

Cisco Catalyst SD-WAN Analytics

First Published: 2019-07-19

Last Modified: 2025-12-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

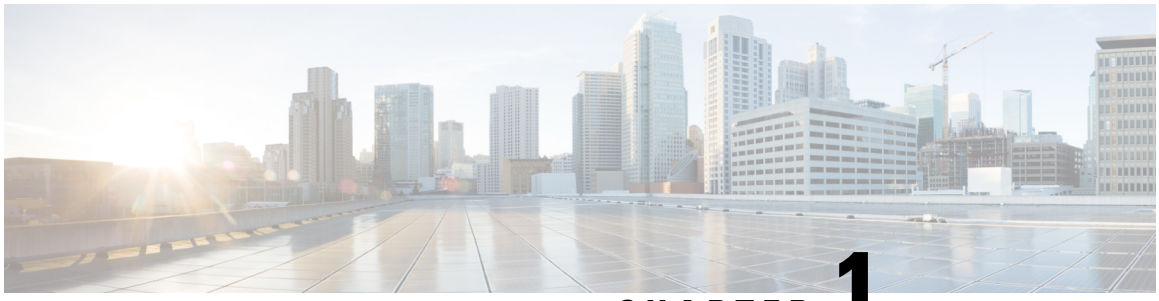
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2025 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Cisco Catalyst SD-WAN Analytics

Table 1: Feature History

Release	What's New
October 2025	The Optimization tab displays the APPQoE dashboard that provides insights into the performance and enablement of the AppQoE features. For more information. see Optimization, on page 45. The **App Flow** feature in the Application 360 page offers insights into application behavior, SLA violations, and network anomalies, enabling users to detect underlying patterns and identify root causes. For more information, see the **App Flow Heat Map** section in Application Dashboard, on page 26. The **Logs** tab is a network flow monitoring tool that provides visibility into traffic logs across all devices. It enables network administrators to search for specific flows, identify traffic patterns, diagnose network issues, and ensure security compliance. For more information, see Traffic Logs, on page 42. Anomaly Detection in usage patterns identifies deviations in cellular link usage across the entire network, providing supporting evidence to determine root causes. This capability enables network operators to verify that traffic flows align with defined policies and to optimize operational costs. For more information, see Anomaly Detection, on page 41.

Release	What's New
December 2024	Anomaly Detection identifies significant deviations in network KPIs like loss, latency, and jitter, helping determine whether issues are persistent or isolated. This enables proactive identification and resolution of potential network problems. By providing detailed insights into affected sites and tunnels, Anomaly Detection facilitates necessary adjustments to optimize networks, enhancing user experience and reducing downtime. For more information, see Anomaly Detection, on page 41.
June 2024	The Threat Intelligence page, powered by Cisco Talos, offers insights into untrusted IP addresses that have been accessed in Cisco Catalyst SD-WAN. For threats detected in Cisco Catalyst SD-WAN involving clients accessing untrusted IP addresses, administrators can enforce security policies to block communication with those IP addresses. For more information, see Threat Intelligence, on page 40.

Release	What's New
August 2023	• Circuits Dashboard: The **Circuits** dashboard provides information on the performance, utilization, and availability of various circuits. It offers a comprehensive view of the performance of multiple circuits across the Cisco Catalyst SD-WAN fabric for all locations, and detailed insights for each individual site. For more information, see Circuits Dashboard, on page 33. • Predictive Path Recommendations: Closed Loop Automation: This feature automates the process of applying policy changes in Cisco SD-WAN Manager by leveraging the Predictive Path Recommendations (PPR) feature available in Cisco SD-WAN Analytics. After the policy changes have been implemented, you can then view the applied changes in Cisco SD-WAN Analytics. For more information, see Predictive Path Recommendations - Closed Loop Automation, on page 39. • Enhancement to Sankey chart: Sankey chart represents any unknown QOE paths as gray paths. For more information, see the section about **Sankey Charts**. • Unknown Availability and Unknown Applications: Unknown sites and circuits: A classification in the Overview dashboard when the availability data for certain sites and circuits cannot be obtained. Unknown applications: Refers to those applications for which the Quality of Experience (QoE) score is not available. • Bandwidth Forecasting: The bandwidth forecasting feature helps you with predicting future network bandwidth needs based on current and historical bandwidth usage data. For more information, see Bandwidth Forecasting, on page 40.
July 2023 (Cisco Catalyst SD-WAN Manager Release 20.9.4 and Cisco Catalyst SD-WAN Manager Release 20.12.1)	Easy Onboarding of Cisco SD-WAN Analytics into Cisco SD-WAN Manager.

Release	What's New
March 2023	Enhancements to Path Recommendations powered by ThousandEyes WAN Insights. For more information, see Predictive Networks, on page 35.
December 2022	• A **Path Analytics** tab on the **Application 360** page is available to display path-telemetry data for Webex. The path-telemetry data includes best path scores across time, the Cisco Catalyst SD-WAN scores computed for each path, the feedback received by Webex for the paths, and latency data. The path-telemetry data for the M365 family of applications (under the **Path Analytics** tab in the **Application 360** page) is currently available with Cisco SD-WAN Analytics Analytics deployments in the Americas (West and East), Europe, and APAC regions. • Access Cisco SD-WAN Analytics from the Cisco SD-WAN Manager menu (Cisco vManage Release 20.9.2 or later). • A Sankey chart to display detailed information about an application flow across various tunnels for a single site. For more information, see the section about Sankey Charts. • View application flows over various network paths for both tunnel and DIA (for Cloud OnRamp for SaaS-enabled applications). For more information about circuit paths, see **App Metrics** in the **Application 360** section. • View underlay path information and hop metrics such as loss and latency. To view underlay path information in Cisco SD-WAN Analytics, you must enable the underlay measurement and tracing services (UMTS) feature in Cisco SD-WAN Manager (Cisco vManage Release 20.10.1 or later). For more information about viewing underlay paths, see **App Flow** in the **Application 360** section.

Release	What's New
August 2022	• Path Recommendations that are powered by ThousandEyes WAN Insights offers proactive insights into the quality of the current network paths that your applications are taking, and the quality of alternate recommended paths. The Path Recommendations feature helps you make informed decisions so that you can modify your Cisco Catalyst SD-WAN policies for a better application experience. • A new **Path Analytics** tab in the **Application 360** page is available to display path-telemetry data for Microsoft 365 (M365) family of applications. The path-telemetry data includes best path scores across time, the Cisco Catalyst SD-WAN scores computed for each of the paths, the feedback received by Microsoft for the paths, and latency data. • Ability to also generate periodic reports in a CSV format for offline review in addition to the PDF format. • Option to deactivate and reactivate data processing for an overlay.

Release	What's New
April 2022	• Refreshed highly intuitive graphical interface. • New status bar showcasing the overall health of sites, applications and circuits, and its change from the past time period. • New summary widgets for applications, sites, and circuits and top clients on the main dashboard to quickly draw attention to problem areas. • New applications summary and sites summary dashboards that allow you to drill down to individual application and site screens to gain more insights of problem areas. • Visibility into top applications trends that have significant rise and drop in their measured QoE score, usage, loss, latency. • An aggregated view into the count and health of applications that are grouped by their application class. • Usage statistics covering both tunnel and DIA traffic (for Cloud OnRamp enabled applications). • Ability to generate periodic reports in a PDF format for offline review. • Expansion in duration of analytics display for up to 12 weeks with option to select custom date range of a maximum of one week.

- Overview of Cisco SD-WAN Analytics, on page 9
- Prerequisites for Cisco SD-WAN Analytics , on page 9
- Restrictions for Cisco SD-WAN Analytics , on page 10
- Onboard Cisco SD-WAN Analytics, on page 10
- Access Cisco SD-WAN Analytics, on page 17
- Authentication and Authorization, on page 17
- Screen Elements, on page 23
- Overview Dashboard, on page 24
- Site Dashboard, on page 26
- Application Dashboard, on page 26
- Circuits Dashboard, on page 33
- Predictive Networks, on page 35
- Threat Intelligence, on page 40
- Anomaly Detection, on page 41
- Traffic Logs, on page 42
- Optimization, on page 45

• Reports, on page 47
• Troubleshooting, on page 48
• Appendix, on page 50

Overview of Cisco SD-WAN Analytics

Cisco SD-WAN Analytics is a cloud-based analytics service for Cisco Catalyst SD-WAN offering comprehensive insights into application and network performance. The analytics service is available with Cisco DNA Advantage and Cisco DNA Premier software subscriptions. Cisco SD-WAN Analytics collects and stores metadata about traffic flows in its cloud storage and produces analytics based on this collected data.

Some of the key benefits of Cisco SD-WAN Analytics service are:

- Network Visibility: Gain visibility into key network performance metrics, such as loss, latency, jitter, and availability.
- Application Experience: Assess Quality of Experience (QoE) for applications deployed in data centres and on cloud.
- Operational Insights: Establish historical benchmarks, identify trends, and correlate application experience with the underlying network behavior.
- Path Recommendations: Gain insights into the quality of the current network paths your applications are taking, and the quality of the alternate recommended paths for better application experience.
- Faster Resolution: Lower the mean time to identification (MTTI) of issues with faster root cause isolation.
- Application Flows: Gain insights into application traffic flows over various network paths.
- Top Talkers: Identify top consumers of network bandwidth.
- Reporting: Generate analysis reports for offline review by CIO/CTO/COO and network teams.

