Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Release 17.18.x

Cisco IOS XE Catalyst SD-WAN Devices Release, 17.18.x

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, 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.

Upgrade Matrix Tool

What's changing

We have transitioned upgrade path information to the new Upgrade Matrix Tool.

Why the new tool

This interactive tool provides a release-specific view of supported upgrade paths, compatibility checks, and prerequisites—helping you quickly identify the optimal upgrade route.

What the tool offers

- Interactive, release-specific upgrade path information
- Compatibility checks and prerequisites
- Advanced search and filtering for faster results

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 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.

New software features

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 guide.

What's new for Cisco Catalyst SD-WAN Control Components 17.18.1a

Table 1. New software features for Cisco Catalyst SD-WAN Control Components

Product Impact	Feature	Description
Upgrade	Log files cleanup during software upgrade	The Cisco IOS-XE software upgrade has been improved to clean outdated files from flash before upgrade.
Cisco Catalyst SD-WAN Monitor and Maintain		
Ease of use	QoS queue statistics	You can monitor traffic across network interfaces and tunnels with real-time and

		historical statistics. This feature extends the existing QoS interface-level view to include class-level traffic insights and per-tunnel QoS statistics.
	Cisco RADKit in Cisco SD-WAN Manager	The Cisco Remote Automation Development Kit (RADKit), a tool for remote automation and troubleshooting, is integrated directly into Cisco SD-WAN Manager. This integration provides the capability to enable or disable the RADKit service using the API in Cisco SD-WAN Manager.
	CoR SaaS - Application Path Status Alarms	Cisco IOS XE Catalyst SD-WAN device triggers three new alarms. These alarms indicate the status of CoR-SaaS application paths. This feature adds a **path-status** field to the **cloudexpress-application-change** notification. Alarms are categorized into Major, Medium and Minor based on the path status: unreachable, reachable and disabled, respectively.
	Cisco Catalyst SD-WAN Analytics Traffic Logs Integration and Insights	This feature introduces traffic logs and security connection event logs in SD-WAN Manager powered by SD-WAN Analytics for filtered data retrieval.
	Advisory	This feature provides centralized visibility into security vulnerabilities and critical Field Notices for your Cisco SD-WAN network. It offers EoX Status section that provides detailed End-of-Support and End-of-Sale information for effective replacement and upgrade planning.
	BFD Troubleshooting for Cisco Catalyst SD-WAN	This feature allows you to get detailed BFD session information on devices to diagnose issues like packet flow, state transitions, and configuration discrepancies.
	Pending requests for upgrading a device Protocol Pack	If you attempt to execute a Protocol Pack upgrade for a set of devices, it is possible that one or more of the devices are using a software version that does not support the Protocol Pack. In this case, the upgrade does not proceed for those devices. You can choose an option for Cisco SD-WAN Manager to keep the pending request to upgrade the device's Protocol Pack, to execute later. Cisco SD-WAN Manager checks the device when it receives a software upgrade, and if the new software version supports the Protocol Pack, Cisco SD-WAN Manager completes the upgrade.
	Delete Protocol Packs	You can delete a Protocol Pack loaded into Cisco SD-WAN Manager. This is useful for removing Protocol Packs that are no longer in use in your network.
Upgrade	Cisco SD-WAN Control Components Upgrade Workflow	With the guided workflow you can upgrade the software image of all the Cisco SD-WAN Control Components.

