Release Notes for Cisco Catalyst SD-WAN Control Components, Release 20.18.x

Cisco Catalyst SD-WAN Control Components Release, 20.18.x 3
New software features 3
Changes in behavior 14
Resolved issues 18
Open issues 28
Compatibility 34
Supported hardware 35
Related resources 35
Legal information 35

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst SD-WAN Control Components Release, 20.18.x

Cisco SD-WAN Control Components provide centralized management, policy enforcement, and secure connectivity for Cisco Catalyst SD-WAN deployments. This document includes release-specific information for all three components: Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, and Cisco SD-WAN.

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 20.18.1

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		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.
	Advisories	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

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		From Cisco Catalyst SD-WAN Control Components Release 20.18.1, you can schedule full OS and patch upgrades for Cisco SD-WAN control plane components (SD-WAN Manager, SD-WAN Validator, SD-WAN Controller) for a specific future date and time.
	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.
	Device version compliance in Cisco Catalyst SD-WAN Manager	The Device Version Compliance feature in Cisco SD-WAN Manager ensures device compatibility when upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1. The Cisco Catalyst SD-WAN Manager Release 20.18.1 supports devices up to N-2 long-lived releases and does not support older versions in the Cisco Catalyst SD-WAN overlay. This feature implements the following key aspects: • Upgrade Blocking: Prevents Cisco SD-WAN Manager upgrades through the user interface if the overlay contains devices with software versions older than N-2. • Post-Upgrade Notification: After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance banners and alarms. • Removal of End-of-Life (EOL) Platforms from ZTP Settings: Removes unsupported device families from the Zero Touch Provisioning settings page in Cisco SD-WAN Manager. • Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers Default Operating System Recognition: Changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system when they are added to and recognized by Cisco SD-WAN Manager. This change removes the Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers Migration menu when Cisco IOS XE operating system is detected.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
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 set up 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
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 Configuration Groups		
Hardware reliability	Cisco Secure Platforms support with configuration groups	From Cisco Catalyst SD-WAN Manager Release 20.18.1, these Cisco Secure Platforms are introduced and can only be configured using configuration groups. • C8151-G2 • C8161-G2 • C8355-G2 • C8231-E-G2 • C8235-E-G2
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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
	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
Ease of use	SD-AVC Troubleshooting alarm	The SD-AVC troubleshooting alarm is generated for out-of-sync information between the SD-AVC component and Cisco SD-WAN Manager. The information can relate to Protocol Packs, cloud-sourced applications, custom applications, or SaaS feeds. This alarm also indicates device alerts.
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 real-time monitoring	Configure and monitor ignition power and sensing capabilities of IR1800 routers using Cisco SD-WAN Manager. It prevents the router 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		

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
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.
Ease of use	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.
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

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		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
Cisco Catalyst SD-WAN Routing		
Software reliability	OSPFv3 IPSec Authentication	OSPFv3 authentication protects OSPFv3 routing payload with IPSec encryption and hashing. The solution is based on statically configured cryptographic keys that build on top of crypto map solutions. OSPFv3 is supported on service side and transport side.

What's new for Cisco Catalyst SD-WAN Control Components 17.18.2

Table 2. New software features for SD-WAN, Release 17.18.2

Product impact	Feature	Description
Ease of use	IPsec scale enhancement	From Cisco IOS XE Catalyst SD-WAN Release 17.18.2, the maximum supported SD-WAN IPsec tunnel scale for C8500 - 20X6C, C8570-G2, and C8550-G2 is 12,000 BFD sessions.
Cisco Catalyst SD-WAN Getting Started		

