Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.13.x

First Published: 2023-12-18

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

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.

Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.13.x

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.

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager, as applicable to Cisco IOS XE Catalyst SD-WAN devices.

Related Releases

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.13.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.13.x

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections	This feature adds support for the Transport Layer Security (TLS) 1.3 protocol for Cisco Catalyst SD-WAN control connections.

Feature	Description
Configure Third-pary CA Certificates to Cisco IOS XE Catalyst SD-WAN Devices using Cisco SD-WAN Manager	Directly upload CA (Certificate Authority) certificates to Cisco SD-WAN Manager and manage the certificates. This feature makes certificate management simpler, you just select the CA certificate file from your device and upload to Cisco SD-WAN Manager ensuring secure communication and data transfer over the network.
Enhancements in License Management	Updated license management as follows: Moved selection of license type from license synchronization to license assignment. Added preview of existing template when selected during license assignment. Removed Mixed mode from license types. Added ability to view devices associated with a template and delete a template.
Specify a Region and Subregion When Deploying a Device	You can specify both a region and a subregion when deploying a device.
Cisco Catalyst SD-WAN Security	
Cisco Secure Access Integration	Cisco Secure Access is a cloud security Secure Service Edge solution, that provides seamless, transparent, and secure Direct Internet Access (DIA). This feature supports Cisco Secure Access integration through policy groups in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Cloud OnRamp	
Add Cloud OnRamp for SaaS support for loopback, dialer, and subinterfaces	This feature extends the Cloud OnRamp for SaaS support to SD-WAN supported WAN interfaces that includes loopback, dialer, and subinterfaces. It also adds support for TLOC-extension and SIG on loopback, dialer, and subinterfaces.
Option to exclude data prefixes from Cloud OnRamp for SaaS optimization	This feature allows you to define IP prefixes that you want to exclude from being treated for Cloud OnRamp for SaaS optimization.
Enable faster failover by associating a DIA tracker with Cloud OnRamp for SaaS	This feature allows you to associate a tracker with Cloud OnRamp for SaaS for a DIA or gateway site that detects a failed interface faster than Cloud OnRamp for SaaS probing.
AWS Cloud WAN Integration with Dynamic Routing	This feature is an enhancement to the AWS Cloud WAN integration to support site to site communication using dynamic routing.
Cisco Catalyst SD-WAN AppQoE	

Feature	Description
SSL Proxy Support for TLS 1.3	With this feature, SSL proxy in AppQoE supports the TLS protocol version 1.3.
Cisco Catalyst SD-WAN Monitor and Maintain	
Generate Admin-tech File with the Feature Filter	This feature enhances the admin-tech file to generate or collect more detailed feature specific information. The feature-specific technical information is generated in addition to the regular information using the tech filter. The admin-tech file can collect more detailed feature-specific information with the tech feature filter. For example, you can generate separate folders in the admin tech file for IPsec and security policy, which can be helpful when troubleshooting.
Network-Wide Path Insight Integration with Cisco Identity Services Engine	When Cisco Identity Service Engine is integrated with Cisco Catalyst SD-WAN, this feature enables traces to provide the identity of users who send traffic to and receive traffic from applications.
IPv6 support in Cisco SD-WAN Manager UI Troubleshooting	Added support for using an IPv6 address when pinging a device. Also added support for using an IPv6 address when running a traceroute, configuring packet capture, and simulating flows.
Cisco Catalyst SD-WAN NAT	
ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces	This feature allows you to configure an ICMP endpoint tracker over a DIA path. You can configure the ICMP tracker for NAT DIA on IPv4 or IPv6 endpoints. You can configure ICMP tracker using the **Tracker** or the **IPv6 Tracker** features under transport profile in configuration groups.
Support to automatically configure IPv6 address on a WAN interface by using SLAAC with a Router Advertisement (RA) prefix.	You can configure the Stateless Address Autoconfiguration (SLAAC) by using the RA prefix to automatically assign IPv6 addresses for NAT66 prefix translations.
Support for Flow Stickiness	Flow stickiness records the flow level state of the NAT path and ensures that the application flows don't get reset due to a change in the NAT path. When the first packet match fails in deep packet inspection (DPI), the Edge router ensures the first flow for this unknown application to stick to the original path, bypassing the policy to change the path when it is recognized by the DPI engine a few packets later.