Prerequisites for Cisco SD-WAN Analytics

- Synchronize your license information. From the Cisco Catalyst SD-WAN Manager menu, choose **Administration** > **License Management**. Click **Sync Licenses & Refresh Devices**. For more information, see Synchronize Licenses.

Note If your license or subscription to Cisco DNA software is not valid, Cisco Catalyst SD-WAN Manager displays a license alarm. Therefore, synchronize your license information in Cisco Catalyst SD-WAN Manager if you have a Cisco DNA Advantage subscription.

To purchase a license, or for more information about licensing, see Licensing on Cisco Catalyst SD-WAN.

You can continue to use Cisco SD-WAN Analytics with a valid DNA software subscription.

- Configure the following options in Cisco SD-WAN Manager to use Cisco SD-WAN Analytics:
  - Configure app-visibility. See Configure global application visibility.
  - Configure the network time protocol (NTP) servers. NTP must be configured to synchronize time on all the control components and devices in the Cisco Catalyst SD-WAN fabric. See Configure NTP using Cisco SD-WAN Manager .

Restrictions for Cisco SD-WAN Analytics

- Cisco SD-WAN Analytics shows usage statistics for custom applications flowing through the exit path of the Direct Internet Access (DIA). To monitor the Quality of Experience (QoE) for these applications, enable Cloud OnRamp for SaaS for the custom applications.
- Cisco SD-WAN Analytics accounts for only the egress traffic. Therefore, you may notice variations between application usage statistics reported by Cisco SD-WAN Manager and the statistics reported by Cisco SD-WAN Analytics.
- Cisco SD-WAN Analytics provides insights only on sites and circuits that were actively used by application traffic on the overlay. Insights are not available for unused sites and circuits.
- Cisco SD-WAN Analytics provides insights only for traffic passing through the Cisco Catalyst SD-WAN tunnels or taking a DIA path (with CoR SaaS Enabled). Non Cisco Catalyst SD-WAN tunnels (SIG Tunnels) are not supported in Cisco SD-WAN Analytics.
- The Circuits dashboard does not display the transmission (Tx) or reception (Rx) bitrate statistics for subinterfaces on Cisco IOS XE Catalyst SD-WAN devices.

Onboard Cisco SD-WAN Analytics

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1,Cisco SD-WAN Analytics can be onboarded into Cisco SD-WAN Manager with easy and automated onboarding capabilities for different Cisco SD-WAN Manager deployment types. The following table shows the different deployment types for Cisco SD-WAN Manager and the method of onboarding Cisco SD-WAN Analytics into Cisco SD-WAN Manager.

Table 2: Onboard Cisco SD-WAN Analytics

Deployment Type	Cisco Catalyst SD-WAN Manager Version	Description
Cloud-delivered Cisco Catalyst SD-WAN	Versions of Cisco Catalyst SD-WAN Manager are not applicable. Cisco SD-WAN Analytics is automatically onboarded.	While provisioning a new Cisco Catalyst SD-WAN fabric, Cisco SD-WAN Analytics is automatically onboarded into Cisco SD-WAN Manager. For more information, see Cloud-delivered Cisco Catalyst SD-WAN, see Onboard Cisco SD-WAN Analytics for a Cloud-Delivered Cisco SD-WAN Manager Deployment, on page 13
Cloud-Hosted Cisco SD-WAN Manager	Versions of Cisco Catalyst SD-WAN Manager are not applicable. Cisco SD-WAN Analytics is automatically onboarded.	**Onboard New Cisco SD-WAN Analytics** - Cisco SD-WAN Analytics is automatically onboarded into Cisco SD-WAN Manager when you accept the Cisco End User License agreement. For more information, see Onboard New Cisco SD-WAN Analytics, on page 13 **Onboard Existing Cisco SD-WAN Analytics** - Onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager. For more information, see Onboard Existing Cisco SD-WAN Analytics, on page 14.

Deployment Type	Cisco Catalyst SD-WAN Manager Version	Description
On-Premise or Customer-hosted Cloud Cisco SD-WAN Manager	Cisco vManage Release 20.3.x, Cisco vManage Release 20.4.x, Cisco vManage Release 20.5.x, Cisco vManage Release 20.6.x, Cisco vManage Release 20.7.x, Cisco vManage Release 20.8.x, Cisco vManage Release 20.9.1, Cisco vManage Release 20.9.2, Cisco vManage Release 20.9.3, Cisco vManage Release 20.10.x, Cisco vManage Release 20.11.x	Onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager. For more information, see, Onboard Cisco SD-WAN Analytics for an On-Premise or a Customer-Hosted Cloud Cisco SD-WAN Manager Deployment for Older Releases, on page 16
	Cisco vManage Release 20.9.4 and Cisco Catalyst SD-WAN Manager Release 20.12.1	Onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager For more information, see Onboard Cisco SD-WAN Analytics for an On-Premise or a Customer-Hosted Cloud Cisco SD-WAN Manager Deployment, on page 14.

Cisco SD-WAN Analytics collects metadata about traffic flows, events, activity, and inventory in the Cisco Catalyst SD-WAN overlay network to provide analytics about traffic flows, network conditions, and application experience. The metadata is exported at periodic intervals from Cisco SD-WAN Manager to Cisco SD-WAN Analytics using APIs over a secure, FIPS-compliant HTTPS channel that uses TLS 1.3. This feature is available for Cisco vManage Release 20.3.1 and later releases.



Note From Cisco Catalyst SD-WAN Manager Release 20.16.1, Cisco SD-WAN Manager deletes statistics files older than 14 days, if the speed at which data is received is faster than the system's ability to process. This prevents disk fill-up.

See the Cisco privacy data sheet to know more about how Cisco Catalyst SD-WAN Cloud handles data.

Before Cisco vManage Release 20.3.1, the APIs that were used to export metadata used nonstandard authentication. The support for APIs with standard authentication was introduced in Cisco vManage Release 20.3.1 and is available in all later versions. Cisco is committed to responsible use of technology and ensures product security and integrity. Cisco disables Cisco SD-WAN Analytics if your Cisco SD-WAN Manager release version is earlier than Cisco vManage Release 20.3.1Cisco vManage Release 20.3.1 or later releases.

The following are some groups of metadata that is exported from Cisco SD-WAN Manager to Cisco SD-WAN Analytics:

- Device configurations
- Device statistics
- Interface statistics
- Alarm statistics
- Audit logs

- Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow statistics

Note In Cisco vManage Release 20.7.1 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

After you have onboarded Cisco SD-WAN Analytics to Cisco SD-WAN Manager, enable data collection in your Cisco SD-WAN Manager configuration as described in the respective section below:

- Enable Data Collection (Cisco vManage Release 20.3 or Later), on page 50
- Enable Data Collection (Cisco vManage Release 20.1 or Earlier), on page 50
- Additional Steps to Enable Data Collection on an On-Premises Cisco SD-WAN Manager Instance, on page 51

Onboard Cisco SD-WAN Analytics for a Cloud-Delivered Cisco SD-WAN Manager Deployment

With the Cloud-delivered Cisco Catalyst SD-WAN deployment, Cisco SD-WAN Analytics is automatically onboarded into Cisco SD-WAN Manager when a new Cisco Catalyst SD-WAN fabric is provisioned. For more information about the Cisco Catalyst SD-WAN fabric provisioning process, see Create a Fabric in the Cisco Catalyst SD-WAN Portal.

Onboard Cisco SD-WAN Analytics for a Cloud-Hosted Cisco SD-WAN Manager Deployment

Onboard New Cisco SD-WAN Analytics

Cisco SD-WAN Analytics is automatically onboarded to Cisco SD-WAN Manager when you accept the Cisco end user license agreement when you create a Cisco Catalyst SD-WAN overlay network through the Cisco Catalyst SD-WAN Self-Service Portal. For more information about creating a Cisco Catalyst SD-WAN cloud-hosted overlay network, see Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric.

Note Accept the Cisco end user license agreement to onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager. If you do not accept the Cisco end user license agreement, Cisco SD-WAN Analytics is not onboarded. Cisco SD-WAN Analytics can be onboarded into Cisco SD-WAN Manager later by following the steps that are described in Existing Deployment.

Onboard Existing Cisco SD-WAN Analytics

Perform the following steps to onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager for an existing a Cloud-hosted Cisco SD-WAN Manager deployment:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud Services**.
3. In the **Cloud Services** field, click **Enabled** next to **Analytics**.

   To disable this feature, change its status to Disabled (or toggle the switch off).

Note If you are on Cisco SD-WAN Manager version release greater than 20.9.4 or Cisco Catalyst SD-WAN Manager Release 20.12.1, you must accept the end user license agreement when enabling Cisco SD-WAN Analytics. For Cisco SD-WAN Manager versions before 20.9.4 or Cisco Catalyst SD-WAN Manager Release 20.12.1, the end user license agreement is not explicitly displayed, and it is an implicit acceptance of the user license agreement.

4. Click **Save**.

Onboard Cisco SD-WAN Analytics for an On-Premise or a Customer-Hosted Cloud Cisco SD-WAN Manager Deployment

Minimum supported releases:

- Cisco SD-WAN Manager release 20.12.1 and later releases
- Cisco SD-WAN Manager release 20.9.4 and later releases of 20.9.4

Perform the following steps to onboard Cisco SD-WAN Analytics to Cisco SD-WAN Manager release 20.9.4, 20.12 and later:

Single Tenant

1. Log in to Cisco SD-WAN Manager.

   The **Credentials for Cisco Smart Account** dialog box for onboarding Cisco SD-WAN Analytics.
2. Enter your smart account or virtual account credentials in the **Credentials for Cisco Smart Account** dialog box.

