

# 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

- [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.

## 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	

Feature	Description
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.
Configure Third-party 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.
<b>Cisco Catalyst SD-WAN Security</b>	
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.
<b>Cisco Catalyst SD-WAN Cloud OnRamp</b>	
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.

Feature	Description
<a href="#">AWS Cloud WAN Integration with Dynamic Routing</a>	This feature is an enhancement to the AWS Cloud WAN integration to support site to site communication using dynamic routing.
<b>Cisco Catalyst SD-WAN AppQoE</b>	
<a href="#">SSL Proxy Support for TLS 1.3</a>	With this feature, SSL proxy in AppQoE supports the TLS protocol version 1.3.
<b>Cisco Catalyst SD-WAN Monitor and Maintain</b>	
<a href="#">Generate Admin-tech File with the Feature Filter</a>	<p>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.</p> <p>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.</p>
<a href="#">Network-Wide Path Insight Integration with Cisco Identity Services Engine</a>	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.
<a href="#">IPv6 support in Cisco SD-WAN Manager UI Troubleshooting</a>	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.
<b>Cisco Catalyst SD-WAN NAT</b>	
<a href="#">ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces</a>	<p>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.</p> <p>You can configure ICMP tracker using the <b>Tracker</b> or the <b>IPv6 Tracker</b> features under transport profile in configuration groups.</p>
<a href="#">Support to automatically configure IPv6 address on a WAN interface by using SLAAC with a Router Advertisement (RA) prefix.</a>	You can configure the Stateless Address Autoconfiguration (SLAAC) by using the RA prefix to automatically assign IPv6 addresses for NAT66 prefix translations.
<a href="#">Support for Flow Stickiness</a>	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
<a href="#">Support for Centralized data policy for NAT66 DIA.</a>	<p>You can configure the Centralized data policy by using the <code>nat use-vpn 0</code> command, which ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)</b>	
<a href="#">Specify Path Type Preference with Restrict Mode</a>	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.
<a href="#">Management Region</a>	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.
<a href="#">Configure Multi-Region Fabric and Related Features Using Configuration Groups</a>	Configure Multi-Region Fabric features, such as role, region, and so on, and configure transport gateway path behavior on routers, using configuration groups.
<b>Cisco Catalyst SD-WAN Policy Groups</b>	
<a href="#">Configure Traffic and Flow Visibility for Application Priority and SLA policy</a>	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.
<a href="#">Configure Secure Service Edge</a>	This feature supports Secure Service Edge configurations for Cisco Secure Access as provider.
<a href="#">Application Catalog</a>	<p>The <b>Application Catalog</b> 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.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN Systems and Interfaces</b>	

Feature	Description
<a href="#">Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment</a>	<p>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.</p>
<a href="#">Support for EtherChannels on the Transport Side</a>	<p>Adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN device.</p> <p>This feature also introduces support for aggregate EtherChannel Quality of Service (QoS) on the transport side.</p> <p>By combining EtherChannel and QoS, you can optimize network utilization, enhance performance, and maintain quality for specific traffic types.</p> <p><b>Note</b> This feature has limited availability.</p>
<a href="#">Co-Management: Granular Role-Based Access Control</a>	<p>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.</p> <p>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.</p>
<a href="#">IP DHCP Smart-Relay</a>	<p>This feature allows the DHCP relay agent to set the gateway address to the secondary IP address when there is no DHCP OFFER message from the DHCP server. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers.</p> <p>This functionality is useful when the DHCP server cannot be configured to use secondary pools.</p>
<a href="#">Support for Traffic Flow Collectors</a>	<p>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).</p> <p>You can configure the traffic flow collectors by navigating to <b>Configuration &gt; Network Hierarchy &gt; Collectors</b>.</p>
<p><b>Cisco Catalyst SD-WAN Segmentation Configuration Guide</b></p>	
<a href="#">Added Support for 2,000 VRFs</a>	<p>Increased support from 300 VRFs to 2,000 VRFs in the overlay network, with up to 500 for a single device.</p>
<p><b>Cisco Catalyst SD-WAN High Availability Configuration Guide</b></p>	
<a href="#">Disaster Recovery Reliability Improvements Phase 1</a>	<p>This feature removes the <b>Pause Replication</b> button from the <b>Disaster Recovery</b> screen. Replication pauses automatically when you pause disaster recovery and resumes when you resume disaster recovery.</p>

## 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 <a href="#">RMA Replacement of the Cisco ASR 1006-X Chassis</a> and <a href="#">RMA Replacement of the Cisco RP3 Module</a> 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 <a href="#">Support for SNMP Traps on Cisco Catalyst SD-WAN devices</a> 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 <a href="#">Configure SNMP using Cisco SD-WAN Manager</a> 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 <a href="#">Flexible Port Speed</a> 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 <a href="#">Cisco Catalyst SD-WAN Device Compatibility</a> page shows the supported releases for each model.

