Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.7.x

First Published: 2021-12-17

Last Modified: 2022-06-25

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 17.7.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 17.7.x, which provides Cisco 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 vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.7.x.

For release information about Cisco SD-WAN Control Components, refer to Release Notes for Cisco Catalyst SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.7.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.7.x

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 SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco IOS XE Release 17.7.1a

Feature	Description
Cisco SD-WAN Getting Started	
Support for the Cisco Catalyst 8000V Edge Software Platform on OpenStack Train	This feature introduces support for managing a Cisco Catalyst 8000V Edge software platform hosted in the OpenStack cloud computing platform "Train" release.
Day 0 WAN Interface Automatic IP Detection using ARP	This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process.
Certificate Revocation	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.
DigiCert Migration	This feature replaces the Symantec Certificate Authority (CA) server with Digicert Certificate Authority server for signing the controller device certificates on Cisco SD-WAN controllers including Cisco vSmart Controller, Cisco vBond Orchestrator, and Cisco vManage. You can protect, verify, and authenticate the identities of organizations and domains using these certificates.
Cisco SD-WAN Systems and Interfaces	
Cisco Unified Border Element Configuration	This feature lets you configure Cisco Unified Border Element functionality by using Cisco IOS XE SD-WAN device CLI templates or CLI add-on feature templates.
Cisco ThousandEyes Support for Cisco 1000 Series Integrated Services Routers	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco ISR 1100X-6G devices.
Support for HSRP and HSRP Authentication on Cisco IOS XE SD-WAN Devices	This feature allows you to configure HSRPv2 and HSRP authentication on Cisco IOS XE SD-WAN platforms via CLI template. HSRP is a long-standing Cisco proprietary First Hop Redundancy Protocol (FHRP) to support version 2 of the protocol and authentication.
Added Support for Configuring Geofencing Using a Cisco System Feature Template	This feature adds support for configuring the geographical boundary of a device using a **Cisco System** feature template. With this feature, you can also configure automatic geolocation detection, where the device determines its own location, while configuring geofencing. A new parameter **auto-detect-geofencing-location** is added to the **geolocation (system)** command.

Feature	Description
VRRP Interface Tracking for Cisco IOS XE SD-WAN Devices	This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco IOS XE SD-WAN devices.
TCP/UDP Endpoint tracker and Dual Endpoint Static route tracker for Cisco IOS XE SD-WAN devices	This feature enables you to configure the TCP/UDP individual Endpoint static route tracker and to configure tracker group with IPv4, TCP/UDP Dual Endpoint static route trackers for service VPNs to enhance the reliability of the probes.
DHCP for IPv6	This feature allows you to configure DHCP for IPv6 (DHCPv6) on Cisco IOS XE SD-WAN devices to assign IPv6 addresses to hosts on an IPv6-enabled network. Assigning of IPv6 addresses is accomplished using SLAAC, DHCPv6 with SLAAC, DHCPv6 with SLAAC, DHCPv6 Prefix Delegation, or DHCPv6 Relay. A Cisco IOS XE SD-WAN device can be configured for DHCPv6 as a DHCP server, DHCP client, or as a DHCP relay agent.
Hierarchical SD-WAN	Hierarchical SD-WAN provides the ability to divide the architecture of the Cisco SD-WAN overlay network into multiple regional networks that operate distinctly from one another, and a central core-region network for managing inter-regional traffic. The hierarchical architecture enables you to use different traffic transport service providers for each region, and for the central core-region network, to optimize cost and traffic performance. It also simplifies traffic configuration for some scenarios, and provides a robust, adaptive topology that can help prevent routing failures in specific network scenarios.
Co-Management: Granular Role-Based Access Control for Feature Templates	This feature introduces greater granularity in assigning role-based access control (RBAC) permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Cisco SD-WAN Routing	
RIPv2 support on Cisco IOS XE SD-WAN Devices	This feature enables you to configure RIPv2 on Cisco IOS XE SD-WAN devices. Routers redistribute RIPv2 routes to OMP for advertisement in the SD-WAN overlay and to OSPFv3 for service-side routing.
Cisco SD-WAN Policies	
Configure Default AAR and QoS Policies	This feature is an enhancement to the centralized and localized policies feature. This feature allows you to configure default application-aware routing (AAR) and quality of service (QoS) policies on Cisco IOS XE devices.
Flexible Netflow for VPN0 Interface	This feature supports Netflow on VPN0 interfaces. Flexible Netflow acts as a security tool, enables exporting data to Cisco vManage and detects attacks on devices and monitors traffic.
Cisco SD-WAN Security	