Note This account is the Cisco account credentials that are associated with the smart account or virtual account to which your provider organization controller profile belongs to.

3. Click the **End User License Agreement** check box to accept the license agreement.
4. Click **Save**.

   Cisco SD-WAN Analytics is onboarded when the first communication is established in the back end.

Note If you click the **Do not show this again** check box, and then click **Remind Me Later**, Cisco SD-WAN Analytics will not be onboarded to Cisco SD-WAN Manager.

To onboard Cisco SD-WAN Analytics to Cisco SD-WAN Manager, perform these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud Services**.
3. In the **Cloud Services** field, click **Enabled**. By default, Cisco SD-WAN Analytics is enabled.

   To disable Cisco SD-WAN Analytics, change its status to Disabled (or toggle the switch off) .
4. Enter your smart account credentials.
5. Click **Save**.

Multi-Tenant

1. Log in to Cisco SD-WAN Manager as a managed service provider.
2. Enter your smart account or virtual account credentials in the **Credentials for Cisco Smart Account** dialog box.

Note This account is the Cisco account credentials that are associated with the smart account or virtual account to which your provider organization controller profile belongs to.

3. Click the **End User License Agreement** check box to accept the license agreement.
4. Click **Save**.

   At this point, cloud services is enabled for the tenants by the Provider.
5. Log in to Cisco SD-WAN Manager as a tenant admin.
6. Click the **End User License Agreement** check box to accept the license agreement.

   Cisco SD-WAN Analytics is onboarded when the first communication is established in the back end.

Note If you click the **Do not show this again** check box, and then click **Remind Me Later**, Cisco SD-WAN Analytics will not be onboarded to Cisco SD-WAN Manager.

To onboard Cisco SD-WAN Analytics to Cisco SD-WAN Manager, perform these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud Services**.
3. If you are the Provider, execute the following steps:

a. In the **Cloud Services** field, click **Enabled**.

b. Enter your smart account credentials.

If you are a tenant administrator:

In the **Cloud Services** field, click **Enabled** next to **Analytics**.

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



Note In a single tenant environment, enabling cloud services automatically enables Cisco SD-WAN Analytics. However, in a multitenant environment, the provider enables cloud services after which tenants can log and enable Cisco SD-WAN Analytics.

4. Click **Save**.

Onboard Cisco SD-WAN Analytics for an On-Premise or a Customer-Hosted Cloud Cisco SD-WAN Manager Deployment for Older Releases

If you are on a Cisco vManage release earlier than 20.9.4 or 20.12 (20.3.x, 20.4.x, 20.5.x, 20.6.x,20.7.x, 20.8.x, 20.9.3.x, 20.10.x, 20.11.x), perform the following steps to onboard Cisco SD-WAN Analytics to Cisco SD-WAN Manager:



Note In a multitenant Cisco Catalyst SD-WAN environment, a smart account user or virtual account user with access to the provider organization's controller profile must run this workflow. Therefore, this workflow must be executed by the provider, and not by a tenant.

In a single tenant Cisco Catalyst SD-WAN environment, a smart account user or a virtual account user who has access to the controller profile of the organization can execute this workflow.

1. From the Cisco SD-WAN Self-Service Portal menu, choose **Create Overlay**.
2. From the **Select Smart Account** drop-down list, choose the name of the smart account from which you want to associate the overlay network.

   You can search smart accounts by account name or by domain ID.
3. From the **Overlay** drop-down list, choose the name of the virtual account for which you want to associate the overlay network.
4. Choose the deployment model as **Non-Cisco Hosted**, and proceed with the Non-Cisco Hosted deployment model workflow.
5. Review your non-Cisco Hosted overlay fabric in the workflow.
6. Copy the OTP (token) next to **vAnalytics/Cloud Connector Token**. To copy the OTP, click **...**, and choose **Copy to Clipboard**.
7. Log in to Cisco SD-WAN Manager.

8. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
9. Click **Edit**, next to **Cloud Services**.
10. Paste the OTP that you copied in the OTP field.
11. Click **Save**.

    Cisco SD-WAN Analytics is onboarded to Cisco SD-WAN Manager when the first communication is established in the back-end.

Access Cisco SD-WAN Analytics

Starting from Cisco vManage Release 20.9.2, use the Cisco SD-WAN Manager menu to access Cisco SD-WAN Analytics.

From the Cisco SD-WAN Manager menu, choose **Analytics**. Cisco SD-WAN Analytics has the following options to view Cisco SD-WAN Analytics:

- Overview: View an overall network summary for sites and applications.
- Sites: View into the site availability and usage across the entire network.
- Applications: View of how different applications are performing across an overlay for all sites, and for a single site.

You can also access Cisco SD-WAN Analytics using one of the following URLs based on the location of your Cisco SD-WAN Analytics:

- Americas (West): 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:

- Overview Dashboard: The Overview Dashboard is displayed when you log in to Cisco SD-WAN Analytics. You can view an overall network summary for sites and applications.
- Application Dashboard: View of how different applications are performing across an overlay for all sites, and for a single site.
- Site Dashboard: View into the site availability and usage across the entire network.
- Reports: A menu option to schedule executive summary and detailed reports periodically.

Authentication and Authorization

Cisco SD-WAN Analytics users can be authenticated using one of the following methods or 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 SAML 2.0 or OIDC protocol to interoperate with Cisco SD-WAN Analytics

- Existing Okta ID: The Cisco-assigned Okta ID

Note Support for login using Cisco-assigned Okta ID has been deprecated, and in some cases it may still be in use. Cisco recommends such users to transition to using either your CCO ID or your organization's Id at the earliest.

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 SD-WAN Analytics 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 SD-WAN Analytics screens for the overlay. In addition, the user can configure the IdP to be used for user authentication for the overlay.
- Virtual Account User and Virtual Account Viewer: The user can access all Cisco SD-WAN Analytics screens for the overlay associated with that particular Virtual Account.

Alternatively, you can add a user to a Smart Account. Doing so allows the user to access Cisco SD-WAN Analytics for all Virtual Accounts 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 SD-WAN Analytics screens for all the overlays. In addition, the user can view the reports tab and generate reports for anlysis. This user can also 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 SD-WAN Analytics screens for the overlay.

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 default role assigned to them while defining organization IdP on Cisco SD-WAN Analytics. Alternatively, user role can be updated by using the `authzCiscovAnalytics` attribute on the organization IdP.

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 `*`.

The Cisco Smart Account or Virtual Account administrator must first login to Cisco SD-WAN Analytics service using the Cisco CCO ID. After login, the administrator can view a list of Smart Accounts or Virtual Accounts that they have access to. The administrator will then be able to define organization IDP against Cisco SD-WAN Analytics for subsequent access through organization ID by users.

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

For an overlay, if Cisco SD-WAN Analytics has been onboarded, the entry under **vAnalytics Status** reads **Active**; if Cisco SD-WAN Analytics is not onboarded, the entry reads **New**. If Cisco SD-WAN Analytics 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 overlay reads **New**, but you are aware that Cisco SD-WAN Analytics has been onboarded, verify whether you have logged in using the correct Cisco SD-WAN Analytics URL. See Access Cisco SD-WAN Analytics, on page 17 to use one of the URLs based on the location of your Cisco SD-WAN Analytics.

To pause data processing for an overlay, click **…** adjacent to the overlay name and choose **Deactivate**. When data processing is paused, the **vAnalytics Status** reads **InActive (Paused)**. To resume data processing, choose **Activate**.

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 SD-WAN Analytics 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 SD-WAN Analytics 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 SD-WAN Analytics users for the overlay.

1. Log in to Cisco SD-WAN Analytics.

Note If this is your first login to Cisco SD-WAN Analytics for your overlay, log in with the Cisco CCO ID. The organization IdP you define for the overlay authenticates and authorizes users in subsequent log-in 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:
   a. To configure your organization's IdP for a Smart Account, click **Define IDP**.
   b. To configure your organization's IdP for a virtual account, hover the mouse pointer over **...** under **Actions**. Then, click **Define IDP**.
4. In the **Define IDP** dialog box, click **OIDC IDP** or **SAML IDP**.
   a. For an SAML 2.0 IdP, do the following:

Table 3: SAML IdP Properties

IDP Metadata	Click browse file and upload the SAML 2.0 metadata file to Cisco SD-WAN Analytics. Cisco SD-WAN Analytics 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 SD-WAN Analytics 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. A user can be assigned the following roles: • The `basic` role allows a user to access all the Cisco SD-WAN Analytics 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 SD-WAN Analytics screens for the overlay. • The `admin` role allows a user to access all the Cisco SD-WAN Analytics screens for the overlay. In addition, the user can also define an IdP for the overlay.
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 4: 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 SD-WAN Analytics 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. A user can be assigned the following roles: • The `basic` role allows a user to access all the Cisco SD-WAN Analytics 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 SD-WAN Analytics screens for the overlay. • The `admin` role allows a user to access all the Cisco SD-WAN Analytics screens for the overlay. In addition, the user can also define an IdP for the overlay.
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:

   The required claims are firstName, lastName, and email.