Feature	Description
Support for Centralized data policy for NAT66 DIA.	You can configure the Centralized data policy by using the `nat use-vpn 0` command, which ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria. This feature is supported from service and from tunnel. The fallback option ensures that the traffic falls back to routing and takes the overlay path when the DIA route is not available.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Specify Path Type Preference with Restrict Mode	With this feature, the preferred color group action in app-route and data-policy has additional color-restrict option available to restrict traffic to configured colors. With this option, if multi tiered preferred colors are not available then, the traffic is dropped.
Management Region	A management region is a specialized region that can span all access regions in a Multi-Region Fabric architecture. A management region enables hub-and-spoke connectivity between any router in the network and one or more management gateways. Connectivity between a router and a management gateway uses access region transport services. The connectivity does not use the core region transport service, even when the router and management gateway are in different access regions.
Configure Multi-Region Fabric and Related Features Using Configuration Groups	Configure Multi-Region Fabric features, such as role, region, and so on, and configure transport gateway path behavior on routers, using configuration groups.
Cisco Catalyst SD-WAN Policy Groups	
Configure Traffic and Flow Visibility for Application Priority and SLA policy	This feature allows you to configure additional settings to enable traffic and flow visibility for the application priority and SLA policy in Cisco Catalyst SD-WAN. After you have configured the Cflowd collector in the Network Hierarchy menu in Cisco SD-WAN Manager, you can monitor application and traffic flow over IPv4, IPv6, or both networks at the global hierarchy level.
Configure Secure Service Edge	This feature supports Secure Service Edge configurations for Cisco Secure Access as provider.
Application Catalog	The **Application Catalog** feature provides visibility and identification for applications running in your network environment. The Application Catalog is continuously updated as new applications are developed and existing ones are updated, ensuring that your Cisco SD-WAN Manager environment can adapt to changes in application use. The Cisco SD-WAN Manager integrates Kubernetes cluster discovery and monitoring to monitor your network infrastructure and your containerized applications from a single interface. The feature streamlines the monitoring of your network and applications while providing superior visibility and control.
Cisco Catalyst SD-WAN Systems and Interfaces	

Feature	Description
Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment	This feature supports the migration of a tenant from a multitenant overlay to a single-tenant deployment. To migrate a tenant between two Cisco Catalyst SD-WAN deployments, move the tenant configurations, statistical data and WAN edge devices from one deployment to another.
Support for EtherChannels on the Transport Side	Adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN device. This feature also introduces support for aggregate EtherChannel Quality of Service (QoS) on the transport side. By combining EtherChannel and QoS, you can optimize network utilization, enhance performance, and maintain quality for specific traffic types. **Note** This feature has limited availability.
Co-Management: Granular Role-Based Access Control	This feature introduces role-based access control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scope, users and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
IP DHCP Smart-Relay	This feature allows the DHCP relay agent to set the gateway address to the secondary IP address when there is no DHCPOFFER message from the DHCP server. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers. This functionality is useful when the DHCP server cannot be configured to use secondary pools.
Support for Traffic Flow Collectors	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through Cisco Catalyst SD-WAN devices in the overlay network and exports flow information to the collector. Security logging allows the security logging server to collect and export the syslogs and provides an option to specify a server for high-speed logging (HSL). You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.
Cisco Catalyst SD-WAN Segmentation Configuration Guide	
Added Support for 2,000 VRFs	Increased support from 300 VRFs to 2,000 VRFs in the overlay network, with up to 500 for a single device.
Cisco Catalyst SD-WAN High Availability Configuration Guide	

Feature	Description
Disaster Recovery Reliability Improvements Phase 1	This feature removes the **Pause Replication** button from the **Disaster Recovery** screen. Replication pauses automatically when you pause disaster recovery and resumes when you resume disaster recovery.

New and Enhanced Hardware Features

New Features

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.13.x

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Behavior Change	Description
Controller mode for Cisco ASR 1006-X routers containing RP3 module is no longer supported.	The RMA Replacement of the Cisco ASR 1006-X Chassis and RMA Replacement of the Cisco RP3 Module sections describe the behavior change in detail.
The enterprise certificate notifications for Cisco IOS XE Catalyst SD-WAN devices are enhanced to include critical notifications about certificate expiry.	The Support for SNMP Traps on Cisco Catalyst SD-WAN devices section describes the behavior change in detail.
If your system is configured with an SNMP community string that is longer than 15 characters, in some situations SNMP configuration must be reconfigured after upgrading to Cisco Catalyst SD-WAN Manager Release 20.13.1.	The Configure SNMP using Cisco SD-WAN Manager section describes the behavior change in detail.
You cannot update the Cisco Catalyst 8500-12X4QC port configuration to 2 ports of 100GE by using the Flexible Port Speed feature.	The Flexible Port Speed feature describes the behavior change in detail.
This release ends Cisco Catalyst SD-WAN support for most Cisco ISR 4000 Series Integrated Services Routers, with the exception of the Cisco ISR 4461 router, which is still supported. For the routers no longer supported in this release, Cisco IOS XE Catalyst SD-WAN Release 17.12.x is the last supported release.	The Cisco Catalyst SD-WAN Device Compatibility page shows the supported releases for each model.

Important Notes, Known Behaviors, and Workarounds

SFP-10G-SR module

Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of the module.