Feature	Description
Configure Interface Based Zones and Default Zone	This feature enables you to configure an interface-based firewall policy to control traffic between two interfaces or an interface-VPN-based firewall policy to control traffic between an interface and a VPN group. This feature also provides support for default zone where a firewall policy can be configured on a zone pair that consist of a zone and a default zone.
Resource Limitations and Device-global Configuration Options	This feature enables you to define resource limitation options such as idle timeout and session limits, and device-global options in the policy summary page to fine-tune a firewall policy behaviour after a firewall policy is implemented in Cisco SD-WAN.
Unified Logging for Security Connection Events	This feature supports Unified Logging which is used to capture information about connection events across different security features at different stages during policy enablement and execution. With Unified Logging, you can have visibility to the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol or applications. Additionally, this feature also provides support for On-Demand Troubleshooting. On-Demand troubleshooting allows a user to view the connection events of inspect flows of traffic from a device within a configured period of time.
GRE Over IPsec Tunnels Between Cisco IOS XE Devices	This feature allows you to set up GRE over IPsec tunnels with IKEv2 RSA-SIG authentication on Cisco IOS XE SD-WAN devices in the controller mode to connect to Cisco IOS XE devices in the autonomous mode. This set up enables Cisco IOS XE SD-WAN devices to use OSPFv3 as the routing protocol and multicast traffic across the WAN network. You can configure GRE over IPsec tunnels using the CLI device templates in Cisco vManage.
High Availability	
Disaster Recovery User Password Change	This feature lets you change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.
Cisco SD-WAN Cloud OnRamp	
Cloud onRamp for SaaS Support for Webex	Added Webex to the list of cloud applications for which Cloud onRamp for SaaS can determine the best network path to the cloud server. Cisco vManage periodically downloads a list of Webex servers organized by geographic region. Cloud onRamp for SaaS uses this server list to help calculate the best network path for Webex traffic in different regions.

Feature	Description
Support for Using Microsoft Telemetry Metrics for Microsoft 365 SharePoint and Teams Traffic.	This feature adds support for using Microsoft telemetry metrics for Microsoft 365 SharePoint and Teams (Skype). Cloud onRamp for SaaS uses the metrics data when determining the best path for Office 365 traffic.
Azure Scaling, Audit, and Security of Network Virtual Appliances	This feature allows you to edit the SKU Scale value, carry out the audit to identify discrepancies, and have better security for your Network Virtual Appliances (NVAs).
Support for Cisco VM Image Upload in qcow2 Format	This feature allows you to upload a virtual machine image to Cisco vManage in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.
Packet Capture for Cloud onRamp Colocation Clusters	This feature lets you capture packets at either the physical interface level (PNIC) or the virtual interface level (VNIC) on a CSP device of a colocation cluster. You can capture packets on one or more PNICs or VNICs on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format and therefore helps in application analysis, security, and troubleshooting.
Cisco SD-WAN Monitor and Maintain	
Additional Diagnostics Information Added to Admin-Tech File	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	This feature enables you to upload an admin-tech file directly from Cisco vManage when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests (SRs) from Cisco vManage. This streamlines the steps required for working with TAC to troubleshoot a problem.
Bidirectional Packet Capture for Cisco IOS XE SD-WAN Devices	This feature enhances the embedded packet capture functionality to support bidirectional packet capture through Cisco vManage.
Software Upgrade Using a Remote Server	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco vManage, and add locations of software images on the remote server to the Cisco vManage software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.