   An optional claim attribute `authzCiscovAnalytics` is also available. For more details, see the section **Authorization with Organization ID**.

Any users logging in to Cisco SD-WAN Analytics 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 SD-WAN Analytics 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 SD-WAN Analytics users for the overlay.

1. Log in to Cisco SD-WAN Analytics.
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 SD-WAN Analytics 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.

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, one month or custom range. While selecting a custom date range, a maximum of one week may be selected at a time.

Filter Options: Use the filter options to narrow your view of analytics to a more granular level. For example, while viewing application-level analytics, you can apply filters to view the analytics for a particular application at a specific site.

Sort Order: Use the sort option to 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 25 rows. You may choose to display 10, 50 or 100 rows and then the pagination option to see more entries 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.

Cisco SD-WAN Analytics supports Google Chrome and Mozilla Firefox.

Overview Dashboard

The **Overview Dashboard** is the first page that you see when you log in to Cisco SD-WAN Analytics. The **Overview Dashboard** page displays header data for sites, applications, and circuits at an overlay level. The widgets in the **Overview Dashboard** provide a top-level view of the performance of the sites, applications, circuits, and users.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, if Cisco SD-WAN Analytics fails to load on a converged dashboard, the system will automatically fall back to the default Cisco SD-WAN Manager dashboard. For more information about converged dashboard, see Converged Dashboard for SD-WAN Analytics and SD-WAN Manager.

The **Overview Dashboard** page presents an overall network summary of a selected overlay site and applications for analysis. For the selected overlay, all the sites to which the user has access are displayed.

Table 5: Overview Dashboard

Page Element	Description
View All Overlays	Click to go to the Smart Accounts screen.
All Sites	Click the drop down list to choose a site or search for a site.
Sites	Displays the percentage of sites having high availability for the selected time range, and the percentage of change compared to the previous time range of the same duration.

Page Element	Description
Applications	Displays the percentage of applications having good QoE for the selected time range, and the percentage of change compared to the previous time range of the same duration. **Note** When you choose a single site on the Overview dashboard, the circuit count displayed in the Application widget might be incorrect. This can happen because of network changes, problems like outages, or delays in the network.
Circuits	Displays the percentage of circuits having high availability for the selected time range, and the percentage of change compared to the previous time range of the same duration.

Sites

The **Sites** summary widget includes the total count of sites and their distribution based on percentage availability (a site's uptime). When the availability information for certain sites cannot be obtained, these sites are categorized as **unknown**. When sites are administratively down, the availability data cannot be generated for them.

The widget also displays the bottom five sites that are sorted by their availability and percentage-change in terms of availability compared to the previous time period of the same duration.

Applications

The **Applications** summary widget includes the total count of applications and their distribution based on QoE score of good, fair, and poor. Applications for which the health score is unavailable, or whose Quality of Experience (QoE) score is unknown, such applications are classified as **unknown**. Similarly, applications where all the traffic flows through DIA paths, which do not have a QoE score, are also classified as unknown applications.

The widget also displays the bottom five applications that are sorted by the worst QoE score and the change in QoE values for these five applications, and site wise distribution indicating the application health for these five applications in terms of QoE score depicted by a bar chart.

Click an application for more information about the sites. The **Application 360** page displays where you can get a site level view of the application, the top sites using the application, its QoE, and usage information.

Circuits

The **Circuits** summary widget includes the total count of circuits and their distribution based on percentage availability. When the availability information for certain circuits cannot be obtained, these circuits are categorized as **unknown**. When circuits are administratively down, availability data cannot be generated for them.

The widget also displays the bottom five circuits that are sorted by their availability and percentage-change in terms of availability compared to the previous time period of the same duration.

When you click the **View Bandwidth Forecast** link, you can view a Bandwidth Forecasting chart that can be used to predict network bandwidth requirements based on current and historic bandwidth usage. For more information, see Bandwidth Forecasting, on page 40.

Clients

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

From the **Overview Dashboard** page, when you filter by sites, you can get an overview for the selected site. You can retrieve useful information about a site as to how many applications are running on this site, the number of devices on the site, the total data usage in the site, the circuits in the site, and the top clients of the site.

The **Devices** widget displays the list of devices on the site and other relevant information.

From the **Overview Dashboard** page, click **Applications** to navigate to the **Application Dashboard** page or click **Sites** to navigate to the **Site Dashboard** page.

Site Dashboard

From the **Overview Dashboard** page, click **Sites** to navigate to the Site Dashboard. The Site Dashboard provides a map view of all the sites. Alternatively, you can click the Cisco SD-WAN Analytics menu, and choose **Sites** to access the **Site Dashboard** page.

The **Site Dashboard** page provides visibility into site availability and usage across the entire network for the selected time period. The **Site Dashboard** page helps you to view the performance of applications on the overlay from a site perspective. It provides the ability to view overlay performance in terms of sites and provides insights into how different sites are performing in terms of availability, utilization and by latency and comparing them to corresponding metrics from the previous time period.

You can hover over a specific site to view the site-related information, or you can use the table view where you can view the list of all the sites with summary information. Click a site to drill down and view the performance metrics for a site.

Application Dashboard

From the **Overview Dashboard** page, click **Applications** to navigate to the Application Dashboard. Alternatively, you can click **View Details** or **Applications** in the Applications widget.

The **Application Dashboard** page displays information on how different applications are performing across an overlay for all sites, and also for a single site.

The **Application Dashboard** gives an overview of Application performance (QoE) for all applications across an overlay and across all sites, and compares it to other metrics such as overall bandwidth and bandwidth increase.

The **Application Dashboard** represents the performance metrics in these widgets:

- Application Experience

- Application Trend Analysis
- QoE Distribution by Application Classes
- Trending Applications

You can also view the metrics in a tabular format. With the tabular format, you can search and view the metrics for any application.

Application Experience

The Application Experience widget displays utilization details, the number of applications that were good, fair, poor, and unknown by counts, and the total volume of traffic. An accordion chart shows the top applications by usage with the color indicating the application health in terms of QoE score. This helps draw attention to the most critical application performance issues. Applications with an unknown QoE score are represented in gray.

To view more information about an application, hover the mouse pointer over a specific application.

Application Trend Analysis

Click **Application Trend Analysis** in the Application Experience widget to launch the Application Trend Analysis widget to view trends of applications for a selected time period in the form of charts.

With the Application Trend Analysis widget you can visualize trends of applications from the following perspectives:

- Plot of numbers of Good/Fair/Poor applications by QoE over a selected time-interval.
- QoE trend-line of top five applications (by bandwidth) over a selected time-interval.
- Ability to specify a custom list from the table of applications, where you can select or deselect applications to view information.

Click a trend-line to view more details about a selected application. You can view the top applications by bandwidth usage, ordered High to Low. Hover the mouse pointer on the graph to see the performance measure values for the applications at a particular time.

Click an individual application block in the accordion chart to navigate to the Application 360 page to view more detailed information about the application you selected.

Application 360

Click an application in the Application Experience widget to navigate to the **Application 360** page. Alternatively, you can click an application in the Trending Application widget, or on an application in the page elements that are listed in the table below, or on any application in the Application widget in the Overview Summary Dashboard to retrieve the Application 360 page.

The **Application 360** page gives you a view of a single application performance across all sites with the capability to further drill down to in-depth details about an application at a single site and tunnel.

From the **Application 360** page, you can visualize how the QoE for a specific application has changed over a selected time period. You can use the **Application 360** page to do the following:

- Compare an application's performance across each site, showing aggregated counts of Good/Fair/Poor sites on a map view.

- View the network path taken by an application across time for a single site.
- View metrics of applications across an overlay corresponding to various network Key Performance Indicators (KPI), with the ability to select specific sites to view loss, latency, jitter, users, and usage per site.

Note The **Application 360** page for a single site does not present statistics for applications flowing through a Direct Internet Access (DIA) exit for Cisco vEdge devices.

Table 6: Application 360

Page Element	Description
Sites	Hover the mouse pointer over a specific site for information on usage and QoE score. You can switch from a map view to a table view to view additional information about the application across all sites.
App Metrics	This tab displays information about an application's network usage—The network loss, latency, and jitter, and the count of users using the application for a single site. Also, this tab displays the circuit that is used by an application, and the usage details about a circuit at different points in time for a single site.

Page Element	Description
App Flow	The **App Flow** tab offers insights into application behavior, SLA violations, and network anomalies, enabling users to detect underlying patterns and identify root causes. For more information, see the **App Flow Heat Map** section. **Sankey Chart:** A Sankey chart provides detailed information about an application flow across various tunnels for a single site. For more information, see the **Sankey Chart** section. **View Path Trace**: Click this link to view underlay path information and hop metrics such as loss and latency for the following scenarios: • Trace and view the exact paths on demand. • Trace tunnel paths when triggered by events. • View historical data for path tunnel paths. **Note** To trace paths and view underlay path information in Cisco SD-WAN Analytics, enable the underlay measurement and tracing services (UMTS) feature in Cisco SD-WAN Manager, and use a Cisco SD-WAN Manager version Cisco vManage Release 20.10.1 or later. For more information about the UMTS feature, see Underlay Measurement and Tracing Services.
Clients	Displays the client across different sites by usage, QoE, KPI metrics for correlation. **Note** Only those entities that initiate a network session are treated as clients.

