Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.14.x

First Published: 2024-04-30

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 17.14.1a

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 17.14.1a, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco Catalyst 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 20.14.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

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 17.14.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
New Procedure for Enabling Cisco SD-AVC Cloud Connector	This release introduces a new procedure for enabling Cisco SD-AVC Cloud Connector from the Cloud Services option in **Administration** > **Settings**. From this release, enabling Cloud Connector does not require an OTP or opening a TAC case.

Feature	Description
Cisco SD-WAN Manager Cluster Upgrade Compatibility Check	This feature helps to upgrade Cisco SD-WAN Manager cluster and ensures that all the software devices are running on same version and are compatible. Using this feature, you can check pre-upgrade and post-upgrade checks to verify node health and identify the cause for inconsistent failures.
License Compliance Messaging	Cisco SD-WAN Manager actively monitors the compliance status of Cisco Catalyst SD-WAN licenses to identify issues with license synchronization, device assignments, or expired licenses. In case of an issue, it displays a compliance error message. In addition, on the **License Management** page, the device list indicates the license compliance status of each device.
Release a License from a Device	You can manually release a license from a device without having to remove or decommission the device. This leaves the license available to use with other devices.
Multitenant License Management	In a multitenant scenario, Cisco SD-WAN Manager supports license management at the provider level for multitenant edge devices. In Cisco SD-WAN Manager, in Provider mode, assign a base license and tenant licenses for multitenant edge devices.
Cisco Catalyst SD-WAN Security	
Match Traffic Using Custom Applications	Added support for matching traffic using a custom application in a custom-defined application list.
IPv6 Support for UTD policies	This feature adds IPv6 support for UTD security features and Unified Logging. IPv6 support for UTD security feature includes configuration and inspection of IPv6 traffic, IPS, URL filtering, and AMP. The feature also adds IPv6 support for operational command related to UTD.
SLA Profile support for Layer 7 Health Check	This feature uses jitter and packet loss, in addition to latency in SLA metrics to determine the health of the tunnel.
Zscaler Integration	This feature adds Zscaler integration with Cisco Catalyst SD-WAN as a Security Service Edge (SSE) solution. You can provision both IPSec and GRE tunnels to Zscaler using policy groups in Cisco SD-WAN Manager.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices over a transport VPN	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a transport VPN.
Cisco Catalyst SD-WAN Cloud OnRamp	
Configure Devices for AWS Integration Using Configuration Groups	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices for AWS integration.

Feature	Description
Configure Devices for Azure for US Government Using Configuration Groups	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure for US Government.
Pay As You Go and IP-Transit License Management for Megaport	This feature introduces support for Pay As You Go (PAYG) licenses for Megaport. The PAYG model is a usage-based model which allows users to pay based on how much they consume. For example, a cloud storage service provider could charge based on the amount of storage used.
Cisco Catalyst SD-WAN AppQoE	
IPv6 Protocol support for AppQoE Services	This feature allows AppQoE clusters to handle both IPv4 and IPv6 traffic.
DRE Optimization Using Configuration Groups	With this feature you can enable DRE optimization using **AppQoE** feature under **Service Profile** in a configuration group in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Monitor and Maintain	
Cellular Modem Firmware Upgrade	Cisco SD-WAN Manager supports upgrading the cellular modem firmware of devices that include a cellular modem.
Protocol Pack Management and Compliance	Cisco SD-WAN Manager management of Protocol Packs includes upgrading Protocol Pack releases on routers in the network and flagging the status of routers using an older Protocol Pack release than the current reference release. Cisco SD-WAN Manager uses the latest Protocol Pack release that it has available as a reference for comparing against the Protocol Packs loaded on devices in the network.
Export and Import Cisco Catalyst SD-WAN Configurations	Export and import configuration groups, policy groups and toplogies from your Cisco SD-WAN Manager as .tar.gz files to your local storage and customize your deployments.
Cisco Catalyst SD-WAN System and Interfaces	
L2VPN Support on Cisco Catalyst SDWAN Overlay	The feature adds Layer 2 VPN support on the Cisco Catalyst SD-WAN overlay network. It allows you to configure Layer 2 point-to-point and point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.
Support for Load Balancing for EtherChannels on the Transport Side	This feature adds the ability to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices using the **port-channel load-balance-hash-algo sdwan** command.
Cisco Catalyst SD-WAN Rugged Series Router Configuration Guide	