## Important Notes, Known Behaviors, and Workarounds

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

## 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
<a href="#">CSCwf71116</a>	Static route keep advertising via OMP even though there is no route.
<a href="#">CSCwf44703</a>	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
<a href="#">CSCwf45486</a>	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
<a href="#">CSCwi31833</a>	UTD deployment failing if deployed from remote server hostname rather than ip
<a href="#">CSCwi33634</a>	Cisco IOS XE Catalyst SD-WAN device is incorrectly consuming icmp reply packets.
<a href="#">CSCwi35716</a>	AAR backup preferred color not working as expected from 17.12.1
<a href="#">CSCwh84068</a>	Cisco Catalyst 8000V crashes after changing NAT HSL configuration.
<a href="#">CSCwi16716</a>	Cisco Catalyst 8500 : Router crashed upon increasing the gatekeeper cache size
<a href="#">CSCwh77221</a>	SNMP Unable to poll Cisco Catalyst SD-WAN Tunnel Data after a minute
<a href="#">CSCwi15930</a>	ASR1001-HX failing to upgrade from 17.6.3a to 17.6.5 due to CDB issue
<a href="#">CSCwi36062</a>	Cisco IOS XE Catalyst SD-WAN device - 'show isdn' and 'debug isdn' commands are missing
<a href="#">CSCwi31523</a>	After reboot EPBR does not work on C8500-12X4QC
<a href="#">CSCwi14178</a>	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed
<a href="#">CSCwh01678</a>	20.12 ISR1100 platform FTM crash with SIG enabled
<a href="#">CSCwi32883</a>	Cisco Catalyst 8500 crashes from PA Interrupt running NAT
<a href="#">CSCwi05680</a>	Cisco Catalyst 8300 Crashed generating multiple system reports
<a href="#">CSCwf69062</a>	SDRA-SSLVPN : The sslvpn session closes with re-authentication error after some interval of time
<a href="#">CSCwi31747</a>	SymNat with low bandwidth is not working
<a href="#">CSCwi00369</a>	Cisco IOS XE Catalyst SD-WAN device lost security parameter after upgrade
<a href="#">CSCwi13563</a>	IP SLA probe for End-point-tracker doesnt work once endpoint tracker is changed until reload



Identifier	Headline
<a href="#">CSCwi27400</a>	Last-resort circuit delay coming up with TLOC extension when multiple name-servers configured
<a href="#">CSCwi25476</a>	Cisco Catalyst 8500 crash with mDNS packet due to IOSXE-RP Punt Service Process
<a href="#">CSCwi05395</a>	The snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs
<a href="#">CSCwi46413</a>	Cisco IOS XE Catalyst SD-WAN device does not install OMP route with high preference using service chaning
<a href="#">CSCwi32044</a>	Device reboot due to "Critical process vip_confid_startup_sh"
<a href="#">CSCwi15688</a>	Unexpected NAT translation occurs in a specific network
<a href="#">CSCwi44633</a>	Fragmented Radius Access-Request packets are dropped when NWPI is running
<a href="#">CSCwi16015</a>	[SIT]: SSE tunnels don't come up with Dialer interface.R relax check in IKE
<a href="#">CSCwh52440</a>	IP SLA doesnt have checks for ICMP probes to be sent on source interface.
<a href="#">CSCwi46034</a>	OnDemand TLOCs installed without traffic passing through
<a href="#">CSCwi19875</a>	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

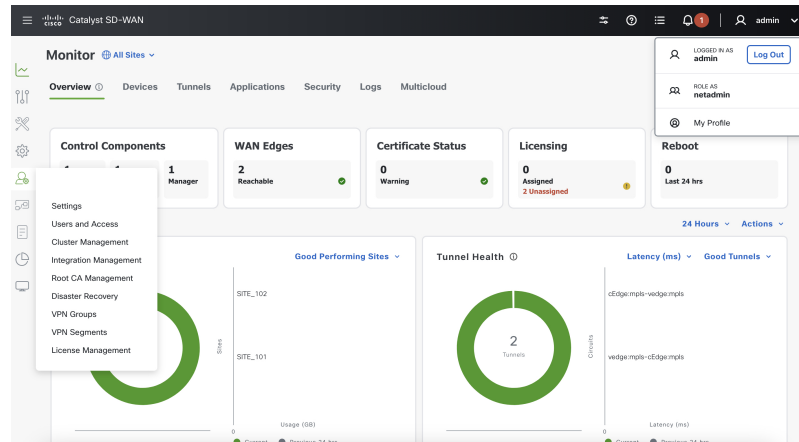
The Cisco Catalyst SD-WAN Manager Release 20.13.1 GUI is now updated, based on the Cisco design system, which enhances the look and feel of the dashboard. This upgrade offers a unified experience across various other Cisco products by maintaining consistent design and theme elements.

