `authzCiscovAnalytics` attribute for users on your organization's IdP. For more information on the available roles and the syntax to be used for specifying the roles, see Authorization with Organization ID.
Domain Identifier	Specify the domain identifier contained by every user ID. For example, if user IDs defined on your organization's IdP have the format `userID@example.com`, the common domain identifier is `example.com`.

c. Click **Save**.

5. To complete the IdP definition, send the required claims with non-empty values:
   a. For an SAML 2.0 IdP, download the IdP metadata file and send the four claims listed in the file.
   b. For an OIDC IdP, send the firstName, lastName, and email.

Any users logging in to Cisco vAnalytics after the IdP is configured are redirected to the IdP's page for authentication.

Manage a Defined Organization IdP

As an administrator for a Smart Account, you can view, modify, or delete the organization IdP defined for authenticating Cisco vAnalytics users for all or some of the overlays. As an administrator for a Virtual Account or an overlay, you can view, modify, or delete the organization IdP defined for authenticating Cisco vAnalytics users for the overlay.

1. Log in to Cisco vAnalytics.
2. If you see the **Dashboard**, click **View all overlays** to go to the **Smart Accounts** screen.
3. To manage a defined IdP, hover the mouse pointer over **...** under **Actions**.
   - To view the IdP properties, click **View IDP**.
   - To modify the IdP properties, click **Edit IDP**.

     You can edit only the default user role and domain identifier for a defined IdP. If you need to modify any other properties, you must delete the IdP definition, and define the IdP again.
   - To delete the defined IdP, click **Delete IDP**.

After you delete the IdP, Cisco vAnalytics users cannot log in using IDs that are defined in and authenticated by the organization IdP. Any user sessions that are active when the IdP is deleted are not ended, but subsequent log-in attempts fail.

Screen Elements

Each category has multiple pages which in turn include graphs, tables, aggregate counts, and other such performance measures.

The graphs use either a bar chart or a line chart. You can click on a bar or a line to view more details. For example, if you click on a bar representing an application performance measure, you can view more details about the application.

The graphs are generally ordered by the value of the respective performance measure. Some graphs have additional tab options to change the default sorting order.

Some pages include both tables and graphs with a few pre-selected entries. You can uncheck or check up to a maximum of five entries in the table to view the respective graphs.

The tables may also be sorted by various column fields, from High to Low or Low to High. Additionally, many of the data points include hyperlinks and you can view additional contextual information by clicking on the links.

The pages and tabs have the following configurable aspects:

Time Window: Choose the time window for which you wish to view the analytics. The default time period is the past 12 hours. You can change the time period to the past 24 hours, 7 days, or 4 weeks.

Filter Options: Use the filter options to focus the analytics on a more granular level. The filter options available depend on the category of analytics. For example, while viewing application-level analytics, you can apply filters to view the analytics for a particular application instance hosted at a specific site.

Sort Order: With a table of counts and performance measures, you can choose the count or performance measure to be used as the basis for listing the table entries. You can further sort the entries in a High to Low or Low to High order based on the value of the chosen count or performance measure.

Alternatively, you can hover the mouse pointer on a column name in the table and click the Up or Down arrows that appear next to the name to sort table entries in the ascending or descending order of values in the column.

Rows: By default, tables display a maximum of 100 rows. You may choose to display 10, 100, 250, or 500 rows in the table.

You can expand a page to fill the screen or download a snapshot of the page by clicking the appropriate button at the top-right corner of the page.

Dashboard

Summary

The Summary dashboard is the first page you see when you log in to Cisco vAnalytics.

This page offers a quick summary of the entire SD-WAN infrastructure, including usage, performance, and aggregate count of key constituents such as applications, sites, devices, and circuits.

Page Element	Description
Counts	Total number of applications, WAN sites, and WAN edge devices.
Application Usage	The graph summarizes bandwidth usage for a maximum of 10 applications. Default Selection: Top applications by bandwidth usage, ordered High to Low. Click on a bar to view more details about the selected application.
Application Performance	This graph summarizes application performance through one of the following four measures for up to 10 applications. • Quality of Experience (QoE): A 0 (lowest) to 10 (highest) score reflecting end-user experience. The QoE score is computed from observed latency, loss, and jitter values, customizing the calculation according to the needs of each application. • Loss: Packet loss • Latency: Network latency • Jitter: Network jitter Default Selection: Top applications by QoE, ordered High to Low. Click on a bar to view more details about the selected application.
WAN Sites – Usage and Performance	This graph summarizes various performance measures for up to five SD-WAN sites. Default Selection: Top WAN sites by bandwidth usage, ordered High to Low. Click on a line to view more details about a site.
Carrier Usage	This table summarizes the behavior of various carrier links used in the overlay network. Click on the name of a carrier to view more details about it.

Application Dashboard

This page offers a quick summary of applications, application families, application classes, and their behavior.

Page Element	Description
Counts	Number of applications, application families, and application classes.
Application Usage and Performance	The graph summarizes bandwidth consumption, QoE, loss, latency, jitter, and device count for a maximum of 10 applications. Default Selection: Top applications by bandwidth usage, ordered High to Low. Click on a line to view more details about an application.