Software maintenance upgrade (SMU)

The minimum supported release for software maintenance upgrade (SMU) is Cisco IOS XE Catalyst SD-WAN Release 17.12.3a. It was previously described as Cisco IOS XE Catalyst SD-WAN Release 17.12.1a. See Supported Devices for Software Maintenance Upgrade.

esp-null Deprecated

In Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the esp-null encryption algorithm is deprecated. When configuring Secure Internet Gateways (SIG), selecting the NULL-SHA1 cipher will invoke esp-null and result in template push failures. To avoid deployment errors, configure SIG with a supported encryption algorithm.

Disaster Recovery

The user account used for disaster recovery supports only local authentication and does not support remote authentication methods such as TACACS+ or RADIUS. This user must be dedicated solely to disaster recovery tasks and must not be used for any other functions, such as cluster management because of the following reasons:

- Reliability: Using dedicated accounts for DR sync minimizes configuration errors and reduces operational risks.
- Resilience: Prevents issues related to user lockouts or account overrides, ensuring DR processes are not impacted by administrative changes to other accounts.
- Audit and compliance: Dedicated users provide clear separation for auditing purposes, making it easier to track and log DR-related activities.
- Industry standard: All our customers, including those in highly regulated sectors such as finance, follow this model. It is the recommended and supported deployment standard.
- Avoid remote authentication issues: TACACS-based users are prone to disruptions due to potential latency or connectivity issues with remote authentication servers. Using local accounts eliminates these risks, ensuring uninterrupted DR sync and cluster operations.
- Password rotation: Capabilities are provided via API/GUI on active cluster and through CLI on standby cluster.

TLOC extension configuration

If a device

- is using Cisco IOS XE Catalyst SD-WAN Release 17.9.x or earlier, and
- the device has a tunnel interface configuration includes a TLOC extension,

then you cannot upgrade to one of these:

- 17.12.1 through 17.12.4
- 17.15.1 through 17.15.2

Attempting such an upgrade causes the device to crash and enter a rollback state.

If you have a TLOC extension configured and need to perform such an upgrade, remove the TLOC extension configuration from the tunnel interface configuration before upgrading.

This issue was fixed and does not apply for upgrades from one of these releases:

- 17.12.5 and later releases of 17.12.x
- 17.15.3 and later releases of 17.15.x
- 17.18.1a and later

Resolved and Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.13.x

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Identifier	Headline
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
CSCwf45486	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Identifier	Headline
CSCwi31833	UTD deployment failing if deployed from remote server hostname rather than ip
CSCwi33634	Cisco IOS XE Catalyst SD-WAN device is incorrectly consuming icmp reply packets.
CSCwi35716	AAR backup preferred color not working as expected from 17.12.1
CSCwh84068	Cisco Catalyst 8000V crashes after changing NAT HSL configuration.
CSCwi16716	Cisco Catalyst 8500 : Router crashed upon increasing the gatekeeper cache size
CSCwh77221	SNMP Unable to poll Cisco Catalyst SD-WAN Tunnel Data after a minute
CSCwi15930	ASR1001-HX failing to upgrade from 17.6.3a to 17.6.5 due to CDB issue
CSCwi36062	Cisco IOS XE Catalyst SD-WAN device - 'show isdn' and 'debug isdn' commands are missing
CSCwi31523	After reboot EPBR does not work on C8500-12X4QC
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed
CSCwh01678	20.12 ISR1100 platform FTM crash with SIG enabled

Identifier	Headline
CSCwi32883	Cisco Catalyst 8500 crashes from PA Interrupt running NAT
CSCwi05680	Cisco Catalyst 8300 Crashed generating multiple system reports
CSCwf69062	SDRA-SSLVPN : The sslvpn session closes with re-authentication error after some interval of time
CSCwi31747	SymNat with low bandwith is not working
CSCwi00369	Cisco IOS XE Catalyst SD-WAN device lost security parameter after upgrade
CSCwi13563	IP SLA probe for End-point-tracker doesnt work once endpoint tracker is changed until reload
CSCwi27400	Last-resort circuit delay coming up with TLOC extension when multiple name-servers configured
CSCwi25476	Cisco Catalyst 8500 crash with mDNS packet due to IOSXE-RP Punt Service Process
CSCwi05395	The snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs
CSCwi46413	Cisco IOS XE Catalyst SD-WAN device does not install OMP route with high preference using service chaning
CSCwi32044	Device reboot due to "Critical process vip_confd_startup_sh"
CSCwi15688	Unexpected NAT translation occurs in a specific network
CSCwi44633	Fragmented Radius Access-Request packets are dropped when NWPI is running
CSCwi16015	[SIT]: SSE tunnels don't come up with Dialer interface.Relax check in IKE
CSCwh52440	IP SLA doesnt have checks for ICMP probes to be sent on source interface.
CSCwi46034	OnDemand TLOCs installed without traffic passing through
CSCwi19875	Cisco IOS XE Catalyst SD-WAN device is unable to process hidden characters in a file while trying to use bootstrap method

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

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Supported Devices

For device compatibility information, see Cisco Catalyst SD-WAN Device Compatibility.

