Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.11.x

First Published: 2023-04-06

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 17.11.1a

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 17.11.1a, 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 SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.11.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

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

Cisco is constantly enhancing the 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 17.11.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	
Support for Specifying Any Organization for WAN Edge Cloud Device Enterprise Certificates	When configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in the **Organization** field. You are not limited to organization names such as **Cisco Systems**. This feature enables you to use your organization's certificate authority name or a third-party certificate authority name.

Feature	Description
SMU Support for Cisco ISR1100 and ISR1100X Series Routers	Added SMU support for Cisco ISR1100 and ISR1100X Series Routers.
Cisco Catalyst SD-WAN Systems and Interfaces	
Cisco Catalyst SD-WAN Remote Access Configuration	This feature enables you to configure a remote access feature in system profile of the configuration groups. You can configure the following remote access parameters in system profile–Private IP Pool, Authentication, AAA Policy, IKEv2 Setting, and IPSec Settings.
Device Variable Option	This feature enables you to read or write variables from the Associate Devices page while deploying the devices.
Configuration Groups and Feature Profiles	The following new features are introduced to the Configuration Groups and Feature Profiles–Cisco Security in System Profile, IPV4-Device-Access-Policy in System Profile, IPV6-Device-Access-Policy in System Profile, OSPF Routing in Transport Profile, VPN Interface GRE in Transport Profile, IPSEC in Transport Profile, Tracker Group in Transport Profile, GPS in Transport Profile, IPSEC in Service Profile, Tracker in Service Profile, Tracker Group in Service Profile, UCSE in Other Profile, AppQoE in Other Profile, Remote Access feature in System Profile.
Support for Software Defined Remote Access Pools	Remote access refers to enabling secure access to an organization's network from devices at remote locations. The resource pool manager manages the IPv4 and IPv6 private IP address pools for Cisco Catalyst SD-WAN remote access devices. You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page.
TLOC Extension Over IPv6	This feature enables the support of TLOC extension for IPv6.
GRE-in-UDP	This feature enables you to configure GRE-in-UDP tunnel.
Assigning Roles Locally to a User Defined by an Identity Provider for SAML SSO	If you are using an identity provider, such as Okta, for security assertion markup language (SAML)-based single sign-on (SSO), then you can define user roles through the identity provider. This feature enables you to assign user groups locally in Cisco SD-WAN Manager, when no roles are defined for the user by the identity provider.
Cisco Catalyst SD-WAN Policies	
Log Action for both Localized and Centralized Data Policies	With this feature, you can set log action parameter for data policy, application route policy and localized policy while configuring data policies on Cisco IOS XE Catalyst SD-WAN devices. The log parameter allows packets to get logged and generate syslog messages. Logs are exported to external syslog every five mins when flow is active. Logs are exported to external syslog server only when one is configured in the system, or else only console logging is done. Policy logs further can be controlled as per the configured rate. A new command **policy log-rate-limit** is introduced to support this feature.

Feature	Description
QoS for Router Generated Cisco SD-WAN Manager Traffic	This feature helps you to prioritize or queue router-generated Cisco SD-WAN Manager traffic based on your specific requirements. Achieve routing vManage traffic through a queue of your choice using QoS policies and configuring class maps.
Cisco Catalyst SD-WAN Security	
IPv6 Support for Zone-based Firewall	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.
Security Logging Enhancements	This feature allows you to configure up to four destination servers to export the logs, and an option to specify a source interface for high-speed logging (HSL). The IP addresses for the destination servers can be IPv4, IPv6, or both.
Security Logging Enhancements	This feature enhances the capability of UTD logging in a unified security policy. When you configure UTD logging for exporting the UTD logs to an external syslog server, you can now specify the source interface from where the UTD syslog originate from.
Cisco Umbrella Multi-Org Support	This feature supports management of multiple organizations through a single parent organization. With this feature, Cisco Catalyst SD-WAN and umbrella for SIG supports different security policy requirements for different regions of the Cisco Catalyst SD-WAN network.
Cisco Catalyst SD-WAN Cloud OnRamp	
Support for Multiple Virtual Hubs per Region	You can create multiple virtual hubs in a single Azure region.
Audit Management	The audit management feature helps in understanding if the interconnect cloud and provider connection states are in sync with the Cisco SD-WAN Manager connection state. The State refers to the various connection statuses that Cisco SD-WAN Manager establishes with cloud services and providers. The audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud.
Cisco Catalyst SD-WAN Monitor and Maintain	
Security Dashboard Enhancements	This features introduces enhancements to the security dashboard in Cisco SD-WAN Manager. The security dashboard introduces a drop-down list **Actions** that enables you to edit the security dashboard and reset the security dashboard to the default view when you have modified the security dashboard, view the **SecureX** ribbon once it is configured. Additionally, you can access the Cisco Talos portal from Cisco SD-WAN Manager. A hyperlink of the Cisco Talos portal is added to the security dashboard.
SCM Integration Improvements	With this feature, you can access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco SD-WAN Manager without having to go to a different Case Manager portal.