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of setup	TAC case access for AI Assistant in Cisco SD-WAN Manager	The AI Assistant now lets you open, view, and close technical assistance center (TAC) cases. The foundational infrastructure of AI Assistant is included in this release. As a cloud-delivered component of Cisco Catalyst SD-WAN Manager, AI Assistant's capabilities will continue to expand, providing even greater value for customers.
	Authentication for Cisco services	Cisco SD-WAN Manage registers for Cisco services using identity provider-based (IdP) authentication. The Cisco services registration page enables you to register for and authenticate multiple services at once.
Cisco Catalyst SD-WAN Policy Groups		
Ease of setup	IPv6 Rule and Rule Set Support in Security Policies	You can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager.
Cisco Catalyst SD WAN Routing		
Software reliability	OMP RIB-Out Optimization using TLOC Path	This feature introduces an optimization to the OMP protocol by flattening vRoute RIB-Outs from a per-TLOC (Transport Locator) basis to a per-SysIP (System IP) basis. This significantly reduces memory consumption on Cisco Catalyst SD-WAN Controllers, improves overall scalability, and enhances convergence performance in large-scale SD-WAN deployments.
Cisco Catalyst SD WAN Security		
Ease of use.	Cisco Identity Services Engine (ISE) integration with Cisco SD-WAN Manager	Cisco SD-WAN Manager serves as a central hub for the ISE system. It receives updates from the ISE servers and distribute those updates to Cisco SD-WAN Controllers and Cisco SD-WAN Analytics. Cisco SD-WAN Manager connects to ISE to retrieve identity data, such as IP-User Sessions and IP-SGT Bindings, and distributes it to Cisco SD-WAN Controllers to enable identity-based policy enforcement.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		This approach simplifies the architecture and improves management efficiency.
	DHCP high availability for Cisco IOS XE Catalyst SD-WAN devices	This feature introduces DHCP high availability for Cisco IOS XE Catalyst SD-WAN devices, to ensure continuous DHCP server operation on the LAN side. It utilizes an Active/Standby deployment model where two Cisco IOS XE Catalyst SD-WAN devices synchronize DHCP bindings (IP address records). This synchronization ensures that if the Active device fails, the Standby device seamlessly assumes the Active role, preserving IP address records and maintaining uninterrupted network service.
Ease of setup	Private Application Access	This integration allows Cisco Secure Routers and the Catalyst SD-WAN solution to automatically establish secure connections to Cisco Secure Access. Remote users in a hybrid work environment can seamlessly and securely access private applications located behind SD-WAN. Controlled Availability: Contact your Cisco account team before deploying this feature.
Cisco Catalyst SD WAN Systems Interfaces		
Ease of use	Extended Device Support for the Cisco ThousandEyes Agent to Industrial Routers	Support for the Cisco ThousandEyes Enterprise Agent is extended to include industrial routers in SD-WAN deployments.
Managing HSEC Licenses in Cisco Catalyst SD-WAN		
Licensing process	Support for managing HSEC licenses on rugged series routers	This feature enables you to install high security (HSEC) licenses on devices managed by Cisco SD-WAN Manager. An HSEC license is required to enable devices to support encrypted traffic throughput of 250 Mbps or higher.
Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources		
Upgrade	Support for the Nutanix hypervisor	Added support for using the Nutanix hypervisor for SD-WAN Control Components.

Resilient infrastructure

Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those

© 2026 Cisco and/or its affiliates. All rights reserved.

transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.

This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release.

- **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files. Recommendation: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.
- **SSHv1** Recommendation: Use SSHv2.
- **SNMPv1 and SNMPv2, or SNMPv3** without authentication and encryption recommendation: Use SNMPv3 with authentication and encryption (authPriv).
- **MD5** (authentication) and 3DES (encryption) in SNMPv3 Recommendation: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.
- **IP source routing based on IP header options** Recommendation: Do not use this legacy feature.
- **TLS 1.0 and TLS 1.1** Recommendation: Use TLS 1.2 or later.
- **TLS ciphers using SHA1** for digital signatures Recommendation: Use ciphers with SHA256 or stronger digital signatures.
- **HTTP** Recommendation: Use HTTPS.
- **Telnet** Recommendation: Use SSH for remote access.
- **FTP and TFTP** Recommendation: Use SFTP or HTTPS for file transfers.
- **On-Demand Routing (ODR)** Recommendation: Use a standard routing protocol in place of CDP-based routing information exchange.
- **BootP server** Recommendation: Use DHCP or secure boot features such as Secure ZTP.
- **TCP and UDP small servers** (echo, chargen, discard, daytime) Recommendation: Do not use these services on network devices.
- **IP finger** Recommendation: Do not use this protocol on network devices.
- **NTP control messages** Recommendation: Do not use this feature.
- **TACACS+** using pre-shared keys and MD5 Recommendation: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1.