Feature	Description
Enhanced Cisco vManage User Interface for a Consolidated Monitoring View	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all monitoring components have been organized into pill buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu so that you can easily locate these features.
Cisco SD-WAN SNMP	
Support for SNMPv3 AES-128 and AES-256 bit Encryption Protocol	This feature allows you to configure SNMPv3 users in support with SHA-1 authentication protocol and AES-128 and AES-256 encryption on Cisco IOS XE SD-WAN devices.
Cisco SD-WAN NAT	
Dual Endpoint Support for Interface Status Tracking on Cisco IOS XE SD-WAN Devices	This feature allows you to configure tracker groups with dual endpoints using the Cisco System template and associate each template group to an interface. The dual endpoints provide redundancy for tracking the status of transport interfaces to avoid false negatives.
Intra-VPN Service-Side NAT Support	Intra-VPN allows service-side LAN interfaces to communicate with other service-side LAN interfaces within the same VPN. Configure the **ip nat outside** command on the LAN interface for which you require translation of the source IP addresses to the outside local addresses. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface. You configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.
NAT66 DIA Support	The IPv6-to-IPv6 Network Address Translation (NAT66) Direct Internet Access (DIA) feature enables an IPv6 device to translate an inside source address prefix to an outside source address prefix in IPv6 packet headers. NAT66 DIA allows you to direct local IPv6 internet traffic to exit directly to the internet from the service-side VPN (VPN 1) through the transport VPN (VPN 0). You configure NAT66 DIA using Cisco vManage, the CLI, or a device CLI template. This feature introduces new CLI commands. For more information, see the Cisco IOS XE SD-WAN Qualified Command Reference Guide.
Cisco SD-WAN Remote Access	

Feature	Description
SD-WAN Remote Access	Remote access refers to enabling secure access to an organization's network from devices at remote locations. Cisco Catalyst SD-WAN remote access (SD-WAN RA) integrates remote access functionality into Cisco Catalyst SD-WAN. SD-WAN RA enables Cisco IOS XE Catalyst SD-WAN devices to function as RA headends, managed through Cisco SD-WAN Manager. This eliminates the need for separate Cisco Catalyst SD-WAN and RA infrastructure, and enables rapid scalability of RA services. RA users can use the same software- or hardware-based RA clients as with solutions that do not integrate with Cisco Catalyst SD-WAN. For RA users, benefits include extending Cisco Catalyst SD-WAN features to remote users. RA users can access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet

New and Enhanced Hardware Features

New Features

- Support for Cisco IR8140 Heavy Duty Router—Cisco Catalyst SD-WAN capability can now be enabled on Cisco IR8140H and Cisco IR8140H-P Heavy Duty Routers.
- Support for Cisco DSL SFP Module—Cisco SD-WAN Manager CLI device templates now support the Cisco DSL SFP Module SFP-VADSL2+-I= for use with Cisco IR1101 Integrated Services Routers.

Software and Hardware Behavior Changes in Cisco IOS XE Release 17.7.1

Behavior Change	Link to Updated Documentation
The Cisco IOS XE Catalyst SD-WAN device loads automatically with an appropriate message on the console.	A note is added in the usage guidelines section of the request platform software sdwan config reset command.
Admin-Tech file enhancement	Upload an Admin-Tech File to a TAC Case
Angle brackets (< or >) are converted to their HTML equivalents in Cisco SD-WAN Manager feature templates.	A note on special characters is updated in the Feature Templates section.
The upgrade considerations are updated for auto-negotiation support.	Upgrade Considerations
As part of Cloud onRamp for Multi-Cloud functionality, Cisco SD-WAN Manager generates custom applications from the services that it discovers in a Google Cloud account. Cisco SD-WAN Manager now supports longer, more meaningful names for the namespace and service name of services that you create in a Google Cloud account.	Service Directory Lookup and Traffic Policies with Discovered Apps