Feature	Description
Grouping of Alarms	Alarms are filtered and grouped for devices and sites based on severity. View alarm details for a single site in the **Overview** dashboard. View alarms for a particular device by clicking the … icon in the **Monitor** > **Devices** window. View the top five alarms for a particular site in the **Monitor** > **Overview** window by choosing the **Site Topology** view icon and clicking the site. The **Related Event** column is added to the alarms filter.
Grouping of Events	Events are filtered and grouped based on severity for devices and sites. View events for a particular device by clicking the … icon in the **Monitor** > **Devices** window. View the top five events for a particular site in the **Monitor** > **Overview** window by choosing the **Site Topology** view icon and clicking the site.
Automatically Determine File Attributes for a Remote Virtual Image File	When you specify a remote virtual image file, Cisco SD-WAN Manager can extract the necessary image file attributes from the filename.
Unified Debug Condition To Match IPv4/IPv6 Over MPLS	This feature introduces a debug condition to identify and resolve issues related to matching IPv4/IPv6 traffic over an MPLS network.
Packet Trace Improvements	This feature offers the following enhancements to packet trace: • A new command **how platform packet-trace fia-statistics**, available on Cisco IOS XE Catalyst SD-WAN devices, displays Feature Invocation Array (FIA) statistics in a packet trace. In FIA statistics, you can find data about a feature's count, the average processing time, the minimum processing time, and the maximum processing time. • View label information for the Multiprotocol Label Switching (MPLS) feature in packet trace.
Download Output of OMP Routes	You can download the output of the OMP Received Routes or OMP Advertised Routes real time commands on Cisco IOS XE Catalyst SD-WAN device.
Cisco Catalyst SD-WAN SNMP	
Application Route SNMP Trap	Cisco IOS XE Catalyst SD-WAN device support the **AppRouteSlaChange** SNMP trap which is generated when a change in SLA class is detected.
Cisco Catalyst SD-WAN NAT	
Destination NAT Support	This feature changes the destination address of packets passing through WAN edge devices. Destination NAT is used to redirect traffic destined to a private address to the translated destination public IP address.

Feature	Description
Port Forwarding with NAT DIA Using a Loopback Interface	This feature supports port forwarding with NAT DIA by using a loopback interface. You can configure a loopback interface by either using device CLI templates or CLI add-on feature templates.
ALG Support Enhancement for NAT DIA and Zone-Based Firewalls	The ALG support for NAT DIA is extended for the following protocols–Trivial File Transfer Protocol (TFTP), Point-to-Point Tunneling Protocol (PPTP), Sun Remote Procedure Call (SUNRPC), Skinny Client Control Protocol (SCCP), H.323.
Support for IPv6 DIA Tracker	NAT DIA tracker is now supported on IPv6 interfaces. You can configure IPv6 DIA tracker using the **IPV6-Tracker** and **IPV6-Tracker Group** options under transport profile in configuration groups.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Support for Affinity Groups for Service Routes and TLOC Routes	This feature extends support affinity group assignments to service routes and TLOC routes. A common use case is to add further control to routing by using affinity group preference together with control policies that match service routes and TLOC routes.
Set Affinity Group by Control Policy	You can configure a control policy to match specific TLOCs or routes and assign them an affinity group value, overriding the affinity group that they inherit from the router.
Route Aggregation on Border Routers and Transport Gateways	With this feature, you can configure route aggregation on border routers and transport gateways in a Multi-Region Fabric network environment. For a border router, you can optionally specify whether the route aggregation operates only for the router's core region or access region.
Cisco Catalyst SD-WAN Routing	
Support for MSDP to Interconnect Cisco Catalyst SD-WAN and Non-SD-WAN	This feature enables Multicast Source Discovery Protocol (MSDP) interoperability between Cisco IOS XE Catalyst SD-WAN devices in Cisco Catalyst SD-WAN and the devices in a non-SD-WAN setup.
Cisco SD-WAN Controller Route Filtering by TLOC Color	Cisco SD-WAN Controller can reduce the number of routes that they advertise to routers in the network, to exclude routes that are not relevant to a particular device. The filtering to reduce the number of routes is based on the colors of TLOCs on each device. For example, a route to a public TLOC is not relevant to a router that only has private TLOCs. Advertising fewer routes helps to avoid reaching the send path limit for routers in the network.
Cisco Catalyst SD-WAN Bridging	
Layer 2 and Layer 3 Flex Port Support	Cisco SD-WAN Manager provides flex support on Layer 2 switchports on Cisco IOS XE Catalyst SD-WAN devices, allowing flexibility for LAN ports at Layer 2 to be converted to Layer 3 ports. You can configure the flex ports on Layer 2 as Layer 3 ports using feature profiles and CLI add-on profile.