Cisco Catalyst SD-WAN Manager GUI Changes

The following are significant GUI updates in Cisco Catalyst SD-WAN Manager Release 20.13.1.

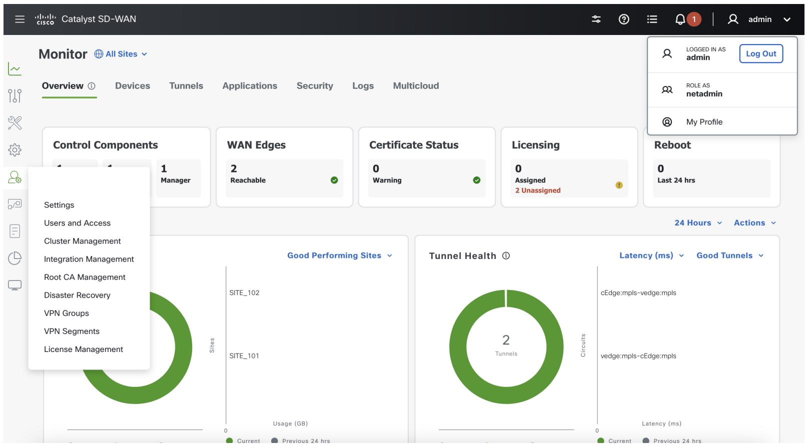
Enhanced Dashboard Experience

The Cisco Catalyst SD-WAN Manager Release 20.13.1 GUI is now updated, based on the Cisco design system, which enhances the look and feel of the dashboard. This upgrade offers a unified experience across various other Cisco products by maintaining consistent design and theme elements.

Some of the significant changes are as follows:

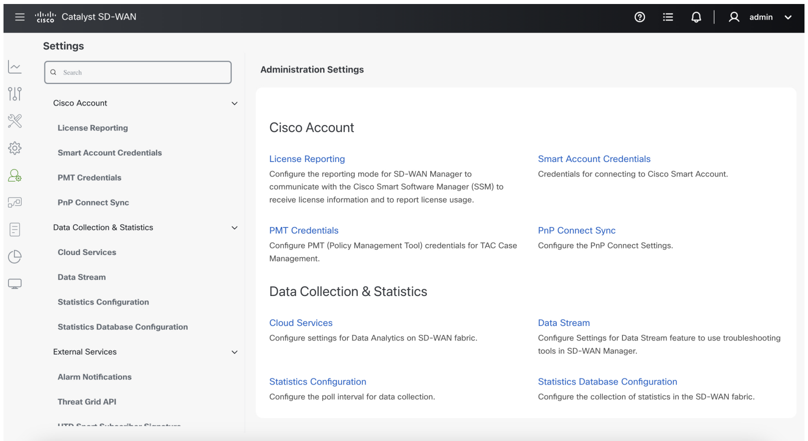
- Monitor Overview page:
  - The navigation panel with menu icons is visible on the left pane. Hover over an icon to view the title or click the hamburger icon to expand the menu options.
  - The **Select Resource Group** option is deprecated.
  - The **Profile** drop-down menu in the top right of the dashboard includes the **My Profile** and the **Log Out** options.
  - In multitenant mode, a **Select Tenant** drop-down list is available at the top-left.

Figure 1: Enhanced Monitor - Overview Page in Cisco Catalyst SD-WAN Manager Release 20.13.1



- **Administration** > **Settings** page - The settings are categorized as follows:
  - **Cisco Account**
  - **Data Collection & Statistics**
  - **External Services**
  - **System**
  - **Trust and Privacy**

Figure 2: New Settings Layout in the Administration Menu in Cisco Catalyst SD-WAN Manager Release 20.13.1



Administration Settings

Cisco Account

License Reporting
Configure the reporting mode for SD-WAN Manager to communicate with the Cisco Smart Software Manager (SSM) to receive license information and to report license usage.

Smart Account Credentials
Credentials for connecting to Cisco Smart Account.

PMT Credentials
Configure PMT (Policy Management Tool) credentials for TAC Case Management.

PnP Connect Sync
Configure the PnP Connect Settings.

Data Collection & Statistics

Cloud Services
Configure settings for Data Analytics on SD-WAN fabric.

Data Stream
Configure Settings for Data Stream feature to use troubleshooting tools in SD-WAN Manager.

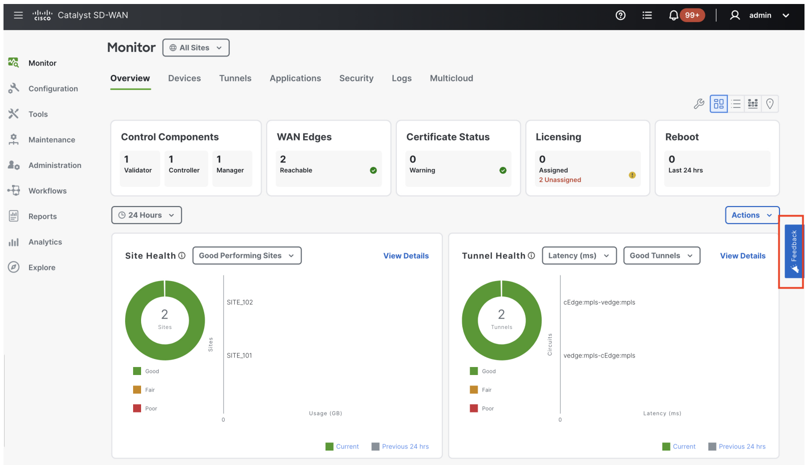
Statistics Configuration
Configure the poll interval for data collection.