App Flow Heat Map

Application flows are represented in the form of a heat map. The heat map helps in recognizing patterns with respect to the quality of experience in the network, specifically identifying flows that violated the SLA, the anomaly rate, or flows where the preferred color was not met. Depending on the option you choose in the App Flow drop-down list (e.g., Anomaly Rate, Flows Violating SLA, Flows with Preferred Color Not Met), the heat map displays the corresponding metrics.

Heat maps display metrics for seven days, highlighting hourly data points. If you click on a particular heat map block for that hour, the App Flow table displays the details of the SLA violation along with the anomaly rate for your selected site. The App Flow table also displays sites paired with your selected site.

Click on a paired site to view the paired site workflow. You will see the tunnels running between site pairs. Examining tunnels between site pairs offers valuable insights, specifically identifying which tunnels experience

the highest latency, jitter, and packet loss. Through this tunnel view, you can observe the underlay hops for traffic and pinpoint where significant degradations occur. This information is vital for optimizing network configurations and enhancing the overall quality of experience for applications.

Sankey Chart

A Sankey chart provides more details about application flows across various Cisco Catalyst SD-WAN tunnels and DIA paths within a single site, and aids in understanding the health of the application over these tunnels, which terminate at the remote sites.

To view a Sankey chart, choose a single site, and then choose an application. Click the **App Flow** tab.

The left side of the chart displays information about the local site and color, followed by the QoE score. The right side displays information about the remote site and its color. The size of each link indicates the cumulative usage volume of the tunnel extending from the local site to the remote site.

By default, the **Site** drop-down list showcases the top five sites with the highest QoE scores. The chart aggregates and displays this site information. Furthermore, you can select and display information for up to six sites from the drop-down list.

The Sankey chart displays information for both Cisco Catalyst SD-WAN tunnels and DIA paths. For the DIA path, the local color represents the interface name, while the remote site is denoted as **SaaS**. A flow without remote color and site information represents a DIA path. The chart also identifies any unknown QoE paths as gray paths.

Click a node to highlight all relevant tunnel paths passing through that node. Hover the mouse pointer over the individual sections to view additional information about the volume of usage traffic. The central link classifies the path's quality, categorizing it as good, fair, poor, or unknown.

Microsoft 365

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1, you can enable Microsoft Informed Network Routing to enable collection of telemetry data for the Microsoft 365 application suite. For information on how to enable collection of telemetry data for Microsoft 365 in Cisco SD-WAN Manager, see Enable Application Feedback Metrics for Office 365 Traffic

The telemetry data for Microsoft 365 applications is displayed on the **Path Analytics** tab on the **Application 360** page.

Path Analytics

The **Path Analytics** tab displays path telemetry data for the Microsoft 365 family of applications if the feature is enabled in Cisco SD-WAN Manager. See Enable Application Feedback Metrics for Office 365 Traffic.

The **Path Analytics** tab displays path telemetry data for Microsoft 365 family of applications. It includes data such as best path scores across time, the Cisco Catalyst SD-WAN scores computed for each path, the feedback received by Microsoft for the paths, and latency data.

To view the telemetry data for Microsoft 365 applications, perform the following steps:

1. From the **Overview Dashboard** page, click **Applications** to navigate to the **Application Dashboard** page.
2. From the **Applications dashboard** page, choose a Microsoft application.
3. Select a site.

   The **Path Analytics** tab displays for the selected site and the Microsoft application.

The **Path Analytics** tab displays only for the Microsoft 365 family of applications if the feature is enabled in Cisco SD-WAN Manager, and the telemetry data is available from Microsoft.

The **Path Analytics** tab displays the following charts:

Table 7: Path Analytics

Page Element	Description
Filter	Use the filter to narrow your view of analytics.
Data Comparison	Displays the data for comparing different devices within the same site, across interfaces, and to the service area that they belong to.
Path chart	Displays the best path that is selected by the device for the application across time.
App Score	Displays the score that is computed by Cisco SD-WAN Analytics on the basis of the feedback from Microsoft. This feedback is used by the edge devices to determine the best path.
MSFT App Score (Received)	Displays the score as received from Microsoft.
Usage	Displays the volume of traffic on the edge devices.
Network Telemetry	Displays the loss and latency of the network for Microsoft applications, as detected by the Cloud onRamp probes.
Microsoft Telemetry	Displays latency of the traffic, as reported by Microsoft.
Network Delay	Displays latency on the server side and the client side of the network.

For more information about the Cloud onRamp for SaaS configuration and viewing the metric logs, see the following sections in the *Cloud OnRamp Configuration Guide*:

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

Webex

The **Path Analytics** tab displays for a Webex application if you have enabled Webex telemetry in Cisco SD-WAN Manager. See Enable Webex Server-Side Metrics.

The **Path Analytics** tab displays path-telemetry data for Webex applications. It includes data such as best path scores across time, and the details about Webex traffic from the edge devices and from the Webex server.

To view the telemetry data for Webex, perform the following steps:

1. From the **Overview Dashboard** page, click **Applications** to navigate to the **Application Dashboard** page.
2. From the **Applications dashboard** page, choose a Webex application.
3. Select a site.

   The **Path Analytics** tab is displays for a selected site.

   The **Path Analytics** tab displays Webex data if the feature is enabled in Cisco SD-WAN Manager.

The **Path Analytics** tab displays the following charts:

Table 8: Path Analytics

Page Element	Description
Filter	Use the filter to narrow your view of analytics.
Data Comparison	Displays the data for comparing different devices within the same site, across interfaces, and to the server region that they belong to.
Path chart	Displays the best path that is selected by the device for the application across time for the selected region.
Network Telemetry	Displays the loss and latency of the network toward a dedicated Webex device.
Usage	Displays the volume of Webex traffic per interface for a region.
Media Type	Displays data from the Webex server for the selected media types. Click a media type to view charts showing loss, latency, and jitter. The **Resolution Height** chart displays the resolution quality of the video per interface and region. The **Frame Rate** chart displays data about the frame rate. The **Media Bit Rate** chart displays the data about bits per second for the selected media type.
Transport Type	Displays data from the Webex server for the selected transport types. Click a transport type to view the charts showing loss, latency, and jitter.

QoE Distribution by Application Classes

The QoE Distribution by Application Classes widget displays the applications against different classes. Application classes are broad categories that are used to group applications based on their behavior and network performance requirements. The plot helps identify systemic network and overlay issues that can cause specific classes of applications to perform poorly in the overlay network. An inconsistent ratio of Poor/Fair/Good/unknown for a specific traffic class could indicate possible policy misconfiguration for that application in the overlay.

Trending Applications

The **Trending Applications** widget lets you compare top applications that have significant rise and drop in their measured QoE score, usage, loss, latency.

Applications

The **Applications** widget displays a table of all applications in an overlay. Applications that have an unknown QoE score are represented with a hyphen.

Circuits Dashboard

From the **Overview Dashboard** page, click **Circuits** to navigate to the Circuits Dashboard. Alternatively, you can click **View Details** in the **Circuits** widget.

The **Circuits Dashboard** page provides valuable insights into the availability, utilization, and network performance of circuits. It offers a comprehensive overview of how different circuits are performing across a fabric for all sites, and for individual sites.

The **Circuits Dashboard** presents the following performance metrics in these widgets:

- Total uptime of circuits
- Traffic routed through Direct Internet Access (DIA) vs Tunnels
- Traffic segmentation by color
- Bandwidth utilization chart
- Circuits distribution in an Cisco Catalyst SD-WAN fabric.

Total Uptime

The **Total Uptime** widget displays the total time the Cisco Catalyst SD-WAN fabric was active.

Circuits Trend Analysis

Click **Trend Analysis** in the **Total Uptime** widget to launch the **Circuits Trend Analysis** page to view the trends of circuits for a selected time period in the form of charts.

The **Circuits Trend Analysis** page displays the availability trend for each circuit. Click a circuit for additional information on the applications that use a specific circuit.

Table 9: Trend by Availability

Page Element	Description
Bandwidth	Displays the time series data for the bandwidth utilization of a specific circuit. Click **View Bandwidth Forecast** to view the bandwidth forecast for a circuit. The bandwidth forecast feature helps you view the generated predictions of bandwidth utilization. For more information, see Bandwidth Forecasting, on page 40.

Page Element	Description
Top 5 Application Usage	Displays the top five applications and their respective usage for a specific circuit.
Top 5 Tunnels Usage	Displays the usage statistics for the the top five tunnels of a specific circuit.
DIA vs Tunnel Usage	Displays a breakdown of the usage between DIA and tunnels for a specific circuit.
Applications	Displays more information about various applications, including details about Quality of Service (QoS), usage, packet loss, latency, and jitter within a circuit.
Tunnels	Displays information about all the tunnels that are associated with a specific circuit.
Flows	Displays information about all user traffic traversing the circuit, including details about each flow. The Flows table provides quick access to recent flow activity. For complete historical flow data, see Traffic Logs, on page 42.

The Circuits table provides a comprehensive display of the circuits within your network, showcasing the bottom 10 circuits ranked by their availability. Click **Custom List** to customize the display of circuits in the page. You can select specific circuits that you want to include or exclude from the displayed information.

DIA Vs Tunnel Usage

The **DIA vs Tunnel Usage** widget provides a breakdown of the usage, specifically highlighting the distribution between DIA and tunnel usage within the circuit.

Click **Trend Analysis** in the **DIA vs Tunnel Usage** widget to view usage trends for DIA and tunnels in the form of charts. This information helps you to know the proportion of traffic that is routed through tunnels versus the traffic that uses DIA.