Feature	Description
Cisco Catalyst SD-WAN AppQoE	
UCS-E Series Next Generation Support for Deploying Cisco Catalyst 8000V	With this feature, you can deploy Cisco Catalyst 8000V instances, on supported routers, using the UCS-E series blade server modules. With this feature, the UCS-E1100D-M6 server module is supported.
Cisco Catalyst SD-WAN Commands	
show tech-support sdwan bfd	This feature adds support for displaying BFD information on Cisco IOS XE Catalyst SD-WAN devices.

New and Enhanced Hardware Features

New Features

- Support for Cisco SM-X-1T3/E3 Module: Cisco SD-WAN Manager CLI device templates now supports Cisco SM-X-1T3/E3 module.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Table 2: Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Behavior Change	Description
To avoid flapping of tracker and tunnels, a interval duration added between the tunnel status. When tunnel status change continuously within a short period of time, tunnel goes to the flapping state. To prevent tunnels flap, an interval multiplier is configured on the tracker configuration.	Updated the Tracker Parameters section with a note for Multiplier field.
When the Cisco Catalyst SD-WAN sessions with QoS policy reaches the maximum limit, QoS policy will not be applied for the new SD-WAN sessions.	Updated the Overview of Per-Tunnel QoS section with the note on Per-Tunnel QoS scale parameter to configure maximum Cisco Catalyst SD-WAN sessions.
DH groups are used in IKE to establish session keys. As part of security hardening and deprecation of weak ciphers, the option to configure Diffie-Hellman groups (DH) groups 1, 2, and 5 are removed and these are not supported.	Updated the Configure IPsec Tunnel Parameters section with the note on supported DH groups.
SNMP v3 users with SHA-256 and AES-256 authentication must use 1161 as special port.	Updated the note on using special port in Configure SNMPv3 section.

Behavior Change	Description
In a multi-tenant scenario, when configuring controller certificate authorization (**Administration** > **Settings** > **Controller Certificate Authorization**), if you configure certificate signing request (CSR) properties manually, some new conditions apply.	Updated the note in the Authorize a Controller Certificate for an Enterprise Root Certificate section.
In Cisco vManage, access the **Cisco Networking Bot** by clicking the **?** icon at the top-right corner of a page and choose **Ask Cisco Networking** from the drop-down list.	You can use Cisco Networking Bot chat to get relevant answers to your questions. A topic in the Cisco IOS XE Catalyst SD-WAN Release Notes 17.11.x covers the details of the CNB.
In Cisco vManage, while configuring devices, you can switch between the **vManage** and **CLI** modes at a device level.	Notes are added to the Change Configuration Modes topic with steps that describe how to switch between the vManage mode and CLI mode.
Alarms display the hostname as **localhost** during the cluster setup until the hostname is configured in Cisco vManage.	Updated the Configure the Cluster IP Addresssection with a note on default hostname.
New commands are added to display data policy that a Cisco SD-WAN Controller has pushed to the devices and the tags downloaded from the Cisco SD-WAN Controller.	Following new commands are added: • show sdwan from-vsmart policy • show sdwan from-vsmart tag-instances is added.
Cisco vManage Release 20.11.1 does not support the QoS map feature in the transport profile and the service profile.	Before upgrading to Cisco vManage Release 20.11.1, ensure that you delete the QoS map feature from the transport profile or the service profile if you have already configured it. For the procedure to delete the QoS map, see: • QoS Map in the Transport and Management profile. • QoS Map in the Service profile.
New debug and show commands are added to Cisco Cloud OnRamp for SaaS.	35 new debug and show commands are added to Debug and Show Commands section.