		It also allows you to apply patch release upgrades to Cisco SD-WAN Control Components, for bug fixes and minor improvements.
	Hosted edge services	You can monitor hosted edge services (IOx applications) for health, associated devices, version, and IOx state using the Cisco Catalyst SD-WAN Manager interface. You can also start or stop the hosted edge services.
	Underlay health visibility	This feature provides enhanced monitoring and troubleshooting capabilities for the underlying network infrastructure that supports your Cisco SD-WAN overlay.
	Device Software Upgrade Workflow Enhancements	The new workflow for device software upgrade includes the following key enhancements: • Uploading software image from local drive. • Filtering devices for software upgrade using device tags and network hierarchy. • Scheduling a software upgrade based on a device's local time zone.
Software reliability	Configuration Consistency across Cisco SD-WAN Controllers	This process ensures consistency in configuration across all Cisco SD-WAN Controllers using a multi-stage approach. The multi-stage approach includes the following stages: * Validation: Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to validate the configuration. * Application: Cisco SD-WAN Manager instructs Cisco SD-WAN Controllers to validate and apply the configuration. * Rollback (Optional): Cisco SD-WAN Manager reverts changes if any issues arise during the application stage. This process prevents issues arising from Cisco SD-WAN Controllers operating on different configurations.
	Safety Barriers	Safety barriers protect the Cisco SD-WAN Controller during resource constraints by monitoring CPU, memory, and disk usage. When thresholds are exceeded, safety barriers generate alarms and restrict services that can further impact resource availability.
Cisco Catalyst SD-WAN Cloud OnRamp		
Ease of use	Cloud OnRamp for SaaS for user-defined SaaS application lists	Cisco SD-WAN Manager supports adding, editing, and deleting user-defined probe endpoints for applications listed in the application catalog. Applications with endpoint details are eligible for: • cloud monitoring, and • steering through best path. You can also create an application list with applications having a common probe endpoint and enable Cloud OnRamp for SaaS for that application list.

Ease of setup	Enhancements to Enable Connectivity to an existing AWS Transit Gateway	This feature enables you to discover and connect a cloud gateway to an existing AWS Transit Gateway created in the AWS portal.
Cisco Catalyst SD-WAN Getting Started		
Ease of setup	Automated Certificate Management with EST and SCEP	With this feature, EST (Enrollment over Secure Transport) and SCEP (Simple Certificate Enrollment Protocol) helps automate the process of enrolling and renewing certificates on devices and services using Cisco SD-WAN Manager.
	Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager	This feature simplifies the configuration of settings for Cisco SD-WAN Control Components.
	First time Settings on Cisco SD-WAN Manager	This feature introduces a task flow to setup all the initial settings by a first-time user of Cisco SD-WAN Manager.
	Default enablement of SD-AVC	The SD-AVC component is enabled by default in new Cisco Catalyst SD-WAN environments. The control for enabling or disabling is in Administration > Settings > SD-AVC.
	Cloud-hosted SD-AVC service for on-premises environments	This release extends the use of a cloud-hosted SD-AVC service to on-premises installations of Cisco Catalyst SD-WAN where internet access is available.
Ease of use	Global search for Cisco SD-WAN Manager	The search box in the SD-WAN Manager header enables you to search for information related to devices, network, and so on. The integration of role-based access control (RBAC) ensures that only authorized users can access data.
	Configuration Database Upgrade for a Cisco SD-WAN Manager Cluster using the CLI	This feature improves configuration database backup and restore functionality with API-driven and manual options, logging and metadata, efficient disk space management, and CLI enhancement for configuration database cloud backup at the cluster level.
	JWT based authentication for APIs	This feature supports Java Web Token (JWT) based authentication, enabling external applications to access Cisco SD-WAN Manager functionalities. API tokens can be generated within the Cisco SD-WAN Manager and shared with these applications, allowing them to access SD-WAN Manager through JWT authorization.
	Add Controller and Validator Components Workflow	The Add Controller and Validator Components workflow adds these SD-WAN Control Components to the Cisco SD-WAN fabric.
Software reliability	Block Netconf on Cisco Catalyst SD-WAN device	This feature introduces a security update for Cisco IOS XE Catalyst SD-WAN devices. It blocks NETCONF requests on all IP addresses except the system IP to enhance device