Color Usage

The **Color Usage** widget provides a visual representation of the distribution of usage per color within a fabric.

Click **Trend Analysis** in the **Color Usage** widget to view the usage trends of circuits based on color. Furthermore, it tracks the usage patterns that are associated with each color within the network fabric using time series data.

Bandwidth Utilization

The Bandwidth Utilization chart showcases the top five circuits based on their hourly bandwidth utilization.

The Bandwidth chart displays the utilization of bandwidth based on received (Rx) and transmitted (Tx) data. By applying the utilization filter, you can narrow down the chart display to showcase the specific bandwidth usage for either Rx or Tx.

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

The Bandwidth chart displays both the absolute bitrate utilization (Rx+Tx) and the percentage utilization of Rx and Tx data. By applying the percentage utilization filter, you can refine the chart to show specific bandwidth usage for either Rx or Tx. To view the percentage utilization, ensure that you have configured the upstream bandwidth (for Tx percentage utilization) and downstream bandwidth (for Rx percentage utilization) settings in the Cisco SD-WAN Manager. For more information, see Monitoring Bandwidth on a Transport Circuit.

Circuits Distribution in an SD-WAN Fabric

The **Circuits** widget presents a comprehensive list of all circuits within a fabric, providing essential metrics such as service provider information, availability, downtime, bandwidth, and details about packet loss, latency, and jitter.

Click a circuit in the **Circuits** widget to navigate to the Circuits 360 page, where you can obtain 360-degree information and detailed insights about the circuit.

On the Circuits 360 page, you can view various components that provide information about the circuit's performance. This includes line charts showcasing metrics such as bandwidth utilization, application usage, tunnel usage, and comparison of DIA versus tunnel usage over time.

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

To view the percentage utilization, ensure that you have configured the upstream bandwidth (for Tx percentage utilization) and downstream bandwidth (for Rx percentage utilization) settings in the Cisco SD-WAN Manager. For more information, see Monitoring Bandwidth on a Transport Circuit.

Table 10: Circuits Distribution

Page Element	Description
Applications	Displays information about various applications, including details about Quality of Service (QoS), usage, packet loss, latency, and jitter within a circuit. Click an application to navigate to the **Application 360** page where you can view more details of the selected application and its performance across all sites with capability to further drill down to in-depth details about an application at a single site and tunnel.
Tunnels	Displays all the tunnels that are associated with a specific circuit.
Flows	Displays all user traffic that traverses the circuit, along with detailed information about each flow.

Predictive Networks

Predictive Path Recommendations

Predictive Path Recommendations (PPR) powered by ThousandEyes WAN Insights aligns with Cisco's vision of predictive networks. The PPR feature analyses historical data on application traffic flows across various

network paths, applies statistical data models to forecast future network issues, and suggests recommendations for using alternate paths to improve application experience for the end users.

Note The PPR feature is generally available in regions where ThousandEyes WAN Insights are available. The PPR feature in Cisco SD-WAN Analytics is referred as WAN Insights in ThousandEyes.

Note For Multi-tenant deployments:

- If you are using the PPR feature, and managing multiple customer organizations or regions with the same Cisco SD-WAN Manager, there may be a few items in the PPR graphical user interface that may work differently than expected.
- Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier versions support only standard application groups. Applications defined using Application Aware Routing (AAR) are not supported in these releases.

Enable Predictive Path Recommendations

To enable the Predictive Path Recommendations feature in Cisco SD-WAN Analytics, an overlay must be onboarded to Cisco SD-WAN Analytics.

To activate the PPR feature in Cisco SD-WAN Analytics, perform the following steps:

1. On the Cisco SD-WAN Analytics dashboard, click **Predictive Networks**.

   For Cisco vManage Release 20.9.2 or later, from the **Cisco vManage** menu, choose **Analytics** > **Predictive Networks**.

2. Click **Activate**.

   This activates the overlay for using the PPR feature. The **Activate** button is available only if a user with administrator privileges for Cisco SD-WAN Analytics. Otherwise, this button is disabled.

Depending upon the size of your overlay network, the activation may take up to 48 hours. An email confirmation is sent from ThousandEyes stating that the Activate action was successfully executed. A second email confirmation is sent when data is fully onboarded and the PPR feature is ready to use. After onboarding is complete, you can access the PPR feature from Cisco SD-WAN Analytics. In addition, you can access the same feature from ThousandEyes. The second email includes instructions for how to access ThousandEyes WAN Insights from ThousandEyes.

Note The basic functionality of the Predictive Path Recommendations feature is embedded with a Cisco DNA Advantage+ license (TE-EMBED-WANI) at no extra charge. With this embedded license, you are entitled to monitor up to six applications or application lists per Cisco SD-WAN fabric.

If the activation fails, an error message is displayed on the page. To resolve the issue, follow the instructions that are provided with the error message. If the issue persists, open a TAC case with Cisco support to resolve the issue.

Ensure that you have the appropriate number of Cisco DNA Advantage+ licenses and TE-EMBED-WANI licenses on your Cisco SD-WAN Analytics virtual account. If not, place the license in the correct virtual account.

Use Predictive Path Recommendations

When the activation of the overlay has been completed successfully, Cisco SD-WAN Analytics analyses the data and displays recommendations in the **Predictive Networks** tab.

To begin using the Predictive Path Recommendations feature:

Alternatively, from the Cisco SD-WAN Manager menu, click **Analytics** and choose **Predictive Networks**. (For Cisco vManage Release 20.9.2 or later)

On the **Overview** dashboard, click **Predictive Networks.**.

Recommendation Summary Widget

The **Recommendations Summary** widget provides a high-level view of path recommendations of application groups that are active across all sites, and information about how many sites have the recommendation state **Ready** or **None**.

An application group is a user-defined bundle of applications with similar traffic characteristics, such as Voice or Google Workspace. Each application group includes multiple applications within it, and user can define the SLA Class which includes quality thresholds for loss, latency, and jitter that apply to all traffic for a given application group. Application Groups can be defined on SD-WAN Manager as Application Lists.

An application group is a user-defined bundle of applications that share similar traffic characteristics, such as Voice or Google Workspace. Each application group includes multiple applications, and users can define an SLA class for it. This SLA class sets quality thresholds for loss, latency, and jitter that apply to all traffic within the given application group. In Cisco SD-WAN Manager, application groups is configured as Application Lists.

Below is a list of the application groups included by default:

- Office365
- Voice
- Salesforce
- Google Workplace
- GoTo Meeting
- Webex

The Quality of Service (QoS) thresholds for each default application category are presented below, with loss expressed as a fraction, and both latency and jitter in milliseconds.

- Office 365: Loss 0.03, Latency 300, Jitter 300
- Voice: Loss 0.03, Latency 300, Jitter 50
- Salesforce: Loss 0.03, Latency 300, Jitter 300
- Google Workspace: Loss 0.03, Latency 300, Jitter 300
- Webex: Loss 0.03, Latency 300, Jitter 50
- GoTo Meeting: Loss 0.01, Latency 300, Jitter 100

The **Recommendations Summary** widget provides details about the following:

- The current path quality, referring to the assessed quality of the current network paths that the applications are taking.
- The recommended path quality, referring to the quality of the alternate recommended paths.
- The number of impacted users.

By default, **All Recommendations** is selected, and the corresponding recommendations across all application groups are displayed in the **Recommended Actions** widget. In the **Recommendations Summary** widget, you can choose an application, and the **Recommended Actions** widget displays the recommendations for that application.

Click **View Details** to view all recommendations across sites for the chosen application group.

Recommended Actions Widget

The **Recommended Actions** widget provides a detailed view of the path recommendations for various application groups across all sites.

The **Recommended Actions** widget displays complete details about the following:

- The recommendation action that includes a suggestion for an alternate path.
- The qualities of the current path and recommended path with estimated gain
- An estimate of the number of users who are impacted.

Use the search box to filter the information. Use the options in the **View by** drop-down list to filter information for your view by application group, gain %, date or by site.

The **Recommended Actions** widget also provides different provides the following views:

- The default view is the card view to view path recommendations in the form of cards.
- The table view where to view all the sites with summary information in a tabular form.
- The map view to view all the sites and summary information on a map.

When you click an application group in the **Recommendations Summary** widget, the corresponding details of the selected application loads in the **Recommended Actions** widget as per the view type you have chosen.

Click **View details** in the **Recommended Actions** widget to view more details about a specific recommendation, an application group at a site, and about path recommendations.

Click **Show Path and QoS details** to view details of available network paths for individual device pairs, their respective path qualities, and graphs showing loss, latency, and jitter.

Apply Recommended Actions

The recommendations suggested in the **Recommended Actions** widget provide an assessment of the likely gains in path quality benefitting users of the applications. You can use these recommendations to proactively adjust your application-aware routing policies in Cisco SD-WAN Manager to improve the application experience.

Predictive Path Recommendations - Closed Loop Automation

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

The Predictive Path Recommendations (PPR) with Closed Loop Automation feature enables you to apply the recommendations that are generated by PPR automatically using a single click via policy in Cisco SD-WAN Manager. When a policy is applied, you can review the implemented recommendations within Cisco SD-WAN Analytics. The closed loop automation feature simplifies the application of PPR, and enhances the overall application experience, and prevents any violations in service level agreements. For more information about PPR, see Predictive Path Recommendations, on page 35.