Feature	Description
Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers	Configure and manage the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Series Routers using Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN NAT	
Support for configuring multiple NAT types	This feature supports configuration of multiple NAT types - interface, loopback interface, or NAT pool for Direct Internet Access (DIA). Use the centralized data policy to assign rules for combining various NAT types for DIA traffic egressing the Edge router. You can also bypass NAT altogether.
Support for redistribution of NAT66 DIA routes	You can configure the redistribution of NAT66 DIA routes into BGP or OSPFv3 protocols.
Support for NAT66 DIA status event.	You can monitor the NAT DIA status in the Cisco SD-WAN Manager logs. A new event called **nat-update** displays the status of NAT DIA in the **Events** screen.
Support for Point-to-Point Protocol (PPP) Dialer Interfaces with NAT66 DIA	This feature adds support for two types of PPP dialer interfaces—PPP over Ethernet (PPPoE) and PPP over Asynchronous Transfer Mode (PPPoA). With this feature, you can configure PPP dialer interfaces for accessing IPv6 services and sites.
Cisco Catalyst SD-WAN Remote Access	
Monitor Cisco Catalyst SD-WAN Remote Access using Cisco SD-WAN Manager	The feature enhances the monitoring of remote access devices. Cisco SD-WAN Manager can provide the following information: Number of remote access (RA) headends in the network and the supported RA mode (IPsec/SSLVPN). Number of remote access sessions in the network and sessions per remote access headend categorized into remote access client type.
Policies	
Service Chaining Trusted and Untrusted Traffic	This feature lets you configure trusted traffic to flow to a trusted high availability pair in a service chain.
Configure a Maximum FNF Record Rate for Aggregated Traffic Data	For a device, you can configure a maximum rate (records per minute) for sending Flexible NetFlow (FNF) records of aggregated traffic data. This can reduce the performance demands on a device, and may be helpful when there is a large number of applications producing network traffic.
Policy Groups	

Feature	Description
Policy Compliance	This feature checks whether existing application-aware policies use applications that have been updated in a later Protocol Pack, and assists you in updating policies to use the latest available applications. The compliance-check uses the Protocol Pack currently loaded in Cisco SD-WAN Manager as a reference.
Cisco Catalyst SD-WAN Configuration Groups	
Support for Additional OK Communications Features	This feature adds support for the Unified Voice configuration features in the UC voice profile.
Network-Wide Path Insight	
Network-Wide Path Insight Integration with Cisco ThousandEyes	With this feature, network-wide path insight presents test results from a Cisco ThousandEyes Enterprise Agent and includes this information in flow results for your review and analysis.
Qualified Command Reference	
Event Commands	The EEM configurations such as else, break, continue, elseif, while, set, increment, handle-error, gets, foreach, divide, decrement, counter, and append are supported.

New and Enhanced Hardware Features

New Features

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Behavior Change	Description
The SLA class components such as loss, latency and jitter values are modified.	The Application Priority and SLA section describes the new SLA class component values.
The **request platform software sdwan software activate** is updated with supported options.	The request platform software sdwan software activate command is updated.
In an environment that mixes Cloud OnRamp for SaaS without SIG tunnels and Cloud OnRamp for SaaS over SIG tunnels, telemetry is supported for sites using Cloud OnRamp for SaaS without SIG.	The Restrictions for Cloud OnRamp for SaaS Over SIG Tunnels section describes the details.