Software and Hardware Behavior Changes in Cisco IOS XE Release 17.7.2

Behavior Change	Description
SNMP appRoute MIB object identifiers (OIDs) are added to support **Mean Jitter**, **Latency**, and **Packet Drop** data requests from SNMP.	A note is added in the Supported SNMP MIBs section.
A notification is generated when there is an SNMP trap for a Bidirectional Forwarding Detection (BFD) state change.	BFD state change entries are added in the Information Abou tables.
A new command **alarms alarm bfd-state-change-syslog** is added for enabling or disabling BFD syslog messages.	A new command alarms alarm bfd-state-change syslog is A note is added in the Using the CLI section.
A limitation on real-time display of omp routes received and advertised in Cisco vManage is added to avoid excessive CPU usage.	A note is added in the OMP Route Redistribution section.

Important Notes, Known Behavior, and Workaround

- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your vAnalytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to vAnalytics using this URL: https://analytics.viptela.com. If you can't find your vAnalytics login credentials, open a case with Cisco TAC support.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the **`table`** keyword is added to all show sdwan commands for which the output needs to be displayed in a tabular format. Using **`| tab`** is restricted for all Cisco SD-WAN commands starting from Cisco IOS XE SD-WAN Release 16.11.x.

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Bugs for Cisco IOS XE Release 17.7.2

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 Release 17.7.2

Identifier	Headline
CSCwa98047	SASE - after Cisco IOS XE Catalyst SD-WAN device upgrade, umbrella dns config set to NONE in show umbrella config
CSCwa38570	SaaS traffic not taking the best SIG tunnels when CoR SaaS with SIG tunnels configured
CSCwa81485	C8200 running 17.7.1a crashed in FNF feature when a local call is done
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwa42747	Fugazi and TSN get crashed consistently when start nwpi trace
CSCvz31260	DP CPU degradation in Collab and Contact center flows on ISR4451 platform on 17.3 throttle
CSCwa92137	17.7.1 - Cisco IOS XE Catalyst SD-WAN device is changing ICMP ID in ICMP echo replies intermittently
CSCwb08636	IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error seen for TLOCExt setup after upgrade
CSCwb21195	Cisco SD-WAN ASR sees Anti-Replay drops when sequence number is beyond 32 bit
CSCvz91487	Cisco IOS XE Catalyst SD-WAN device config changed via CLI while control is down don't revert once the control is restored
CSCvz62032	Attach gateways failed in cloud express
CSCvz90553	Ipv4NoRoute Drops seen on SC with Traffic Test
CSCwa83899	Cisco vManage getting "Non-OK device" error when attaching a template to several devices.
CSCwa73783	Incorrect Cisco IOS XE Catalyst SD-WAN device COR for SAAS Policy Sequence Programming
CSCvz38018	Cisco IOS XE Catalyst SD-WAN device reloads unexpectedly when issuing OMP shutdown from the CLI
CSCwa23789	SNMP Approute MIB nnot working for Mean Jiiter, Latency and Packet Drop
CSCwa64990	Cisco SD-WAN NAT DIA with data policy not work properly with static destination NAT
CSCwa78762	Umbrella SIG tunnel creation failed after config reset for PnP
CSCwa93930	"alarms alarm bfd-state-change syslog" command is getting rejected while reconfiguring the device.
CSCwa96768	SIP/ICMP flow can't be forwared after FEC enabled and WAN link re-connected.

Identifier	Headline
CSCwa71862	Crash may be hit when start stop flow monitor in NWPI domain monitor
CSCvz98955	Cisco IOS XE Catalyst SD-WAN device: bfd session may stuck down
CSCwb59736	CSR BFD tunnel are zero with SDWAN version 17.03.03.0.7
CSCwb07025	Packets are being fragmented even if Dont Fragment is set.
CSCwa53223	Cisco IOS XE Catalyst SD-WAN device app-route policy not load balancing traffic as expected when SLA doesn't meet
CSCvz74773	Discrepancies in CLI and GUI interface details (Truncating interface numbers)
CSCwa35900	Cisco IOS XE Catalyst SD-WAN device may experience an unexpected reset in cpp_cp_svr and fman_fp
CSCwa93189	Cisco IOS XE Catalyst SD-WAN device 17.7 not generating "latency" in Pfr