Statistics Database Configuration
Configure the collection of statistics in the SD-WAN fabric.

Feedback About Cisco Catalyst SD-WAN

Starting from Cisco Catalyst SD-WAN Manager Release 20.13.1, you can provide feedback about Cisco Catalyst SD-WAN by clicking the **Feedback** option that is available on the right as a collapsible side bar.

Figure 3: Feedback in Cisco Catalyst SD-WAN Manager Release 20.13.1



You can select a feedback topic from the following options and rate your experience:

- Analytics, monitoring, or troubleshooting
- Software reliability
- Multicloud or security

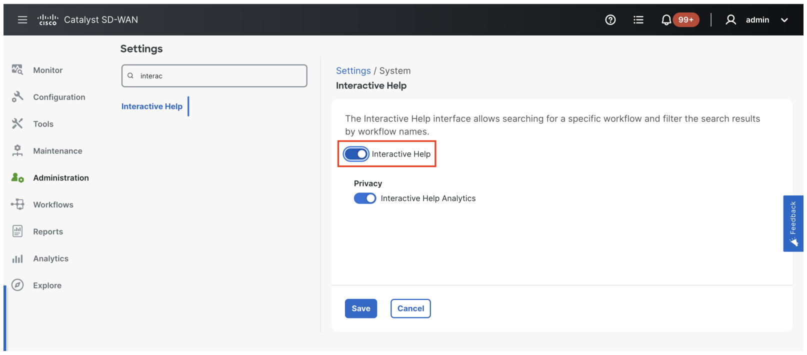
To disable the **Feedback** option, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Navigate to the **System** menu and click **Interactive Help**.
3. Disable **Interactive Help**.

Warning Interactive help setting controls both the **Interactive Help** and the **Feedback** features. Disabling the **Interactive Help** setting disables both the features.

4. Click **Save**.

Figure 4: Administration Settings - Interactive Help in Cisco Catalyst SD-WAN Manager Release 20.13.1



The Interactive Help interface allows searching for a specific workflow and filter the search results by workflow names.

Interactive Help

Privacy

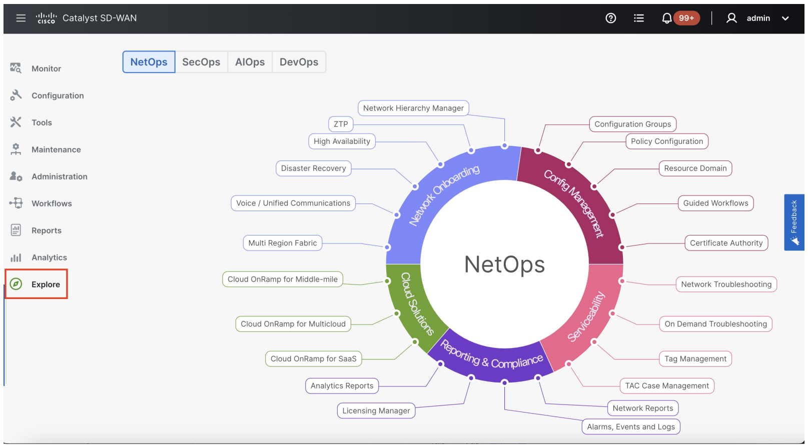
Interactive Help Analytics

Explore Cisco Catalyst SD-WAN Features Based on Job Roles

In Cisco Catalyst SD-WAN Manager Release 20.13.1, the new **Explore** menu option opens a page presenting four job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. Based on the job role that you choose, the Explore page displays relevant Cisco Catalyst SD-WAN features, along with other Cisco resources such as developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more.

A graphic presents the resources relevant to the job role. For more information, see Explore.