Behavior Change	Description
From Cisco SD-WAN Manager, the auto correct option is not available. Instead, display the cloud services audit as follows: From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**, then in the **Intent Management** pane, click **Audit**. Select the cloud provider. Cisco SD-WAN Manager shows the audit report.	The Audit Discrepancies and Resolutions table provides more details.
Advertisement of NAT64 routes through OMP is supported through Cisco IOS XE Catalyst SD-WAN Release 17.12.x.	The Advertise NAT64 Routes Through OMP section is updated.
When a Cisco SD-WAN Controller or Cisco SD-WAN Validator upgrade is in progress, upgrade of tenant edge devices is not supported.	The Restrictions for Cisco Catalyst SD-WAN Multitenancy section describes the details.
AppQoE clusters can handle both IPv4 and IPv6 traffic for TCP and DRE optimization.	The Create a Centralized Policy for TCP and DRE Optimization section describes the details.
In Cisco SD-WAN Manager, the **Data Collection** tab has been removed from **Administration** > **Settings** and integrated into **Network Statistics Configuration and Collection**, and a new tab **Terms & Conditions** now has these two toggle options for collecting telemetry data, **SD-WAN Telemetry Basic** and **SD-WAN Telemetry Advanced**.	The Data Collection and Cisco Catalyst SD-WAN Telemetry section describes the details.

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.
- Prior to Cisco IOS XE Catalyst SD-WAN Release 17.14.1 release, the BFD session on Private TLOC flaps when there is a change in Public IP or port due to transit NAT device. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1 onwards, the BFD session on Private TLOC is not affected by the change in Public IP or port.

Resolved and Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.14.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 17.14.1a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Identifier	Headline
CSCwh94906	9800 WLC segmentation fault crash with Network Mobility Services Protocol (nmsp).
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwi49846	ftmd crashed when SIG GRE tunnels configurations are removed.
CSCwi98537	SIP registered ports 1/0/128 onwards have duplicate MAC addresses for VG420-144FXS SKU
CSCwi55725	SDR CLI config group issue.
CSCwi61369	Cisco IOS XE Catalyst SD-WAN device may unexpectedly reload due to SIGABRT.
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot.
CSCwi35716	AAR backup preferred color is not working as expected from 17.12.1
CSCwi76516	The Managed Cellular Activation solution configuration tamplate deployemt fails.
CSCwj14121	The snmpwalk for OID ifOperStatus gives different output before & after upgrade for serial interface.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwi31110	Traceback seen @_nhrp_cache_delete due to negative global cache count.
CSCwf84567	Unexpected reload after re-connecting to the Cisco SD-WAN Controller.
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed
CSCwi82405	The mGRE Tunnels with shared ipsec profile cause ucode crash.
CSCwi40603	Memory leak in the Crypto IKMP process.
CSCwh36635	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a : Cisco Catalyst 8300 RU : confd / SMP crash.
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many ipsec interfaces.
CSCwi53549	Cisco IOS XE Catalyst SD-WAN device router crash with reason "Critical process fman_fp_image fault on fp_0_0 (rc=134)"
CSCwi60266	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade.

Identifier	Headline
CSCwi67983	Cisco IOS XE Catalyst SD-WAN device / Tracker state log is missing when DNS Query fails.
CSCwh37024	IR1800 PnP gets stuck when Verizon cellular backhaul is used.
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version.
CSCwi66850	C-SM-16P4M2X stuck in Bootloop when "platform urpf" command issued.
CSCwf08658	Edge devices will flap the BFD sessions if we are in a non equilibrium state and have symmetric NAT.
CSCwi82548	Crash in IKEv2 Cluster Load Balancer.
CSCwi51381	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
CSCwi89822	Unexpected reboot due cpp ucode on a Cisco Catalyst 8000 Edge Platforms router.
CSCwh09033	Router unable to boot with C-NIM-8T module.
CSCwf00276	Packets with L2TP headers cause ASR1k to crash.
CSCwh91136	Cisco IOS XE Catalyst SD-WAN device: Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwh16595	Flex: Peer failed to up after shut/noshut L2 port with SFP inserted and switchport mode configured.
CSCwi78365	Trim installed certificate on upgrade.
CSCwi47322	CG113 Syslog Logging not happening on remote server.
CSCwi85293	IKEv2 IPv6 Cluster Load balance: Secondary in cluster unable to connect to cluster in case of FVRF
CSCwi86698	No error msg while using multicast address as system-ip in sd-routing device.
CSCwi93784	(SWI case 01257768)FW upgrade does not work properly on P-LTE-MNA with 17.12.1a and 17.12.2 IOS
CSCwj06622	The segmentation fault and core files are seen on Cisco IOS XE Catalyst SD-WAN device in controller-managed SD-WAN due to speedtest
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure.
CSCwi62230	SIG tunnel: 'SIG STATEâ is showing blank value.
CSCwj25493	Cisco IOS XE Catalyst SD-WAN device crashed twice with Critical process linux_iosd_image fault on rp_0_0
CSCwf98902	Unexpected reboot on Cisco IOS XE Catalyst SD-WAN device during longevity test.
CSCwj27545	Cisco IOS XE Catalyst SD-WAN device router crashing due to ftmd.