Open Bugs for Cisco IOS XE Release 17.7.2

Identifier	Headline
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN device with NAT
CSCwb52616	Cisco IOS XE Catalyst SD-WAN device SD-WAN doesn't inject ping packets due to no route although data policy has nat vpn-0
CSCwa52915	Replicator with direct multicast source reachability should be preferred among selected replicators
CSCwa92082	RG B2B(Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on ISR 4461
CSCwb67406	The IPSLA udp-jitter V3 (optimize timestamp+ precision microseconds) is not supported on C8500 now
CSCwa79322	20.6 vEdge-cloud deployed with v2 cloud-init file fails to set MAC addresses on interfaces
CSCwb73511	Cisco IOS XE Catalyst SD-WAN device is not able to bring up SIG tunnels after reboot
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwb69005	confd crash on controller-managed ISR4K
CSCvx74917	[17.5 Umbrella] DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit
CSCwb43423	Cisco IOS XE Catalyst SD-WAN device: IOS XE image installation fails
CSCwa47197	IPsec destination IP does not get set

Identifier	Headline
CSCwa49721	Cisco SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb13820	C8Kv crashed at high scale with IPSEC and heavy features configured
CSCvz81428	SIT : vedaemon assert noticed in the ISR 4221 over weekend longevity
CSCvz87855	mroute state stuck after Cisco IOS XE Catalyst SD-WAN device failure is restored
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwb02851	ISR1100 get crashed consistently with memory corruption with pppoe dailer interface flap
CSCwa11349	Incorrect topology on TLOC extension causing high QFP
CSCwa34783	BFD session get stuck to down after site to site speedtest with Loopback as WAN + NAT
CSCwb05743	Crash seen with umbrella config during soak run
CSCwb76509	Assert failure while showing FTM (Forwarding Traffic Manager) data in NH TYPE switch case
CSCwa98545	Checks of route leaks creates memory corruption.
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwa14226	Policy commit retry needed when ConfD commit fails.
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently over Utah platform
CSCwb32635	17.6.2 Cisco IOS XE Catalyst SD-WAN device - vdaemon file is incomplete when running admin-tech
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old cert
CSCwb18223	SNMP v2 community name encryption problem
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
CSCwb74821	yang-management process confd is not running, controller mode 17.6.2a
CSCwb20089	Cisco IOS XE Catalyst SD-WAN device ESP crashes after enable platform debug for Cloud onRamp for SaaS

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a

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 17.7.1a

Bug ID	Description
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCvz41647	Partial multicast drops are seen after a failover event in a site with two Cisco IOS XE SD-WAN devices
CSCvz03912	SDWAN 17.6-Cisco vManage is deleting VRF 65529 but device has Loopback65529 which is referencing VRF 65529
CSCvz03330	Overlay to self-zone icmp traffic fails with ZBFW with drop "DROP 191 (FirewallNotInitiator)".
CSCwa19074	Infinite output from command show sdwan tunnel sla
CSCvy83781	Infinite output from command show sdwan tunnel sla
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address
CSCvy56876	DIA route adjacency broken when IP nat route changed and OMP restart is triggered
CSCvz99404	SdwanImplicitAclDrop seen on non-SDWAN interface after upgrade to 17.6.1

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a

Bug ID	Description
CSCvz81428	vedaemon assert noticed in the ISR 4221 over weekend longevity
CSCvz62032	Attach gateways failed in cloud express
CSCwa14636	Cisco IOS XE SD-WAN device stopped forwarding traffic. Suspect OMPd is busy
CSCvz87855	mroute state stuck after Cisco IOS XE SD-WAN device failure is restored
CSCwa35075	Command "controller SHDSL 0/1/0" gets added to SDWAN configuration post upgrade to 17.06.01a.
CSCvz90553	Ipv4NoRoute Drops seen on SC with Traffic Test
CSCvy55408	router multiple crash. - session hash corrupted
CSCvz46516	sit_regression; speedtest.py- test_speedtest_2edges: Failed to start iperf client
CSCwa34648	Incorrect OMP Labels in On-Demand Tunnel H/S Topology
CSCvz37340	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
CSCwa11349	ASR1002-HX High QFP Utilization
CSCwa11628	Umbrella Certificate is not getting copied to HW device causing umbrella integration to fail