Figure 5: Explore Features Based on Job Roles in Cisco Catalyst SD-WAN Manager Release 20.13.1

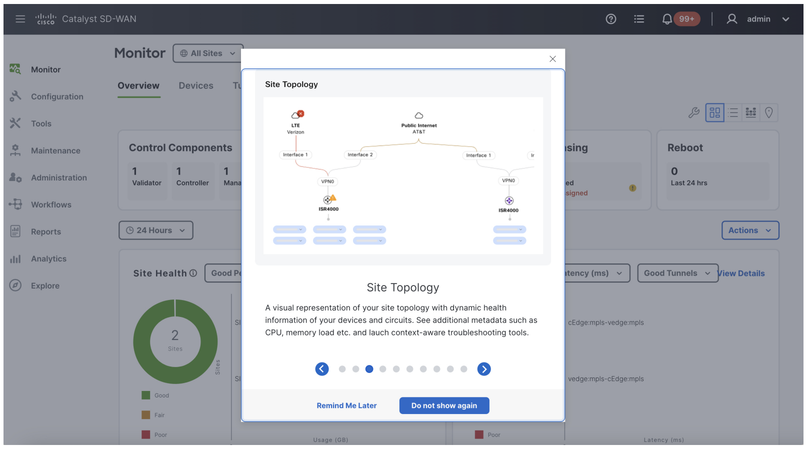


Feature Spotlight

When you log in to Cisco SD-WAN Manager, the **Spotlight** window appears in the overview page, highlighting the new features that are available. The spotlight window displays features along with the feature summary. You can return to the spotlight by clicking the **?** icon in the Cisco SD-WAN Manager menu and choosing **Spotlight**.

Click **Do not show again** to dismiss spotlight. This action ensures that the spotlight window doesn't appear again.

Figure 6: Spotlight in Monitor - Overview in Cisco Catalyst SD-WAN Manager Release 20.13.1

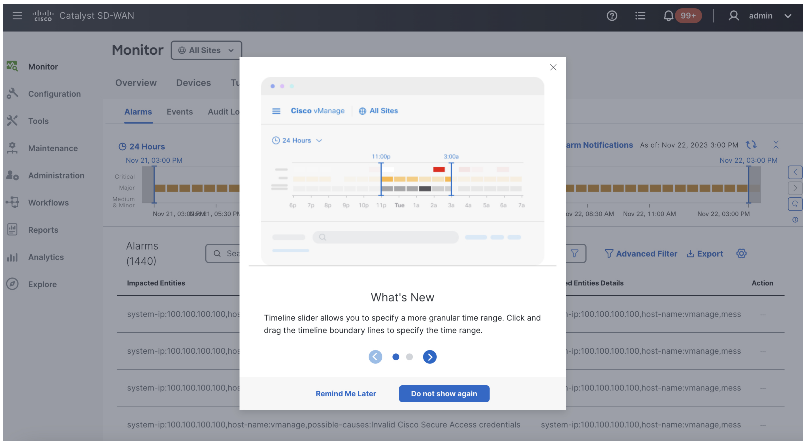


Site Topology

A visual representation of your site topology with dynamic health information of your devices and circuits. See additional metadata such as CPU, memory load etc. and lauch context-aware troubleshooting tools.

The spotlight feature is available in other Cisco SD-WAN Manager pages and highlights features specific to that menu. For example, the spotlight in the **Monitor** > **Logs** page displays only two features:

Figure 7: Spotlight in Monitor - Logs in Cisco Catalyst SD-WAN Manager Release 20.13.1



What's New

Timeline slider allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.

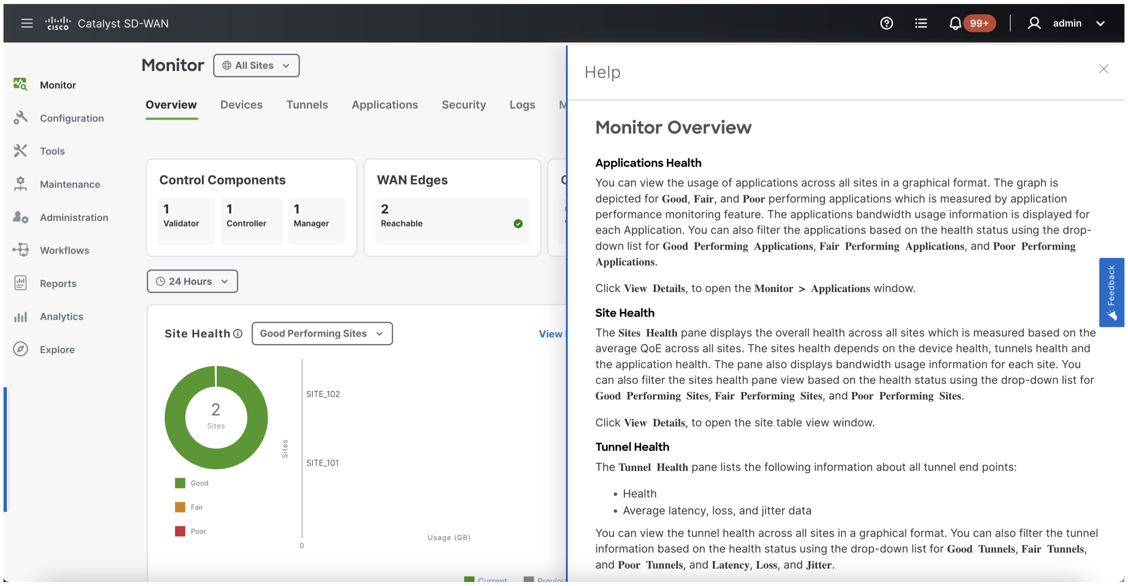
```
system-ip:100.100.100.100,host-name:vmanage,possible-causes:Invalid Cisco Secure Access credentials    system-ip:100.100.100.100,host-name:vmanage,mess
```

In-product Help

In a single-tenant deployment, access help content for Cisco SD-WAN Manager UI pages by clicking the **Help** icon at the top-right corner of a page. The help content is displayed in a slide-in pane in the same browser window.