		security. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, the feature blocks port 830 by default.
	Staging for certificate installation on WAN edge devices	When Cisco SD-WAN Manager installs a new certificate on a WAN edge device, the device first tests the certificate in a staging step before proceeding with installing the certificate. The device verifies that it can successfully establish control connections using the certificate.
	WAN edge device certificate management workflow	The WAN Edges Certificate Management workflow updates the authentication certificates for edge devices in the network. This is useful for updating certificates before they expire.
	SD-WAN Control Components certificate management workflow	The Control Components Certificate Management workflow updates the authentication certificates for SD-WAN Control Components in the fabric. This is useful for updating certificates before they expire.
Licensing process	Support for Cisco PKI Certification	This feature allows Cisco SD-WAN Manager to transition from vManage signed certificates to Cisco PKI as the default certificate method for virtual routers to enhance security and reliability.
Cisco Catalyst SD-WAN Policy Groups		
Ease of use	Version Management for Security Policy	With this feature you can track and manage changes to your security policies using the version history.
	Support for Topology Tagging	With this feature you can add devices to a topology using tags.
Cisco Catalyst SD-WAN Policies		
Ease of use	DTA Support for FNF Statistics	Cisco IOS XE Catalyst SD-WAN devices use DTA to handle all FNF statistics.
Software reliability	Policy Information in Service Tunnel Path	This feature aims to detect when policy download fails and raises an Alarm (policy-enforcement-status). Additionally, this feature introduces new **service-path** show commands.
Cisco Catalyst SD-WAN Security		
Ease of use	Custom IPS signature packages	With the custom IPS signature Packages, you can create custom Snort3 IPS signature sets, modify IPS rule actions, and add comments for traceability in Cisco SD-WAN Manager.
	Security Cloud Control Integration with Cisco SD-WAN Manager	Security Cloud Control is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation. Security Cloud Control's integration with Cisco

		SD-WAN Manager provides centralized management for Cisco Catalyst SD-WAN Branch WAN environments. The integration allows you to do the following: • Efficiently manage security policies and objects, configure and edit them, and push changes using the Security Cloud Control dashboard. • Effective monitoring and detection of security threats from a centralized Security Cloud Control dashboard. • Analyze security threats from logs and events in Security Cloud Control dashboard using data sent from Security Analytics and Logging.
	Anti-Replay Recovery Support	This feature enables recovery support when there is anti-replay packet drops in the data plane with IPsec due to packets delivered out of order outside of the anti-replay window.
Ease of setup	SGT Propagation with Cisco TrustSec Integration using Configuration Groups	With this feature you can configure SGT propagation using TrustSec feature under Other Profile in a configuration group in Cisco SD-WAN Manager.
Cisco IOS XE Catalyst SD-WAN Alarms		
Software reliability	OMP ribout memory usage alarm	The OMP ribout memory usage alarm monitors and alerts about the memory buffer utilization of OMP ribout.
	BFD Scale Threshold Alarm	Cisco IOS XE Catalyst SD-WAN device triggers an alarm based on BFD session usage. The alarm can indicate one of the four states: Healthy, Notice, Warning, or Critical, depending on the level of BFD session usage
Cisco IOS XE Catalyst SD-WAN Qualified Commands		
Ease of use	Removal of Telnet service from IOS-XE	This feature provides a secure method to disable Telnet access on IOS-XE platforms. Once disabled, Telnet can only be re-enabled via factory reset, ensuring tamper-proof access control.
Software reliability	NAT Serviceability	To ease the troubleshooting, **show ip nat status** and **show running nat** commands are introduced.
Cisco Catalyst SD-WAN Rugged Series Router Configuration		
Ease of use	Raw socket	You can transport serial data across your IP networks by configuring TCP or UDP options through configuration groups on supported Cisco rugged routers.
Upgrade	Wi-Fi Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco SD-WAN Manager supports upgrading the Wi-Fi module firmware on Cisco IR1800 platforms.
	Ignition power management: configuration group support and	Configure and monitor ignition power and sensing capabilities of IR1800 routers using Cisco SD-WAN Manager. It prevents the router