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.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.11.x

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Identifier	Headline
CSCwd47940	Cisco IOS XE Catalyst SD-WAN devices: PMTU Discovery is not working after interface flap
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity
CSCwc79115	Cisco IOS XE Catalyst SD-WAN devices Policy commit failure Notification and Alarm from Cisco SD-WAN Controller
CSCwe00946	Cisco Catalyst SD-WAN | System crash after disabling endpoint-tracker on tunnel interfaces
CSCwd67198	17.10: uCode crash seen on Curie 2RU after stopping NWPI trace
CSCwe28204	c8500L: Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwd89012	Tested flap-based auto-suspension - Minimum duration value - no results as expected
CSCwe29430	[SIT] ISR4221X/K9 : Critical process fpmd fault on rp_0_0 (rc=134)
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwd41236	On C8200-1N-4T, sh version points to /harddisk/core dir, but file is present in /bootflash/core dir
CSCwd44439	ASR and c8500 crashing at fman_sdwan_nh_indirect_delete_from_hash_table
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwc72588	Router should not allow weak cryptographic algorithms to be configured for IPsec
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwd65945	[SIT]: LR Interface which has NAT enabled is chosen for webex traffic
CSCwe27241	nbar classification error with custom app-aware routing policy
CSCwc37465	unable to push "no-alias" option on static NAT mapping from Management system
CSCwd49309	17.10: ucode crash seen on Thorium with traffic pointing to segfault in coff handler
CSCwd44006	Control Connection on Cisco IOS XE Catalyst SD-WAN devices doesn't come-up with reverse proxy using Enterprise Certificate
CSCwe18058	Unexpected reload with IPS configured on 17.6.3a
CSCwd67654	[SIT]: In ISR4461 ,fnf stats are getting populated with unknown in egress/ingress interface in vpn0

Identifier	Headline
CSCwb59113	Cisco Catalyst SD-WAN control and bfd session gets nat translated with static ip over Dialer interface
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
CSCwc42978	ISR1100-4G looses all BFD sessions with Invalid SPI
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwc48427	[SITLite] BFD issues with clear_omp -> non-PWK + non-VRRP scenario only
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Identifier	Headline
CSCwd42523	Same label is assigned to different VRFs
CSCwd45508	Cisco IOS XE Catalyst SD-WAN devices does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwe39157	During Soak Run, On C8500L-8S4X, Memif channel's were missing and causing SC-SN state down
CSCwe43341	TLS control-connections down, traffic from controller dropped with SdwanImplicitAclDrop
CSCwe18276	17.6: Route-map not getting effect when its applied in OMP for BGP routes
CSCwe35574	DPDK RX buffer is getting corrupted on both Radium and Fugazi and causing crash
CSCwd97769	Encryption supported still shows AES_256_CBC in security info of Cisco IOS XE Catalyst SD-WAN devices
CSCwe49684	Cisco Catalyst SD-WAN BFD sessions keeps flapping intermittently
CSCwe45169	Data collection from Cisco IOS XE Catalyst SD-WAN devices failing due to netconf rpc-reply timeout
CSCwb39206	Enable VFR CLI in sdwan mode