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.

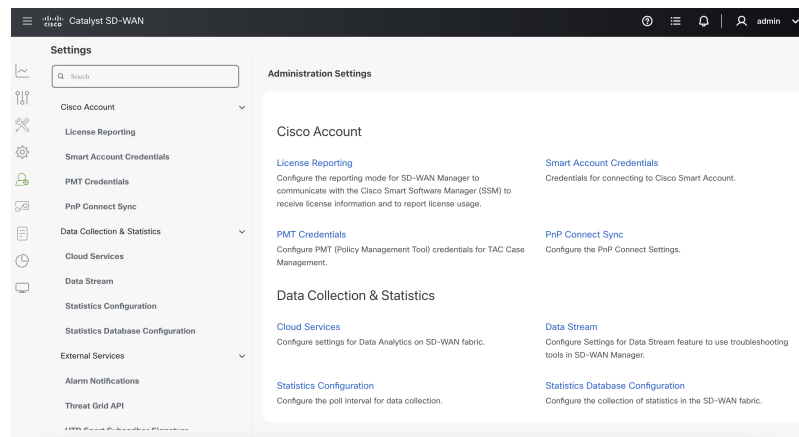
- The **Profile** drop-down menu in the top right of the dashboard includes the **My Profile** and the **Log Out** options.
- In multitenant mode, a **Select Tenant** drop-down list is available at the top-left.

**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**

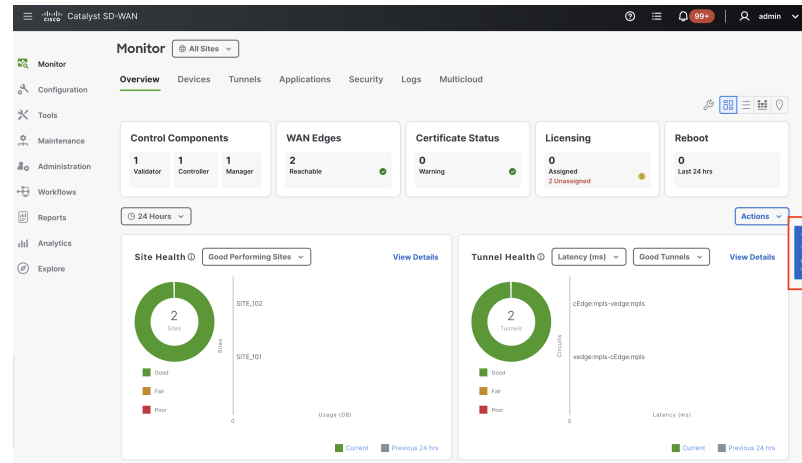
**Figure 2: New Settings Layout in the Administration Menu in Cisco Catalyst SD-WAN Manager Release 20.13.1**



## 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:

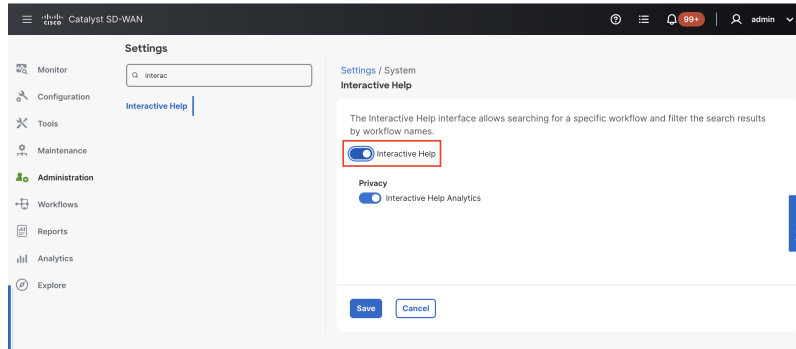
1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Navigate to the **System** menu and click **Interactive Help**.
3. Disable **Interactive Help**.