	real-time monitoring	from draining a vehicle's battery and keeps the router running when the vehicle is stopped, eliminating reload times each time the vehicle restarts.
Cisco Catalyst SD-WAN Licensing		
Licensing process	Assigning high availability licenses	When using the license assignment workflow, an HA License option streamlines the process of assigning high availability (HA) licenses to secondary devices in an HA scenario.
	Cisco Enterprise Agreement Workspace integration	Cisco SD-WAN Manager can transfer licenses from the Cisco Enterprise Agreement Workspace to Cisco Smart Software Manager (Cisco SSM). This enables the synchronization between SD-WAN Manager and Cisco SSM to include licenses acquired through the Cisco Enterprise Agreement system.
	License management report	The license management report describes how many licenses have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. View the reports on the Reports page.
Cisco Catalyst SD-WAN Systems and Interfaces		
Upgrade	P-LTE-450 MHz Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco SD-WAN Manager supports upgrading the P-LTE-450 MHz module firmware on the following platforms: * Cisco IR1101 platform * Cisco IR1800 Series platforms
Ease of use	Reset the profile configuration of a cellular modem	This sub-feature of the Cellular Controller feature enables you to reset the configuration of a cellular modem operating on a device using the CLI.
Ease of setup	Configuring and Monitoring P-LTE-450 modules using Cisco SD-WAN Manager	You can configure category P Long-Term Evolution (LTE) 450MHz Pluggable Interface Module (PIM), referred to as P-LTE-450, on rugged series routers using the Ethernet interface in Cisco SD-WAN Manager. Additionally, Cisco SD-WAN Manager enables you to monitor the module's performance through the monitoring dashboard. P-LTE-450 modules supports Cisco IR1101 Rugged Series Router and Cisco IR1800 Rugged Series Router.
Cisco Catalyst SD-WAN Network-Wide Path Insight		
Ease of use	Automatic security alert tracing option	A new Security Alert option has been added to the auto-tracing features, initiating a trace and capturing details whenever UTD detects security issues like IPS and file reputation alerts in Cisco Catalyst SD-WAN.

	Export and import traces	If you perform a trace and find a network issue, you can export the trace information to analyze externally. For example, the information may be useful for troubleshooting as part of a Cisco Technical Assistance Center (TAC) case. You can import a saved trace to view the details in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN High Availability		
Software reliability	Controller Group Redundancy	Cisco Catalyst IOS XE devices ensure consistent connectivity by connecting to specified controllers in their Control Group List. They maintain redundancy by switching to alternate controllers within or across groups when primary controllers are unavailable.
Cisco Catalyst SD-WAN AppQoE		
Hardware reliability	Cisco Secure Routers support for AppQoE	**The following Cisco Secure Routers are supported for AppQoE:** • **C8231-E-G2** • **C8235-E-G2** • **C8355-G2** • **C8475-G2** • **C8455-G2** • **C8161-G2** • **C8151-G2**

Changes in behavior

To view changes in behavior for 20.18.1, see Changes for 20.18.1

Changes for 17.18.1a

Behavior change	Description
TLOC extension configuration If a device is using Cisco IOS XE Catalyst SD-WAN Release 17.9.x or earlier, and the tunnel interface configuration includes a TLOC extension configuration, then upgrading to certain releases required some steps. This issue has been resolved in various releases, including Cisco IOS XE Catalyst SD-WAN Release 17.18.1a.	See the Restrictions for software upgrade section.