Starting from Cisco SD-WAN Manager Release 20.12.x, In-product help is available for a majority of the Cisco SD-WAN Manager UI pages.

Figure 8: Help Content in a Slide-in Pane



Help

Monitor Overview

Applications Health

You can view the usage of applications across all sites in a graphical format. The graph is depicted for **Good**, **Fair**, and **Poor** performing applications which is measured by application performance monitoring feature. The applications bandwidth usage information is displayed for each Application. You can also filter the applications based on the health status using the drop-down list for **Good Performing Applications**, **Fair Performing Applications**, and **Poor Performing Applications**.

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

Site Health

The **Sites Health** pane displays the overall health across all sites which is measured based on the average QoE across all sites. The sites health depends on the device health, tunnels health and the application health. The pane also displays bandwidth usage information for each site. You can also filter the sites health pane view based on the health status using the drop-down list for **Good Performing Sites**, **Fair Performing Sites**, and **Poor Performing Sites**.

Click **View Details**, to open the site table view window.

Tunnel Health

The **Tunnel Health** pane lists the following information about all tunnel end points:

- Health
- Average latency, loss, and jitter data

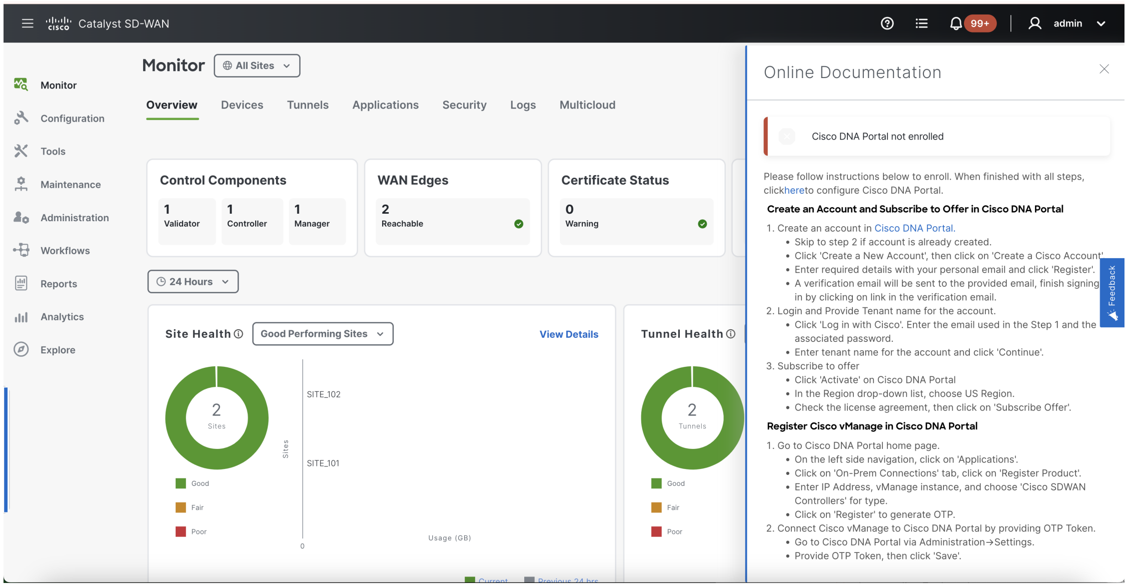
You can view the tunnel health across all sites in a graphical format. You can also filter the tunnel information based on the health status using the drop-down list for **Good Tunnels**, **Fair Tunnels**, and **Poor Tunnels**, and **Latency**, **Loss**, and **Jitter**.

Cisco DNA Sense

Access help content for Cisco SD-WAN Manager UI pages using Cisco DNA Sense by clicking the **?** icon at the top-right corner and choose **Online Documentation** from the drop-down list.

Cisco DNA Sense is not enabled by default for all the users. You should enroll and configure your Cisco SD-WAN Manager using the instructions provided in the **Online Documentation** pane. The help content from Cisco DNA Sense is displayed across all major Cisco SD-WAN Manager pages once you enroll.

If your Cisco SD-WAN Manager is already enrolled to Cisco DNA Sense, choose **Online Documentation** from the **?** drop-down.



Online Documentation

Cisco DNA Portal not enrolled

Please follow instructions below to enroll. When finished with all steps, clickhereto configure Cisco DNA Portal.