Prerequisites

To use the Predictive Path Recommendations - Closed Loop Automation feature, the PPR feature must be integrated with Cisco SD-WAN Analytics. For more information, see Enable Predictive Path Recommendations, on page 36.

Use Closed-Loop Automation

If there are predictive path recommendations available in Cisco SD-WAN Analytics, follow the steps below to implement these suggestions using closed-loop automation.

1. From the Cisco SD-WAN Manager menu, click the bell icon at the top-right corner. The **Notifications** pane is displayed.
2. The **Predictive Networks** section in the **Notifications** pane displays different SD-WAN sites within the network fabric.
3. Click a site.

   You will be redirected to the **Predictive Networks** dashboard in Cisco SD-WAN Analytics.

   The **Recommended Actions** section in Cisco SD-WAN Analytics displays the applications for the selected site.
4. Each application includes an **Apply** button. Click **Apply** to apply the recommendations.
5. Click **Proceed to Apply** to confirm and apply the new recommendations.

   You will be redirected to the Cisco SD-WAN Manager where the policy is automatically updated as per the recommendations.
6. Click **Activate** to confirm activation of the policy with the new recommendations.
7. Cisco SD-WAN Manager displays a preview of the configuration that is ready to be pushed to the device. The right pane displays the device's configuration, and the **Config Preview** tab is selected. Click the

Config Diff tab to view the differences between this configuration and the one currently running on the device.

8. Click **Activate** to push the policy to the Cisco Catalyst SD-WAN Controller, which will then be propagated to the Cisco IOS XE Catalyst SD-WAN devices.
9. View the applied recommendations in Cisco SD-WAN Analytics.

Bandwidth Forecasting

With the Bandwidth Forecasting feature, organizations can predict future network bandwidth needs based on current and historical bandwidth usage data. This feature aids organizations in monitoring usage trends on their circuits and planning their network capacity more effectively for future usage.

In the **Predictive Networks** dashboard, click the **Bandwidth Forecasting** tab to access the Bandwidth Forecasting feature. Alternatively, you can access the **Bandwidth Forecasting** tab through the **Circuits** summary widget, or through the bandwidth utilization chart within the **Circuits** dashboard.

The **Bandwidth Forecasting** tab displays the bandwidth forecast chart for a selected circuit. A table of circuits is displayed with all related metrics such as site, provider information, RX/TX bandwidth, and total usage. Choose a circuit in the table to view its bandwidth forecasting chart.

The bandwidth forecast for a selected circuit shows both the actual and predicted (dotted) lines, offering a forecast for up to 3 weeks from the current date, which is based on data from the past 12 weeks. In addition to showing the current usage, the forecast presents the lower, upper, and mean levels of bandwidth usage for a day. Historical usage data is presented along with the past forecast data points for a quick visual comparison of how the forecast performed against actual recorded values in the past.



Note The minimum data set requirement for forecasts to be generated is 12 weeks of historical daily data for each circuit.

Threat Intelligence

The Threat Intelligence page, powered by Cisco Talos, offers insights into malicious or untrusted IP addresses that have been accessed in Cisco Catalyst SD-WAN.

Talos identifies and lists untrusted IP addresses detected globally. Any threats detected in Cisco Catalyst SD-WAN, where clients are attempting to access these untrusted IP addresses, are displayed on the Security Threat Intelligence page. This information enables you to take appropriate security measures in response to these threats.

Click the **SD-WAN** toggle to view all the sites in Cisco Catalyst SD-WAN. Sites with clients that have interacted with untrusted IP addresses, and which have been marked as untrusted by Cisco Talos with a score between -80 and -100, will be highlighted. You can drill down for additional details about a site that has accessed an untrusted IP address, and the following details are available:

- The physical location of the site.
- The IP address of the site.

- Client interactions over the past 30 days, including the identity information and the frequency of their access to the site.

Anomaly Detection

Anomaly Detection proactively identifies potential network issues by detecting significant deviations in key performance indicators (KPIs) such as loss, latency, jitter, and usage patterns. The system distinguishes between persistent and isolated issues, enabling rapid identification and resolution. By analyzing trends, it provides detailed insights into affected sites and tunnels, guiding actions to optimize network performance. This approach supports early intervention, impact assessment based on site count, usage, and application count, and facilitates adjustments to enhance user experience and reduce network downtime.

Benefits

- Early problem detection: Identify patterns before they escalate into larger issues, allowing for timely intervention.
- Optimize network performance: Fine-tune your network to enhance the end-user experience, ensuring smooth and efficient operation.
- Improve operational efficiency: Streamline operations and reduce downtime, leading to more efficient and reliable network management.

Anomaly Detection in Cisco Catalyst SD-WAN Analytics

To view anomaly information, click the **Anomaly Detection** tab under **Predictive Networks**. You can view network anomalies across the following dimensions:

- Anomaly detection in sites
- Anomaly detection in usage patterns

Anomaly Detection in Sites

This feature helps you detect anomalies at the site level. Select a site with detected anomalies to access a seven-day, hourly overview of anomaly rates, displayed through interactive bar charts. Click on any bar to view specific hourly data. A summary table displays detected anomalies across impacted sites and tunnels.

For deeper analysis, click on a tunnel at a site to view the **Anomaly and Usage Trend** page for that tunnel. This page provides detailed information on loss, latency, and jitter trends over time, enabling you to identify and address anomalies efficiently.

Anomaly Detection in Usage Patterns

This feature helps you to identify anomalies in cellular usage patterns. It presents a seven-day view showing the percentage of cellular circuits with detected anomalies and the total usage across all circuits in Cisco Catalyst SD-WAN.

Table 11: Cellular Usage Information

Anomaly Information	Description
Anomaly Summary	Lists circuits with detected anomalies. Select a specific circuit to view current usage versus baseline.
Circuits usage	Displays the current usage for the selected circuit.
Circuits availability	Displays the usage of alternate circuits during anomaly events and the availability of these alternatives.
Application	Identifies which applications are driving high utilization.
Top clients	Highlights clients using specific applications that contribute to high utilization on cellular circuits.

Traffic Logs

Traffic logs is a network flow monitoring tool integrated into Cisco Catalyst SD-WAN Analytics. It allows authorized users to access and visualize filtered firewall connection event logs derived from voluminous flow records. Users can submit queries specifying criteria such as time frame, site name, devices to get logs on-demand.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, traffic logs are available under **Monitor** > **Logs**.

Benefits of traffic logs

- Provides detailed visibility into raw flow logs, including firewall connection events and related attributes.
- Supports scalable processing and analysis of high-volume flow data.
- Enables users to filter logs of interest to quickly narrow down large datasets, even across millions of records.
- Utilizes SD-WAN Analytics to deliver both the frontend and backend as a cloud-based solution.

Restrictions for traffic logs

- Only one request can be made at a time across the fabric.

  All users of the fabric have to wait for this request to complete.

- There are rate limits at the fabric level.

  24 requests can be made in a period of 24 hours, and 24 exports can be made in a period of 24 hours, which is calculated across all users of the fabric.

- Maximum of five devices can be queried at a time.
- Maximum time duration for filtering is seven days.
- The data fetched for a log query is limited to within the last month.
- Export is limited to 1,048,576 rows to be compatible with tools like Excel.

Generate traffic logs using Cisco SD-WAN Manager

Procedure

Step 1 Click the **Logs** tab.

Step 2 In the query builder section, specify the mandatory filters:

- Time period
- Site(s) (maximum five)
- Device(s) (maximum five). Select a device.

Optional: Click **Advanced** to display the Circuit rule and Firewall rule filters.

Circuit rule: Select one or more circuits.

Firewall rule: Select one or more firewall rules.

Step 3 Click the **Get Logs** button.

Note
If available, the last traffic logs request would be fetched and visualized by default.

The Traffic log requests list displays previous requests, including the request name, created time, status, time period, sites, devices, and expiration time.

To display the logs returned for a request, click **View logs** for that request.

You can rename a request to assign it a more user-friendly name.

To view historical flow information for a circuit, specify the Time period, Site, and Device filters. Click **Advanced**, select one or more circuits using Circuit rule, and click **Get Logs.**

Table 12:

Field	Description
Event Time (in UTC)	Displays the exact date and time thta the event was logged, recorded in Coordinated Universal Time (UTC) for standardization.
Site	Displays the physical location, office, or branch where the event was generated.

Field	Description
Hostname	Displays the name given to a device on a network, which can be used to identify it. It can be up to 128 characters long.
System IP	Displays the IP address assigned to the system or device that generated the event log.
VPN ID	Displays an identifier (such as a number or string) representing the specific VPN tunnel or connection involved in the event.
Source IP	Displays the IP address from which the network traffic originated.
Destination IP	Displays the IP address to which the network traffic was sent.
Source Port	Displays the port number used by the source device in the network communication
Destination Port	Displays the port number used by the destination device in the network communication.
Protocol	Displays the communication protocol used for the network session.
Application Name	Displays the name of the application or service associated with the network traffic
Username/SGT	Displays the account name or ID of the user associated with the event, if available.
Firewall Rule	Displays the specific rule within the firewall that matched and processed the event.
FW Policy	Displays the name or identifier of the firewall policy that applies to the traffic or event.
FW Action	Displays the action taken by the firewall for this event.

Note
For the firewall attribute columns to be populated, you need to set up firewall policies in Cisco SD-WAN Manager. For more information, see Unified Logging for Security Connection Events.