Application Usage	The graph summarizes the bandwidth usage for a maximum of 10 applications. Default Selection: Top applications by bandwidth usage, ordered High to Low. Click on a bar to view more details about an application.
Application Performance	The graph summarizes one of the performance measures QoE, loss, latency, or jitter for a maximum of 10 applications. Default Selection: Top applications by QoE, ordered High to Low. Click on a bar to view more details about an application.
Application Family Usage	Application families are broad categories used to group together applications based on their use. For example, all database management applications are grouped together under the application family ‘database’. Similarly, applications dealing with audio or video traffic types are grouped under the application family ‘audio/video’. This graph summarizes bandwidth usage across various application families. Default Selection: Top application families by bandwidth usage, ordered High to Low. Click on a bar to view more details about an application family.
Application Family Performance	The graph summarizes one of the performance measures QoE, loss, latency, or jitter for a maximum of 10 application families. Default Selection: Top application families by QoE, ordered High to Low. Click on a bar to view more details about an application family.
Application Class Usage and Performance	Application classes are broad categories used to group together applications based on their behavior and network performance requirements. For example, applications involving client-server communication in real-time are grouped under the application class ‘real-time’. Such applications generally require low delay, loss, and jitter. This table summarizes performance measures against the classes of applications observed in a given overlay. Click on the name of an application class to view more details about it.

Popular Applications Dashboard

This page offers the summarized performance information of the two popular applications Microsoft Office 365 (O365) and Cisco Webex.

Page Element	Description
Counts	Number of applications, WAN sites, WAN edge devices and tunnels.
Application QoE Performance	The graph shows how the average QoE of applications varied during the time window. Hover the mouse pointer on the graph to see the average QoE values of the applications at a particular time.

Application Usage	This graph summarizes bandwidth usage for individual applications that fall under Microsoft O365 or Cisco Webex family of applications. Default Selection: Bandwidth usage, ordered High to Low. Click on a bar to view more details about an application.
Application Performance	This graph summarizes QoE, loss, latency, and jitter for individual applications that fall under Microsoft O365 or Cisco Webex family of applications. Default Selection: QoE, ordered High to Low. Click on a bar to view more details about an application.
Application Usage	The graph shows how the bandwidth usage of applications varied during the time window. Hover the mouse pointer on the graph to see the bandwidth usage of the applications at a particular time.
WAN Site – Application Usage and Performance	This graph summarizes performance of Microsoft O365 or Cisco Webex family of applications across top five sites. Default Selection: Top WAN sites by bandwidth usage, ordered High to Low. Click on a line to view more details about a site.
Carrier - Application Usage and Performance	This table summarizes performance of Microsoft O365 or Cisco Webex family of applications across various carrier links. Click on the name of a carrier to view more details about it.

Application

Application – Performance and Usage

This page includes graphs and tables capturing performance and usage information of various applications.

Page Element	Description
Application Performance and Usage Graph	The graph shows how a performance measure (bandwidth usage, QoE, loss, latency, or jitter) varied over time. Hover the mouse pointer on the graph to see the performance measure values for the applications at a particular time. Default Selection: Top applications by bandwidth use, ordered High to Low. The graph includes a maximum of five applications. Choose the applications to be featured in the graph from the Application Performance and Usage Table.
Device Locations	The map shows where WAN edge devices carrying the application traffic are deployed.

Application Performance and Usage Table	The table lists applications, application families and classes, and provides counts and performance measures for each application. Default Sort Order: High to Low by bandwidth usage.

Application Family – Performance and Usage

This page provides performance and usage information for application families through graphs and a table of counts and performance measures.

Page Element	Description
Application Family Performance and Usage Graph	The graph shows how a performance measure (bandwidth usage, QoE, loss, latency, or jitter) varied over time. Hover the mouse pointer on the graph to see the performance measure values for the application families at a particular time. Default Selection: Top application families by aggregate bandwidth use, ordered High to Low. The graph includes a maximum of five application families. Choose the application families to be featured in the graph from the Application Family Performance and Usage Table.
Device Locations	The map shows where WAN edge devices carrying the application family traffic are deployed.
Application Family Performance and Usage Table	The table lists application families and provides counts and performance measures for each application family. Default Sort Order: High to Low by aggregate bandwidth usage.

Application Class – Performance and Usage

This page provides performance and usage information for application classes through graphs and a table of counts and performance measures.

Page Element	Description
Application Class Performance and Usage Graph	The graph shows how a performance measure (bandwidth usage, QoE, loss, latency, or jitter) varied over time. Hover the mouse pointer on the graph to see the performance measure values for the application classes at a particular time. Default Selection: Top application classes by aggregate bandwidth use, ordered High to Low. The graph includes a maximum of five application classes. Choose the application classes to be featured in the graph from the Application Class Performance and Usage Table.
Device Locations	The map shows where WAN edge devices carrying the application class traffic are deployed.