Behavior change	Description
From Cisco Catalyst SD-WAN Manager Release 20.16.1, AWS Direct Connect Gateways are shared only by connections having the same virtual network association type (Direct to VPC, Transit Gateway or Cloud Gateway). When you upgrade to Cisco Catalyst SD-WAN Manager Release 20.16.1 or later releases, ensure that the AWS Cloud Gateway connections and Private VPC connections do not share the same Direct Connect Gateway. We recommend that you delete the existing connection and create new connections before the upgrade.	See Create Multicloud Networks to AWS.
The replication logs are retained for one year. Any historical data older than one year is automatically pruned.	See Guidelines for Registering Disaster Recovery.
ca-check-strict command added under crypto-pki-trustpoint	**ca-check-strict** is a new cli command, added under crypto pki trustpoint. If you enable this command, the peer will reject a CA certificate without basic constraints.
Catalyst 8500 Series Edge Platforms BFD Session increase	From Cisco Catalyst SD-WAN Manager Release 17.18.1a, the maximum SD-WAN IPsec tunnel scale for Catalyst 8500 Series Edge Platforms has been enhanced to 12,000 BFD sessions.
IPsec Rekey Command Restores Flapping BFD Sessions.	Use **the platform software sdwan security ipsec-rekey** command to regenerate IPsec keys. This helps restore stability to BFD sessions that flap or fail due to the IN_US_V4_PKT_SA_NOT_FOUND_SPI drop.
In the Add Site page of Configuration > Network Hierarchy, the address, latitude and longitude fields are added to include the exact location of the site.	See the Create a Site in a Network Hierararchy section for more details.
IKEv2 Rekey Failure When Algorithms Change on Cisco IOS XE.	IKE rekey operations will fail in Cisco IOS XE if the negotiated algorithms from the initial exchange are changed or unavailable thus requiring a full renegotiation with updated algorithms. See Configure Cisco Umbrella Using a CLI Device Template
For an IPv4 SD-WAN tunnel carrying IPv6 traffic, the system uses the IPv6 TCP MSS value. For an IPv6 tunnel carrying IPv4 traffic, the system uses the IPv4 TCP MSS value. This upgrade aligns MSS adjustment with the traffic protocol and tunnel configuration, ensuring more accurate and efficient handling of traffic.	See the Configure TCP MSS and Clear Dont Fragment section.
The default OMP hold time is reduced to 300 seconds.	See the following sections for more details: Configure the OMP Holdtime Timers Timers

Behavior change	Description
When configuring Cisco SD-WAN Controller with multiple policy groups, you can see the tasks listed during the deployment.	Starting with Cisco Catalyst SD-WAN Manager Release 20.18.1, you can monitor the different tasks while configuring Cisco SD-WAN Controller with multiple policy groups.
Mandatory Tenant ID and VPN ID with Prefix address for **show sdwan omp routes** command.	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, and Cisco IOS XE Catalyst SD-WAN Release 17.12.5a, the **show sdwan omp routes** command requires you to specify both the tenant ID and VPN ID when using a prefix address.
Added **cluster-orchestrator** option to the **request nms** command	Added a **cluster-orchestrator** option to the **request nms** command. This enables you to start or stop the cluster-orchestrator service, which is a service that Cisco SD-WAN Manager uses to manage other services. See Operational Commands in the *Cisco Catalyst SD-WAN Command Reference*.
Updated the usage guidelines for **request interface-reset** command.	You can reset only WAN interfaces on Cisco IOS XE Catalyst SD-WAN devices. See Operational Commands in the *Cisco Catalyst SD-WAN Command Reference*.
New user credentials for Megaport account associations.	Use of User name and Password is deprecated from Cisco Catalyst SD-WAN Manager Release 20.18.1 .New Megaport account association authentication is via Customer key and Customer secret. If you upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1 and you already have associated Megaport accounts via User name and Password, the associations continue to work. To reauthenticate, you must use an API key and secret generated for the same account, as username and password authentication is not supported. For more information, see Associate a Megaport Account.
Two distinct icons in Cisco SD-WAN Manager to delete and disassociate a sub feature in configuration groups .	There are two distinct icons on Cisco SD-WAN Manager to delete and disassociate subfeatures. Use the trash icon to permanent delete the subfeature and use the broken link icon to disassociate the subfeature from the feature. You can view the disassociated features in the list view. For more information, see Delete a Subfeature.
Port Hop functionality deprecated.	The port hop functionality for the system port-hop field and interfaces port-hop field is deprecated. Instead, use the Full Port Hop field.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Resolved issues for 17.18.1a