**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**

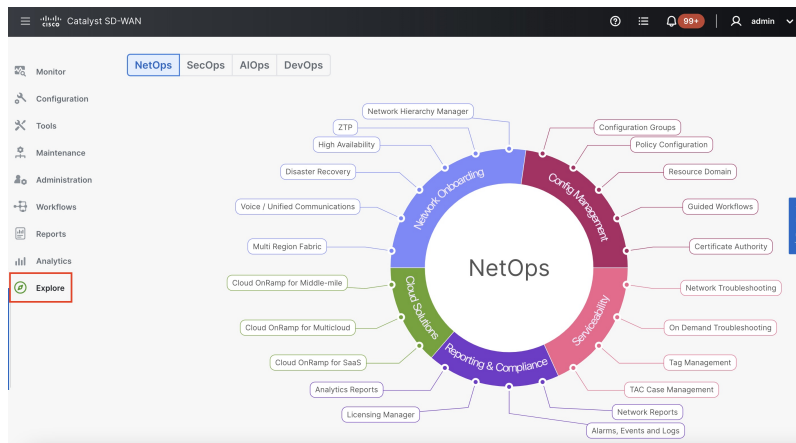


## Explore Cisco Catalyst SD-WAN Features Based on Job Roles

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**

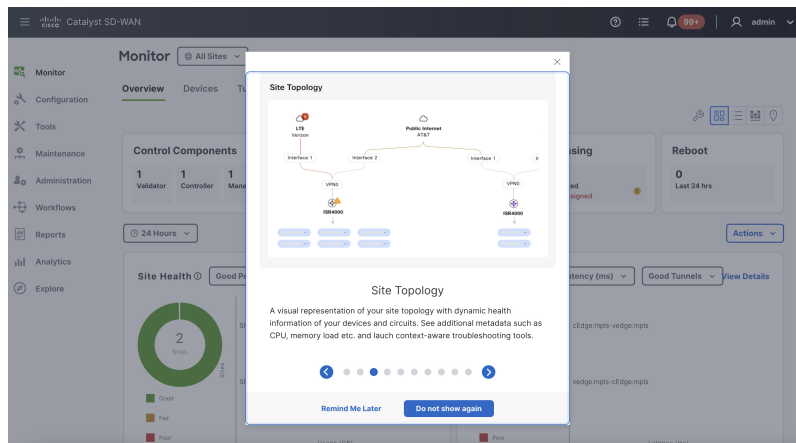


## Feature Spotlight

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**.

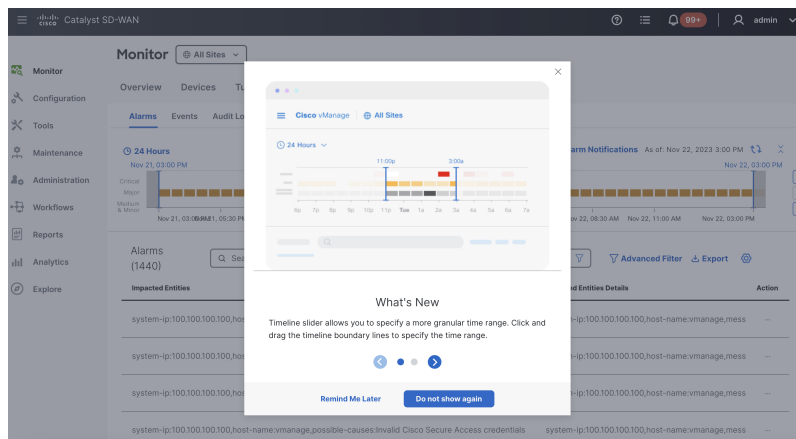
Click **Do not show again** to dismiss spotlight. This action ensures that the spotlight window doesn't appear again.

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



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**



## 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

The screenshot shows the Cisco DNA Sense interface for Catalyst SD-WAN. The main content area displays the 'Monitor Overview' page, which includes sections for Control Components (Validator, Controller, Manager), WAN Edges (Reachable), and Site Health (Good Performing Sites). A 'Help' pane is open on the right, displaying the 'Monitor Overview' help content. The help content includes sections for Applications Health, Site Health, and Tunnel Health, providing detailed information about each feature and how to use it. A 'Feedback' button is visible in the bottom right corner of the help pane.

## 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.

The screenshot shows the Cisco DNA Sense interface for Catalyst SD-WAN. The main content area displays the 'Monitor Overview' page, which includes sections for Control Components (Validator, Controller, Manager), WAN Edges (Reachable), Certificate Status (Warning), and Site Health (Good Performing Sites). An 'Online Documentation' pane is open on the right, displaying instructions for enrolling and configuring Cisco DNA Sense. The pane includes a 'Cisco DNA Portal not enrolled' message and a list of steps to follow for enrollment. A 'Feedback' button is visible in the bottom right corner of the help pane.

## 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.

The screenshot displays the Cisco Networking Bot chat interface. On the left, the chat history includes a greeting "Hi Sri Krishna", a note about a field notice (FN - 72524 Cisco IOS APs Might Remain in Downloading State due to Certificate Expiration), and a self-introduction: "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." Below this is a prompt "How can I help you today?". At the bottom, there is a text input field labeled "Enter your message...". On the right side, a sidebar titled "CISCO NETWORKING BOT" contains a search bar and two sections: "Recently Used" and "All Usecases". The "All Usecases" section lists various topics such as "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", and "Status of a BEMS ticket". At the bottom of the sidebar, it says "For any other questions open a request via our Cisco.com Support Case Manager." At the very bottom of the chat window, there are links for "Help", "Contact", and "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](#)

## 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](http://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)



---

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](http://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)

© 2023 Cisco Systems, Inc. All rights reserved.