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 SD-WAN Manager GUI Changes

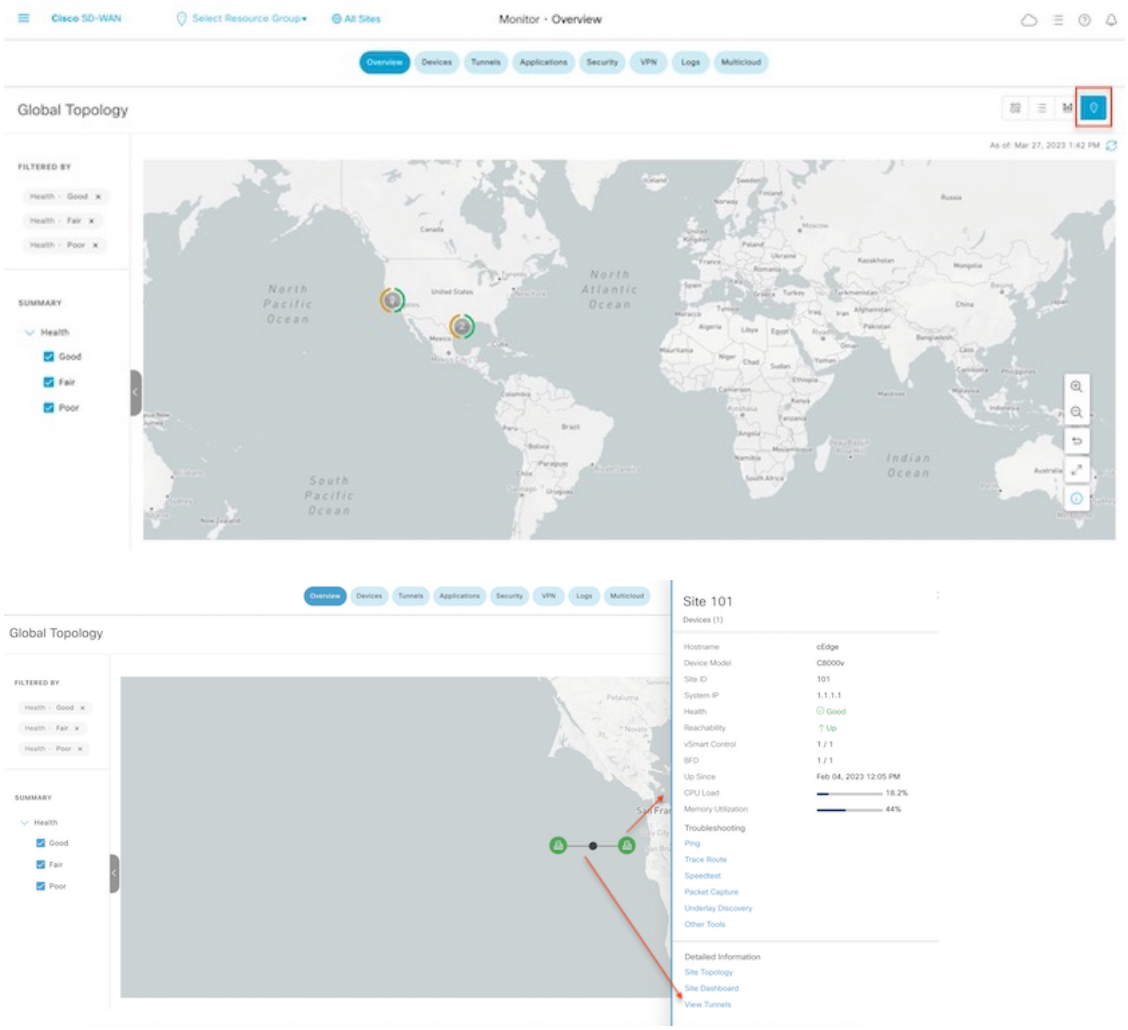
This section presents a comparative summary of the significant GUI changes between Cisco vManage 20.10.x and Cisco vManage Release 20.11.1.

Monitor Overview Page

In Cisco vManage Release 20.11.1, the following GUI changes have been made to the **Monitor** > **Overview** page. For more information about the **Monitor** > **Overview** page, see Cisco SD-WAN Manager Monitor Overview.

- The global topology view has been added to the page.

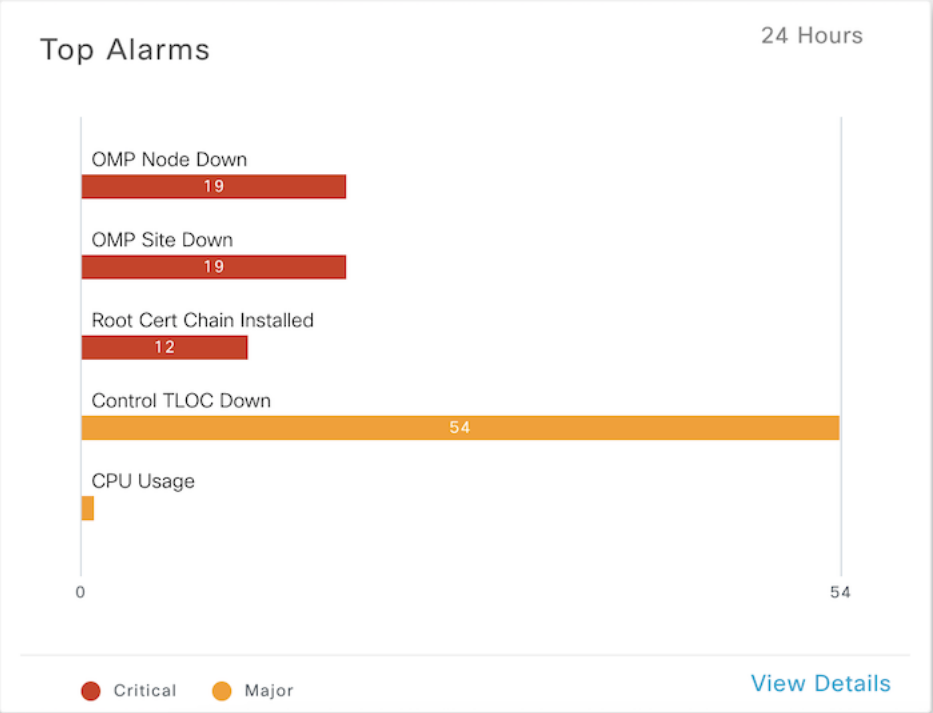
Figure 1: Global Topology View of the Monitor Overview Page in Cisco SD-WAN Manager 20.11.1