Identifier	Headline
CSCwi83365	C1117-4PLTEEA platform crashed with sh pl hard qfp ac feat cef-mpls prefix ip 10.40.201.10/32 vrf 2
CSCwi62239	%IOSXE_MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback managment vrf then removing it.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Identifier	Headline
CSCwh86922	Cisco Catalyst 8300 Series Edge Platforms: Unconfigure EVC will not bring back the original interface mac filter table entries.
CSCwj25508	ASR1k router reports incorrect DOM values over SNMP.
CSCwj51700	CPP crashes after re-/configuring "ip nat settings pap limit ... bpa" feature in high QFP state.
CSCwj59970	Some duplicated packets are dropped when there are frequent BFD flaps on primary path transport.
CSCwj04575	Router crashed during SNMPwalk while removing SFP.
CSCwj48421	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi
CSCwj44868	%GDOI-3-COOP_CONFIG_MISMATCH: Rekey Acknowledgement configuration mismatch LOWER SEVERITY.
CSCwi86227	Cisco Catalyst 8500 Edge Platforms router reports incorrect DOM values over SNMP
CSCwj07584	Cisco Catalyst 8300 Series Edge Platforms: Shared HSRP vMAC between multiple interfaces cause data plane problem.
CSCwj53456	Crash triggered by 'crypto ikev2 cluster detail' command.
CSCwj01917	After Upgrade to 17.9.4a, Cellular Interface Forced to Admin Down.
CSCwj58203	NAT DIA Flow Stickiness not working as expected when maximum paths change.
CSCwj54112	17.9.5 - Seeing discrepancy in the Enterprise cert on the device CLI vs Cisco SD-WAN Manager GUI
CSCwi70306	Packets for DNS were being misclassified by NBAR due to advertised record from SD-AVC.
CSCwj06950	C1117 - DSL module gets stuck in a booting state.
CSCwj60104	Cisco IOS XE Catalyst SD-WAN device- Asymmetric Routing version 17.9.4
CSCwj54205	Cisco SD-WAN Manager: Template push fails with QoS policy.
CSCwj02246	Cisco Catalyst 8200L : The SFP EN LED on C8200L is not lighted up after interface no shutdown.

Identifier	Headline
CSCwj21653	IR1101: Kernel crash over continuous reloads.
CSCwi29637	Cisco Catalyst 8200L SFP interface shut down, but opposing device interface still up
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwi98707	Cisco Catalyst 8300 Series Edge Platforms: NIM module reloads while collecting PCM captures on voice-port.
CSCwj48393	ISG: Service with no priority are not working as expected.
CSCwj40589	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
CSCwj26085	[SIT]: control connections in tls with mode Cisco SD-WAN Controller & Cisco SD-WAN Manager goes to 'trying' state with UTD
CSCwj36946	Cisco Catalyst 8200 Series Edge Platform: ROMMON 17.6(8.1r) release for auto-upgrade.
CSCwj31476	17.14/20.14: DSL device feature template suite fails with CONFD ERROR 'no switchport access vlan 4'
CSCwj29381	Service-policy will not be applied to a new Tunnel interface when sourced using sub-interface.
CSCwj45177	The "dmidecode: command not found" error seen executing "show sdwan certificate validity"
CSCwj53782	If FPM failed and path changes from SIG to DIA, flow stickiness is not triggered.
CSCwh29856	FN980 cellular_term_dip Removing IP DNS profile:0 active_prof:0 immediately after attachment.
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
CSCwi56641	100G/40G: QSFP fiber: C9500X-28C8D reports link-flap error when peer C8500-20X6C reloads.
CSCwi81026	SDWAN BFD sessions flapping during IPSec Rekey in scaled environment.
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process.
CSCwj51102	Cisco Catalyst 8000V Edge Software goes into a hung state with nearly 100% memory utilisation.
CSCwi96692	**** Unable to Install HSEC K9 Licence for PID C1111-8PLTELAWF & C1111X-8P ****
CSCwi67621	Cisco Catalyst 8300 Series Edge Platform: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)