Bug ID	Description
CSCwn26353	Dynamic IPv6 changes prevent BFD sessions via TLOC-Ext from coming up.
CSCwq11845	When you update the service firewall while an NWPI trace runs, the 17.15.2a cEdge-C8500 crashes.
CSCwp07901	C8500: CPP crashes while processing fragments of a jumbo frame.
CSCwm27749	The C8200 platform experiences a speed test download/throughput issue when it uses IPSEC ESP-NULL transform with Zscaler.
CSCwn12594	17.16 SIG Zscaler IPsec does not create VPN credentials for the primary tunnel.
CSCwo75657	Cisco IOS XE Catalyst SD-WAN device's maximum control connection does not equal its maximum OMP sessions.
CSCwp15042	You must perform a hardware slot reload to bring up the SFP-10G-T-X in the C-NIM-1X module.
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole.
CSCwp91064	A cero pointer dereference in FTMD leads to a crash.
CSCwo72675	[SITLite]: All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Open issues for 17.18.1a

Table 2. Open issues for Cisco Catalyst SD-WAN Control Components 17.18.1a

Bug ID	Description
CSCwo66099	Cisco IOS XE Catalyst SD-WAN device service side BFD flaps.
CSCwq65520	Cisco IOS XE Catalyst SD-WAN device is unable to clear zScaler location parameter without reload.
CSCwq55120	Unexpected reload due to IPv6 decapsulation.
CSCwq40026	Unexpected reboot due to process FTMD.
CSCwq56199	High memory usage: "IOSD ipc task" process's allocated is big and increasing, and Freed is insufficient.
CSCwq72772	Cisco IOS XE Catalyst SD-WAN device -FNF exporter is not sending

Bug ID	Description
	data packets when IPv6 collector is defined.
CSCwq73708	For MT environment, swapping to Cisco Catalyst SD-WAN Controller for a tenant is removing an entry from globaldbVSMARTTENANTMAPPINGNODE.
CSCwq74074	Router crashed due to 'Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)'
CSCwq72092	The expiry timer of DNS snoop agent cache entries is populated using the Time-To-Live of the A record.
CSCwq74430	Endpoint tracker flaps UP and Down when FQDN IP changed via DNS while the path is down.
CSCwq71229	Cisco IOS XE Catalyst SD-WAN device experienced an unexpected reboot after pushing policy group .
CSCwe19394	Cisco IOS XE Catalyst SD-WAN device may boot up into prev_packages.conf due to power outage.
CSCwp01089	EPFR-High latency times are observed on the hub device (Cisco Catalyst 8500-12X Edge Platform).
CSCwp12196	Cisco IOS XE Catalyst SD-WAN device unexpectedly reloads due to memory corruption on a notification queue in FTMD.
CSCwq27426	Cisco IOS XE Catalyst SD-WAN device: BFD session are down due to unencrypted outbound BFD packets despite active IPsec SA.
CSCwq60993	EM9293 module is not able to acquire GPS coordinates.
CSCwq58503	TCP Optimization Performance is poor if there are more than 2000 concurrent connections.
CSCwq68385	A link-down event disables TLOC- it does not automatically recover tunnels even after the link restores and TLOC state is up.
CSCwq60615	Device stuck in boot loop due to failure of vip_confd_startup_sh.

Compatibility

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix
- Hypervisor Compatibility Matrix for Cloud Routers
- Hypervisor Compatibility Matrix for Cisco Catalyst SD-WAN Control Components and vEdgeCloud
- For information about upgrade paths, see Upgrade Matrix Tool. (NEW)
- For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco SD-WAN Manager Cluster

Supported hardware

For information on device compatibility with Cisco Catalyst SD-WAN, see Cisco Catalyst SD-WAN Device Compatibility.
For information on system requirements for Cisco SD-WAN Validator server, vEdge Cloud router server, Cisco SD-WAN Manager server, and Cisco SD-WAN Controller server, see Recommended Computing Resources.

Related resources

API documentation

For information on Cisco SD-WAN Manager Release 20.16.x APIs, see Cisco SD-WAN Manager API.

Installation and upgrade

Software Installation and Upgrade for vEdge Routers

User documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Warranty and services

- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.

Legal information