Create an Account and Subscribe to Offer in Cisco DNA Portal

1. Create an account in Cisco DNA Portal.
   - Skip to step 2 if account is already created.
   - Click 'Create a New Account', then click on 'Create a Cisco Account'.
   - Enter required details with your personal email and click 'Register'.
   - A verification email will be sent to the provided email, finish signing in by clicking on link in the verification email.
2. Login and Provide Tenant name for the account.
   - Click 'Log in with Cisco'. Enter the email used in the Step 1 and the associated password.
   - Enter tenant name for the account and click 'Continue'.
3. Subscribe to offer
   - Click 'Activate' on Cisco DNA Portal
   - In the Region drop-down list, choose US Region.
   - Check the license agreement, then click on 'Subscribe Offer'.

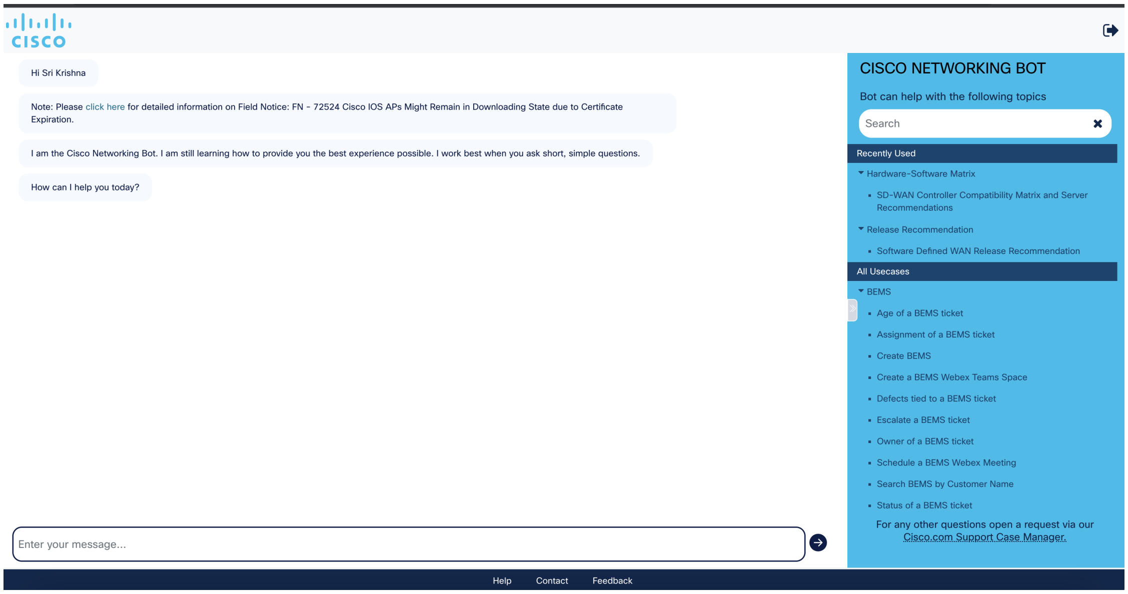
Register Cisco vManage in Cisco DNA Portal

1. Go to Cisco DNA Portal home page.
   - On the left side navigation, click on 'Applications'.
   - Click on 'On-Prem Connections' tab, click on 'Register Product'.
   - Enter IP Address, vManage instance, and choose 'Cisco SDWAN Controllers' for type.
   - Click on 'Register' to generate OTP.
2. Connect Cisco vManage to Cisco DNA Portal by providing OTP Token.
   - Go to Cisco DNA Portal via Administration→Settings.
   - Provide OTP Token, then click 'Save'.

Ask Cisco Networking Bot

To access the **Cisco Networking Bot** click the **Help(?)** icon and choose **Ask Cisco Networking** from the drop-down list.

You can use Cisco Networking Bot chat to get relevant answers to your questions.



Hi Sri Krishna

Note: Please click here for detailed information on Field Notice: FN - 72524 Cisco IOS APs Might Remain in Downloading State due to Certificate Expiration.

I am the Cisco Networking Bot. I am still learning how to provide you the best experience possible. I work best when you ask short, simple questions.

How can I help you today?

For any other questions open a request via our Cisco.com Support Case Manager.

CISCO
CISCO NETWORKING BOT
Bot can help with the following topics
Search
Recently Used
Hardware-Software Matrix
SD-WAN Controller Compatibility Matrix and Server Recommendations
Release Recommendation
Software Defined WAN Release Recommendation
All Usecases
BEMS
Age of a BEMS ticket
Assignment of a BEMS ticket
Create BEMS
Create a BEMS Webex Teams Space
Defects tied to a BEMS ticket
Escalate a BEMS ticket
Owner of a BEMS ticket
Schedule a BEMS Webex Meeting
Search BEMS by Customer Name
Status of a BEMS ticket
Enter your message...
Help
Contact
Feedback

Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for Cisco IOS XE Routers
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins
- Cisco Recommended Catalyst SD-WAN Software Versions for Controllers and WAN Edge Routers

Full Cisco Trademarks with Software License

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)