Application Class Performance and Usage Table	The table lists application classes and provides counts and performance measures for each application class. Default Sort Order: High to Low by aggregate bandwidth usage.

Network Usage

This page provides network usage information across the following transport abstractions:

- Tunnels
- TLOCs
- Transport Paths
- Transport Colors

Page Element	**Description**
Usage and Performance Graph	The graph shows how an application performance measure (bandwidth usage, QoE, loss, latency, or jitter) varied over time. window for a maximum of five transport entities. Hover the mouse pointer on the graph to see the performance measure values at a particular time. Default Selection: Top entities by aggregate bandwidth use, ordered High to Low. The graph includes a maximum of five transport entities. Choose the entities to be featured in the graph from the Performance Measures Table.
Performance Measures Table	The table lists the transport entities and provides counts and performance measures for each entity. Default Sort Order: High to Low by aggregate bandwidth usage.

Network

Sites

This page provides usage and performance information across various WAN sites. The following information is presented across the different tabs.

Page Element	**Description**

Usage and Performance Graph	The graph shows how an application performance measure (bandwidth usage, QoE, loss, latency, or jitter) varied over time. Hover the mouse pointer on the graph to see the performance measure values at a particular time. Default Selection: Top entities by aggregate bandwidth use, ordered High to Low. The graph includes a maximum of five entities (sites, edge devices, or carriers based on the tab). Choose the entities to be featured in the graph from the Performance Measures Table.
Applications	The graph summarizes bandwidth consumption, QoE, loss, latency, jitter, and device count for a maximum of 10 applications mapped to the selected entities (sites, edge devices, or carriers). Select up to a maximum of five entities (sites, edge devices, or carriers) from the Performance Measures Table.
Performance Measures Table	The table lists entities such as sites, location, applications, edge devices, and tunnels, and provides performance measures for each entity. Default Sort Order: High to Low by aggregate bandwidth usage. **Note** Cisco vAnalytics determines the location of a device by looking up the public IP address of its WAN interface on a commercial database. If a device has WAN circuits from multiple providers, with each circuit having a public IP address from the respective provider's IP pool, you may notice multiple locations for the same device or site.

Devices

This page provides an inventory of edge devices in the Cisco SD-WAN overlay network.

The following key information is listed for each edge device:

- device host name
- device model
- device IP
- device site ID

TLOCs (Circuits)

This page provides performance metrics for the TLOC (circuits) in the overlay network.

This page includes a table that lists all the TLOCs and the various performance measures for the TLOCs. Use a combination of search or filter choices to access performance details of a TLOC of interest.

Transport Path

This page provides performance metrics for the transport paths in the overlay network.

This page includes a table that lists all the transport paths and the various performance measures for the transport paths. Use a combination of search or filter choices to access performance details of a transport path of interest.

Transport Color

This page provides performance metrics for the transport colors in the overlay network.

This page includes a table that lists all the transport colors and the various performance measures for the transport colors. Use a combination of search or filter choices to access performance details of a transport color of interest.

Tunnels - Performance and Usage

This page provides performance metrics for the tunnels in the overlay network.

This page includes a table that lists all the SD-WAN tunnels and the various performance measures for the tunnels. Use a combination of search or filter choices to access performance details of a tunnel of interest.

Network Availability

This page summarizes network-wide availability of all devices and circuits.

Page Element	Description
Devices (aggregate)	This section shows device uptime as a percentage and total device downtime in minutes across selected time interval (default is 24 hours). Click on the uptime or downtime value to view more detailed statistics. The detailed statistics show device downtime occurrences during the selected time window. Up to 10 devices that have the highest total downtime are featured.
Circuits (aggregate)	This section shows circuit uptime as a percentage and total circuit downtime in minutes across selected time interval (default is 24 hours). Click on the uptime or downtime value to view more detailed statistics. The detailed statistics show circuit downtime occurrences during the selected time window. Up to 10 circuits that have the highest total downtime are featured.
Devices	This graph summarizes the total device downtime in minutes for a maximum of 10 devices, ordered high to low by device downtime. Click on a bar to view device downtime occurrences during a selected time interval.
Circuits	This graph summarizes the total circuit downtime in minutes for a maximum of 10 circuits, ordered high to low by circuit downtime. Click on a bar to view circuit downtime occurrences during a selected time interval.

Flows

Top Talkers

This page provides statistics about the top traffic flow sources (top users tracked by using respective source IP addresses) in the overlay network.

The source data is presented in a table. By default, the sources are sorted High to Low by bandwidth usage.

Office 365

From Cisco IOS XE Release 17.4.1a, you can enable Cloud onRamp for the Microsoft Office 365 family of applications to determine the best path to reach these SaaS applications.

If the best path functionality is enabled on Cisco vManage, the associated log and path analysis pages are displayed on Cisco vAnalytics.

For more information about the Cloud onRamp for SaaS configuration and viewing the metric logs, see the following sections in *Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x*:

- Enable Application Feedback Metrics for Office 365 Traffic
- Enable Microsoft to Provide Traffic Metrics for Office 365 Traffic
- View Office 365 Application Logs