Identifier	Headline
CSCwi59854	The 'show sdwan policy service-path' command gives inconsistent results with app name specified.
CSCwj42448	The APN password in plain text when Cellular controller profile is configured.
CSCwj02661	The UTD signature update failure and device not recording the update.
CSCwi89510	Cisco Catalyst 8500L - MPLS elephant flow causing overruns.
CSCwj43905	Unexpected reboot due to QFP-Ucode-Cisco Catalyst 8000V failure.
CSCwj05500	Cisco Catalyst 8000V Edge Software (- Accelerated Networking stops working due to driver issue
CSCwj38804	ZBFW FQDN patterns missing from QFP patten-list.
CSCwj03621	ASR-2HX: Ping with smaller packet size is failing on macsec enabled port.
CSCwj02628	Speed-test not working for the Cisco IOS XE Catalyst SD-WAN device running on code 17.12.2
CSCwi59834	C8300 / IOS XE 17.9 / entSensorThresholdValue OID for PDU1 missing
CSCwh91039	CSR1000V/Cisco Catalyst 8000V Edge Software – High System CPU Load Reported due to unsupported number of vCPUs Allocated
CSCwj41331	Guestshell: Fail to run "guestshell run dohost "show version"" on ISR1K since release 17.13
CSCwj36915	C-NIM-2T: macsec not working under LACP port-channel member port.
CSCwi40697	Modem may not come back up from FW upgrade with LM960A18 and FN980 modems.
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented.
CSCwj49297	ISR 4351 send out BYE message with high RTT to CUCM
CSCwj60635	Inconsistency between IOS-XE and sdwan configuration
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwj53986	Extremely poor DMVPN performance on Cisco Catalyst 8500L with TrustSec
CSCwi98171	C8500-20X6C Hundred Gig interface will not come up with autonego enabled
CSCwj53927	Document : Multiple GETVPN groups under same crypto map not supported in IOS-XE
CSCwj58176	Cisco IOS XE Catalyst SD-WAN device performing NAT for Directly connected traffic.
CSCwj49946	ASR 1k | cpp-mcplo-ucode | None pppoe_get_session.
CSCwi34743	ASR1K Tx queue_depth is 2x qlimit and output discards.

Identifier	Headline
CSCwj32347	DIA Endpoint tracker not working with ECMP routes when Loopback is used as source.
CSCwh89618	C8500-20X6C: CRC errors seen with macsec enabled on 100G ports.
CSCwj58398	Bandwidth Policer on Cisco IOS XE Catalyst SD-WAN device is limiting traffic below configured traffic rate.
CSCwi60071	IPv6 PREFIX delegation is not working on ADSL PPPOA.
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwj54851	High Memory UItilization | Process ftmd | ftm_fnf
CSCwj37051	Cisco SD-WAN Manager CLI template fails to attach to CG418-E/CG522-E with error "access-denied"
CSCwj27108	SD-WAN Not Balancing Traffic to Default Route
CSCwj49941	dns-snoop-agent has TCAM entry with all zeros for some regex patterns.
CSCwj31354	Cisco IOS XE Catalyst SD-WAN device | 17.6.6 | Template push failure due to service timestamps
CSCwj30334	CVLA ucode crash when attempting merge on used block.
CSCwj60332	Device certificate import failure on Cisco Catalyst 9800 WLC.
CSCwj13681	Cisco Catalyst 8300 Series Edge Platforms can only store 64 FQDN patterns, but config accepts more than 64.
CSCwj70773	Unable to create a portchannel interface with maximum number limit.