- New dashlets, **WAN Edge Management** in all sites and **Top Alarms** in single site have been added.

Figure 2: New Dashlet WAN Edge Management in the Monitor Overview Page in Cisco SD-WAN Manager 20.11.1

Figure 3: New Dashlet Top Alarms in the Single Site Monitor Overview Page in Cisco SD-WAN Manager 20.11.1



On-Demand Troubleshooting

In Cisco vManage Release 20.11.1, on-demand troubleshooting progress has been added to the page.

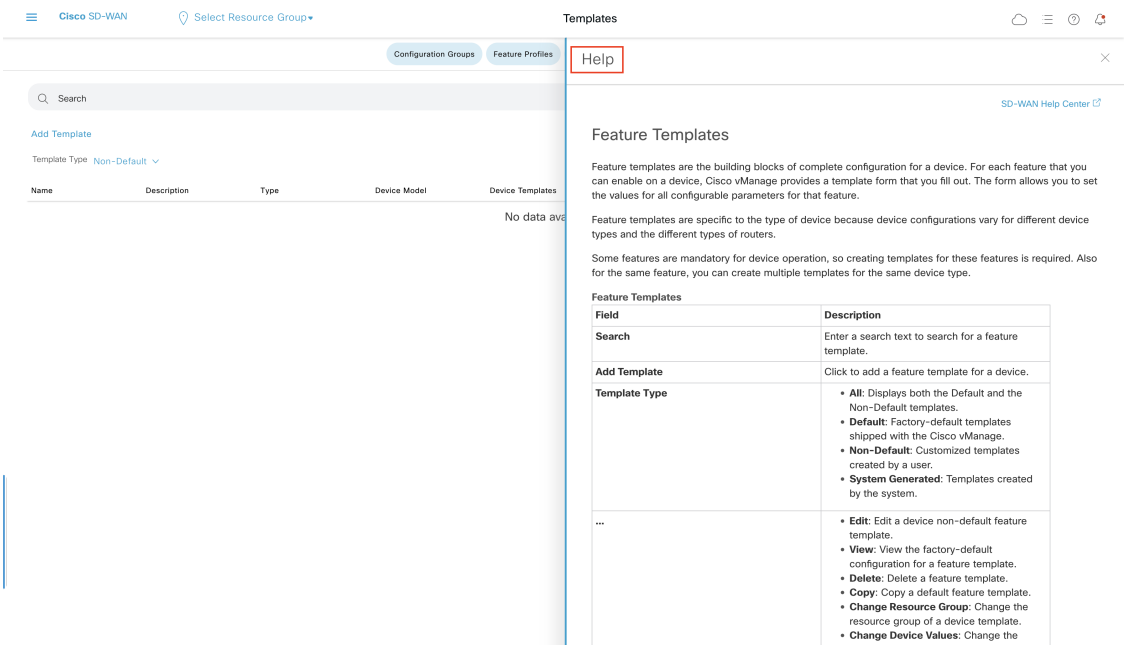
Figure 4: Enhance On-Demand Troubleshooting Processing Time in Cisco SD-WAN Manager 20.11.1

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.