Bug ID	Description
CSCwa16701	after clear sdwan control connections , Tloc on in DB
CSCwa35900	Soln : two core files (cpp_cp_svr and then on fman_fp) on ASR1001-HX during longevity
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old cert
CSCvz91487	Cisco IOS XE SD-WAN device config changed via CLI while control is down don't revert once the control is restored
CSCwa12878	Cisco vManage intermittent netconf connection issue to Cisco IOS XE SD-WAN device
CSCvz98955	Edge:on clear sdwan omp all ,bfd session down for one peer

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.

Redesign of Cisco vManage GUI

From Cisco vManage Release 20.7.1, Cisco vManage GUI is redesigned and offers a new visual display. This section presents a comparative summary of the significant changes between older Cisco vManage releases and Cisco vManage Release 20.7.1 and later.

Changes in Monitor and Tools Menus

Cisco vManage Release 20.7.1 includes the following changes:

- The **Dashboard** menu is removed, and all submenus that were earlier accessible from the **Dashboard** menu are now part of the **Monitor** menu.
- The **Monitor** page provides a real-time user interface with a consolidated view of the monitoring information for the components and services of a Cisco SD-WAN overlay network.
- Using the pill buttons on the **Monitor** page, you can navigate to monitoring information for specific components or services of a Cisco SD-WAN overlay network.
- The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu are now part of the **Tools** menu so that you can easily locate these features.