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

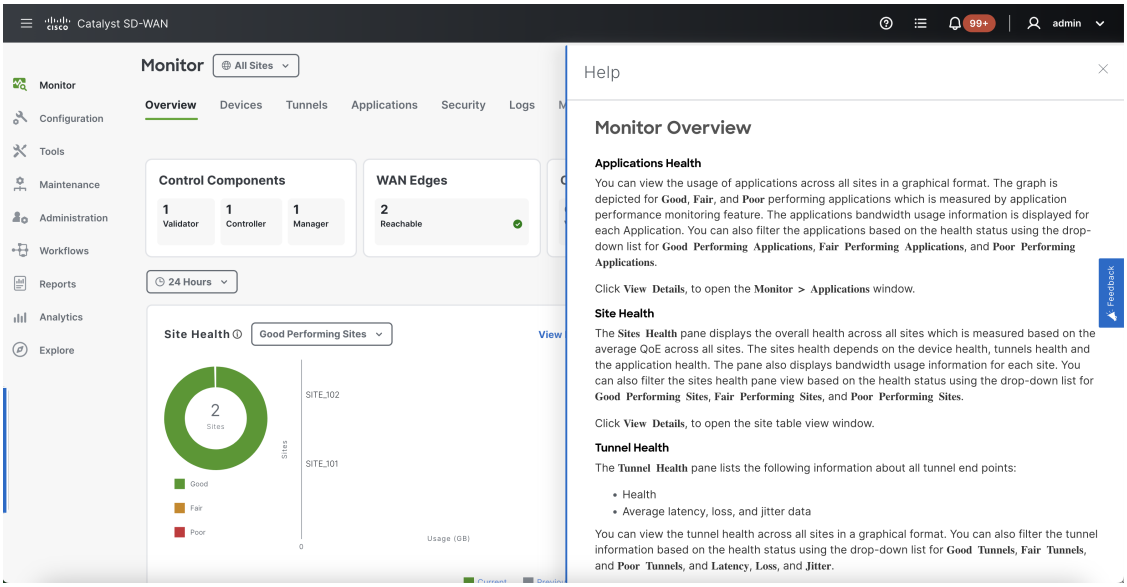
For device compatibility information, see Cisco Catalyst SD-WAN Device Compatibility.

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 1: Help Content in a Slide-in Pane

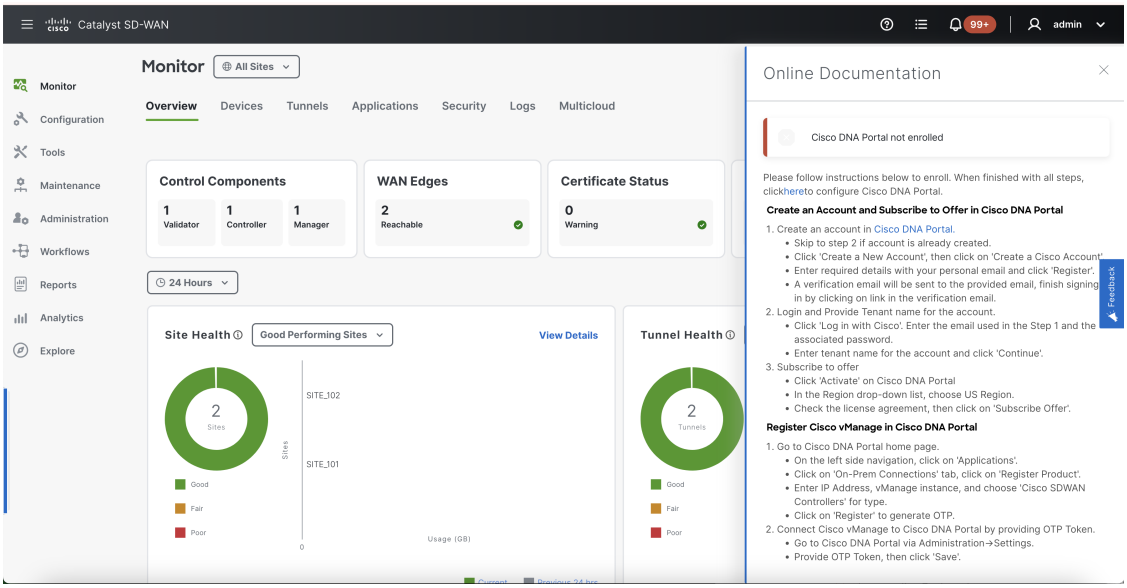


Cisco DNA Sense

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 **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.



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

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)

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)

© 2024 Cisco Systems, Inc. All rights reserved.