What to do next

Click the **Export** button to download the results for offline analysis.

Troubleshoot traffic logs

If you wish to troubleshoot traffic logs, contact Cisco TAC for assistance.

Optimization

The AppQoE solution helps mitigate WAN link limitations to optimize application performance.

The AppQoE solution consists of WAN optimization techniques such as TCP Optimization, Data Redundancy Elimination (DRE), SSL Proxy, Forward Error Correction (FEC) and Packet Duplication.

For more information about AppQoE, see Traffic Optimization with DRE.

The **Optimization** tab displays the AppQoE dashboard that provides insights into the performance and enablement of the TCP Optimization and DRE. It presents key feature metrics, granular per-site views, and helps identify where policies can be applied for further optimization. Data can also be exported for offline consumption.

Optimization metrics

The optimization metrics on the APPQoE dashboard offer a overview of your network's application performance enhancement.

Table 13: Optimization Metrics

Optimization	Description
TCP Optimized Volume	Displays the Percentage of total traffic volume that is successfully TCP optimized, across sites where TCP optimization is enabled.
DRE Bandwidth Reduction Ratio	Displays the average bandwidth reduction achieved by DRE, across sites where DRE is enabled.
Sites Optimizing Traffic using APPQoE	Shows the count of sites where AppQoE is enabled and the total number of sites.

Pie chart visualizations

Table 14: TCP/DRE Optimization Pie Chart

Optimization Categories	Description
Non-TCP Traffic	Total traffic volume at all sites, not eligible for TCP optimization or DRE.
No Policy	Total traffic volume at all sites, eligible for TCP optimization or DRE, but no policy is enabled.
Optimized	Total traffic volume at all sites, subjected to TCP optimization or DRE successfully.

Optimization Categories	Description
Passthrough	Total traffic volume at all sites, subjected to TCP optimization or DRE, but failed. Failures can occur due to various reasons, such as device resource limitations or hardware constraints.

Traffic optimized by APPQoE

The Sites and Applications table provides granular per-site and per-application views of the APPQoE optimization.

Table 15: Traffic optimized by APPQoE for a site

Optimization	Description
Site Name	View the name of the site. Clicking on a site displays comprehensive APPQOE optimization information for that specific site.
Total Volume	The total traffic volume for all applications at the site before optimization.
TCP Optimized Volume	The traffic volume that is successfully TCP optimized at the site.
Pre-DRE Volume	The traffic volume before DRE.
Post-DRE Volume	The traffic volume after DRE.
DRE Bandwidth Reduction %	The bandwidth reduction achieved by DRE.
Paired Sites	When you click on a site, the **Paired Sites** section displays optimization details for traffic between two specific sites where APPQOE optimization is applied. Metrics such as Total Volume, TCP Optimized Volume, Pre-DRE Volume, Post-DRE Volume, and DRE Bandwidth Reduction % are calculated and displayed for these paired sites.
View Details	Provides in-depth information about TCP Optimization and DRE for all applications at a selected site.

Table 16: Traffic optimized by APPQoE for an application

Optimization	Description
Application Name	Displays the name of the application. Clicking on an application displays comprehensive APPQOE optimization information for that specific application.

Optimization	Description
Total Volume	The total application traffic volume across all sites before optimization.
TCP Optimized Volume	The application traffic volume that is successfully TCP optimized.
Pre-DRE Volume	The application traffic volume before DRE.
Post-DRE Volume	The application traffic volume after DRE.
DRE Bandwidth Reduction %	The bandwidth reduction achieved by DRE.

Reports

The Reports feature helps you generate periodic reports for all applications and all sites.



Note You must be a Cisco Plug and Play (PNP) Smart Account Administrator or a Virtual Account Administrator to use the Reports feature.

1. From the Cisco SD-WAN Manager menu, click **Reports**.
2. The **Reports** page displays a list of generated reports. Click **Reports Templates**.

   The **Report Templates** page displays different reporting templates for you to choose from. The options are PDF and CSV formats.
3. Choose PDF or CSV and click **Generate**.
4. Enter a name for the report and click **Next**.
5. Choose the scope of the report and click **Next**.

   Choose **All Applications** or specific applications for which you want to generate the report.
6. Choose a time schedule for the report and click **Next**.
7. Enter the email address of the recipients and click **Next**.

   A confirmation page with the summary of the report displays. You can enter up to five email recipients. The passkey for the report is available on this page, and also on the final summary page.
8. Click **Submit**.

   After the report is generated, it is sent as a PDF to the recipients over email.

   Depending on the file format you have chosen, the report is generated, it is sent as a PDF or a CSV file to the recipients over email.

Note

- The PDF and the CSV file are password-protected. Use the passkey available on the **Delivery and Notification** page, or on the report's **Summary** page to unlock the PDF or the CSV report.
- The Executive Summary report is available only in the PDF format and not in the CSV format.

Troubleshooting

Cannot Log in to the Cisco SD-WAN Analytics Portal

Problem

Unable to log in to the Cisco SD-WAN Analytics portal.

Possible Causes

The issue may be a lack of privileges in the user's Smart account. It is necessary to have Smart Account admin or Smart Account user privileges, Virtual Account admin, or Virtual Account user privileges, to access the Cisco SD-WAN Analytics portal using a Cisco.com ID.

Solution

If a user does not have access to their organization's Smart account, please contact your Smart account administrator to provide access to the Smart account. The user can log in when access has been granted.

No Data in Cisco SD-WAN Analytics

Problem

The Cisco SD-WAN Analytics portal does not show any data.

Possible Causes

It is possible that the edge devices lack DPI configuration, which prevents them from capturing or exporting any application-related data.

Solution

To enable DPI on Cisco IOS XE Catalyst SD-WAN devices, see Cisco Catalyst SD-WAN Application Intelligence Engine Flow.

To enable DPI on Cisco vEdge devices, see app-visibility, flow-visibility.

Some users choose to disable DPI processing Cisco SD-WAN Manager. Disabling DPI processing on Cisco SD-WAN Manager has no effect on Cisco SD-WAN Analytics. Statistics are still exported as long as DPI is enabled on the device.

No Data is Displayed in vAnalytics: DPI Enabled

Problem

vAnalytics portal does not display any data even when DPI is enabled on the edge devices.

Possible Causes

It is possible that the edge devices are only generating DIA traffic and not tunnel traffic.

Solution

The vAnalytics portal displays only site data when tunnel traffic is generated or when DIA traffic is generated with minimum CoR SaaS enabled for the overlay.

Traffic sent directly to the internet, also referred as DIA, is not displayed in the vAnalytics portal.

Error 400, General Non-Success, Seen on Okta Page

Problem

Error 400, General Non-Success, seen on Okta page.

Possible Causes

Most likely caused by missing required SAML or OIDC assertions that are configured on the customer IDP side (first name, last name, and email).

Solution

Add the missing assertions on the customer IDP side.

After Logging in with SSO, a User is Redirected to Cisco Okta Website

Problem

After logging in with SSO, a user is redirected to Cisco Okta website.

Possible Causes

This issue occurs when you open Cisco SD-WAN Analytics using an embedded url instead of using the actual url.

Solution

Use the actual analytics link to log in to Cisco SD-WAN Analytics.

You can use the embedded url if you configure a **relay state** on your SSO client that links to Cisco SD-WAN Analytics.

Appendix

This section provides details on how to request new Cisco SD-WAN Analytics and enable data collection on Cisco SD-WAN Manager.

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 SD-WAN Manager 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 Cisco SD-WAN Analytics.

   If both the Cisco SD-WAN Manager and Cisco SD-WAN Analytics are being newly created, Cisco enables Cloud Services and enters the OTP while configuring the Cisco SD-WAN Manager instance.

   If you using Cisco SD-WAN Analytics and are upgrading your Cisco SD-WAN Manager 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 SD-WAN Analytics using one of the URLs listed in Access Cisco SD-WAN Analytics, on page 17.

Enable Data Collection (Cisco vManage Release 20.1 or Earlier)

1. From the Cisco SD-WAN Manager 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 SD-WAN Analytics using one of the URLs listed in Access Cisco SD-WAN Analytics, on page 17.

Additional Steps to Enable Data Collection on an On-Premises Cisco SD-WAN Manager Instance

Configure the local firewall to allow outbound communication from Cisco SD-WAN Manager (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 SD-WAN Analytics instance.



Note If the network path only supports an MTU smaller than 1500 bytes and PMTU discovery is enabled, ICMP responses blocked by the firewall may prevent Cisco SD-WAN Manager from dynamically adjusting the MTU. In such cases, either configure the Cisco SD-WAN Manager interface MTU to match the network MTU or ensure ICMP traffic is allowed through the firewall. For more information, see *Interface MTU* in the *Cisco Catalyst SD-WAN Interfaces Configuration Guide, Releases 26.x and Later*.

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) https://swapi.cisco.com https://public.ops.analytics.sdwan.cisco.com https://cdn.sdwan.cisco.com
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) https://swapi.cisco.com https://public.ops.analytics.sdwan.cisco.com https://cdn.sdwan.cisco.com

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) https://swapi.cisco.com https://public.ops.analytics.sdwan.cisco.com https://cdn.sdwan.cisco.com
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) https://swapi.cisco.com https://public.ops.analytics.sdwan.cisco.com https://cdn.sdwan.cisco.com

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