Figure 1: Dashboard Menu in Cisco vManage Release 20.6.1 and Earlier

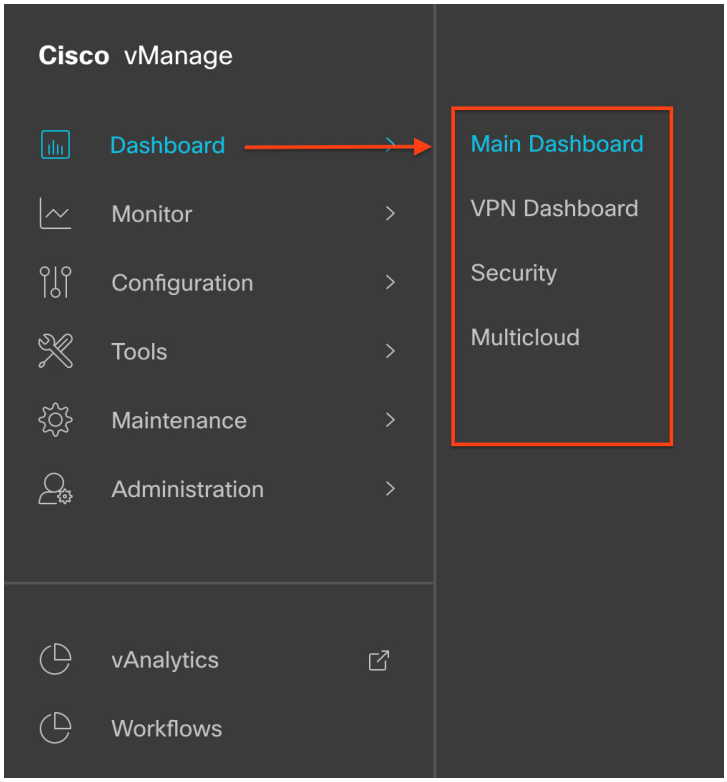


Figure 2: Monitor Menu in Cisco vManage Release 20.7.1 and Later

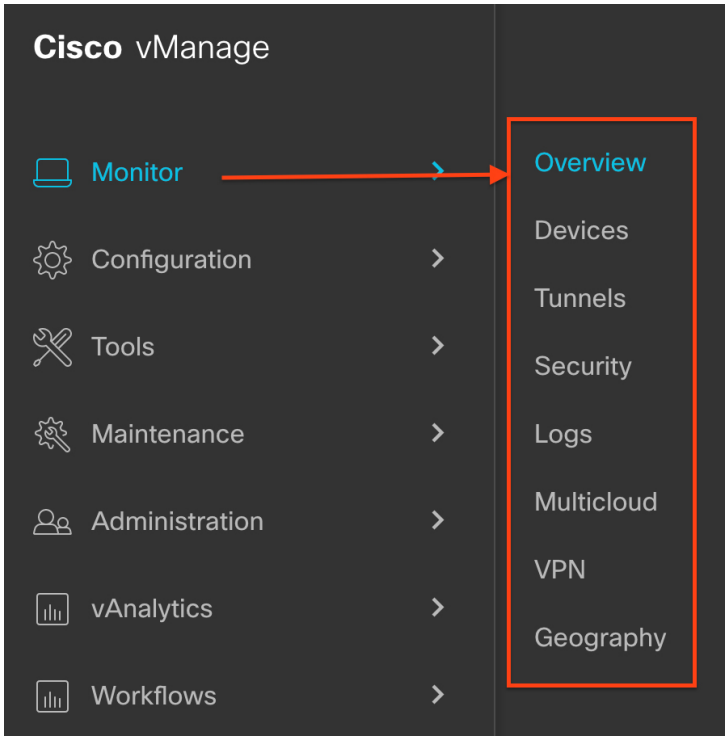


Figure 3: Tools Menu in Cisco vManage Release 20.7.1 and Later

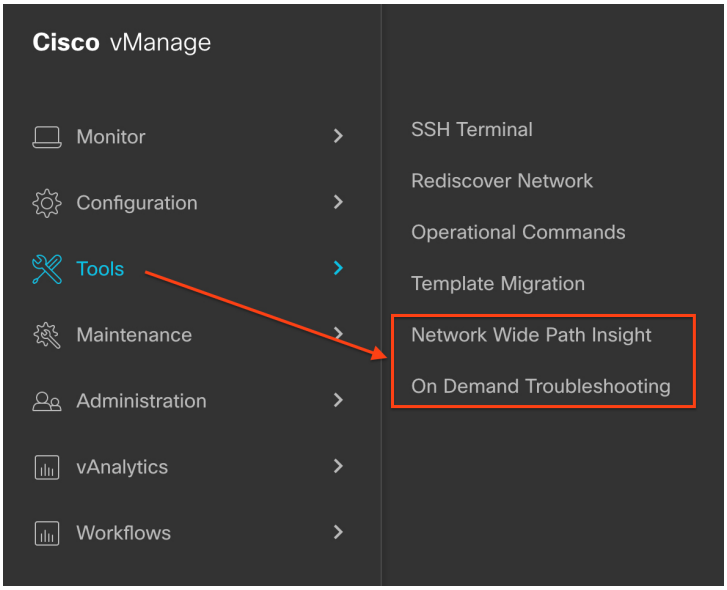


Figure 4: Pill Buttons in Monitor Window in Cisco vManage Release 20.7.1 and Later



Support for Web Content Accessibility Guidelines (WCAG) 2.0 Standard

Cisco vManage Release 20.7.1 supports Web Content Accessibility Guidelines (WCAG) 2.0 standard for the AA conformance level, with the following limitations:

- You cannot exit from SSH terminal using the keyboard.
- Cisco SD-WAN Manager cannot skip repetitive navigation links.
- Data charts on Cisco SD-WAN Manager use colors as the only visual means of conveying information, which is not compliant with WCAG 2.0.
- Some text elements as well as non-text elements in Cisco SD-WAN Manager do not meet the color contrast ratio as defined in WCAG 2.0.

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)

© 2021 Cisco Systems, Inc. All rights reserved.