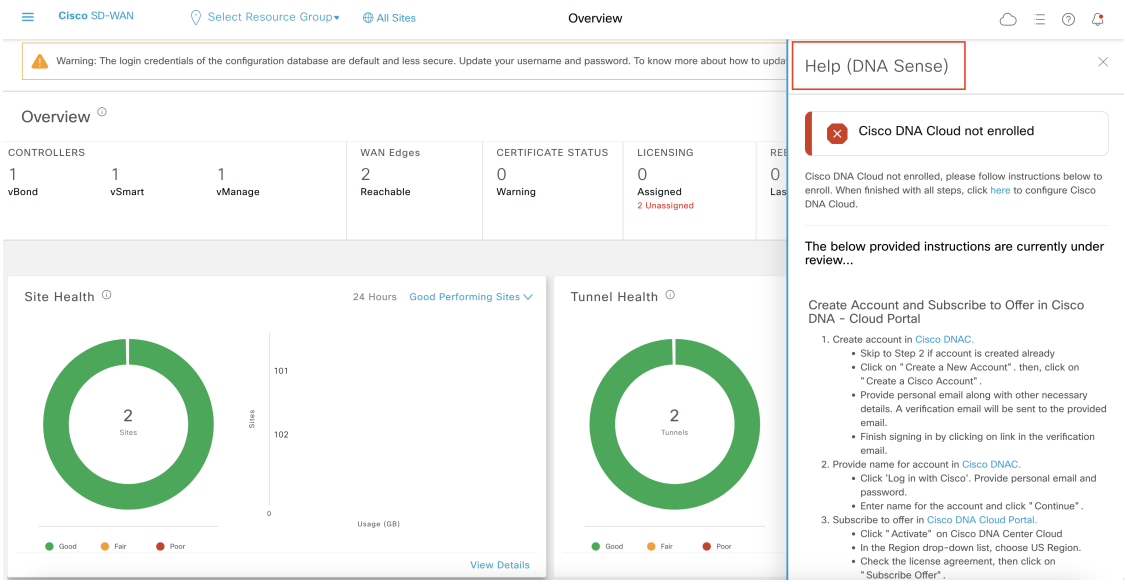
Figure 5: Help Content in a Slide-in Pane



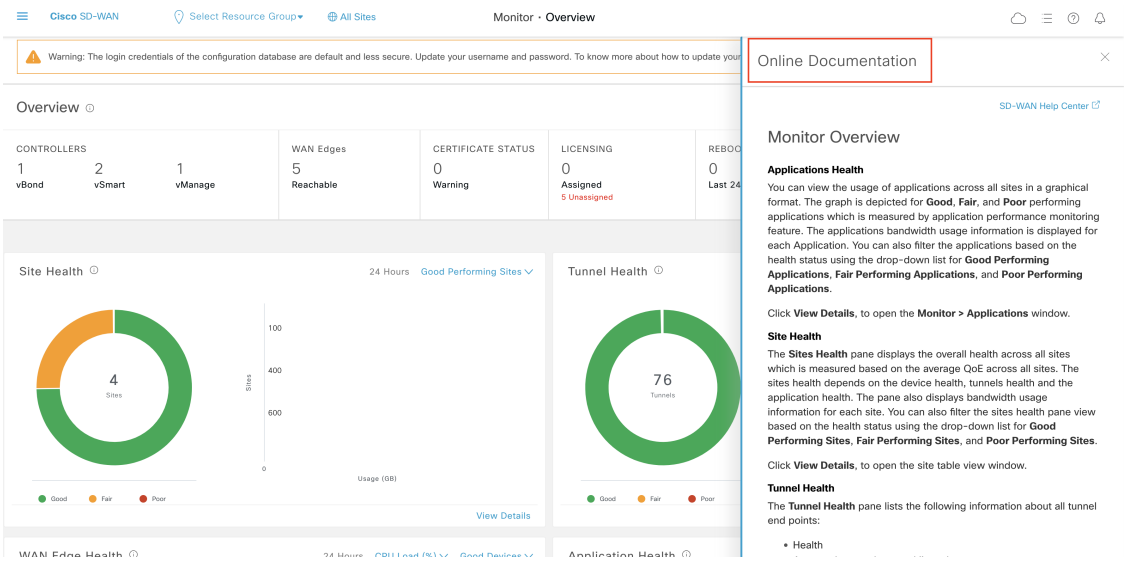
Cisco DNA Sense

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 **Help (DNA Sense)** 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 **Help (DNA Sense)** 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.



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.

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

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)