Cisco is committed to supporting customers through this transition. Subsequent releases in the Cisco IOS XE 17.18 train will continue to support these features but will display warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes.

What's new for Cisco Catalyst SD-WAN Control Components 20.18.3

Product impact	Feature	Description
Cisco Catalyst SD-WAN Monitor and Maintain		
Software reliability	Live Protect for Cisco Catalyst SD-WAN	Live Protect validates security shields that protect Cisco products without

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		requiring device reloads or service interruptions. You can deploy security shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Protecting (Enforce) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the security shields enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed.

Changes in behavior

To view changes in behavior for 17.18.1, see Changes in 17.18.1

Changes for 20.18.1

Behavior change	Description
Cisco Catalyst SD-WAN Validator needs tunnel interface configured in VPN 0.	Refer to Create Configuration Templates for Cisco Catalyst SD-WAN Validator.
In custom role configuration for Role-Based Access Control (RBAC) using Configuration Goups, a **Change device variables** button is added in place of the **Deploy** button that allows you to modify device-specific values during the deploy process, before initiating the deployment.	Refer to the Edit Custom Role.
INFO Alarm for Missing Transceivers on Cisco Catalyst SD-WAN Devices	From Cisco SD-WAN version 20.18.x, an INFO alarm is displayed on Cisco Catalyst devices when a transceiver is missing, and the port remains in a NO shut state. This update reserves the alarm LED for critical issues, ensuring it is not triggered by non-critical conditions while maintaining operational visibility.
Manual save for configuration group updates.	Removed the auto-save feature from configuration groups and added a manual Save button. Also removed the Undo button, which was relevant for auto-save.
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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Behavior change	Description
Multitenancy support: Multitenant environments support integration with Cisco Secure Equipment Access (SEA) and third-party custom applications only at the tenant level.	Refer to the following sections for more details: Restrictions for Cisco Secure Equipment Access integration Restrictions for third-party custom application integration
Cisco Secure Equipment Access (SEA) and third-party custom application integration workflow changes.	Refer to the following sections for more details: Configure Cisco Secure Equipment Access integration, high level Configure third-party custom application integration, high level
The encapsulation command is optional while configuring a tunnel interface in Cisco Catalyst SD-WAN Validator.	Refer to Configure Cisco Catalyst SD-WAN Validator for more details.
The default OMP hold time is reduced to 300 seconds.	Refer to the following sections for more details: Configure the OMP Holdtime Timers Timers
You can disable weak SSH encryption algorithms for Cisco SD-WAN Validator and Cisco SD-WAN Controller.	Refer to the Information About Disabling Weak SSH Encryption Algorithms on Cisco SD-WAN Manager section.
Enable or disable Cisco SD-WAN Analytics.	Cisco SD-WAN Manager provides the option to enable or disable Cisco SD-WAN Analytics. For more information, refer to Enable or Disable Cloud Services.
In Cisco SD-WAN Manager, on the **Configuration > Configuration Catalog** page, the label for a column has changed from Origin to Source. In this column, Catalog indicates that a configuration group has been imported from a catalog and is read-only. You can edit configuration groups with User as the source.	Refer to Install a catalog entry for details.
The character limit for local user accounts remains restricted to 32 characters. However, for TACACS users, usernames extend up to 128 characters.	Refer to the Configuring Local Access for Users and User Groups section.
Third-party custom application images can be uploaded to SD-WAN Manager without activating Cisco IOx on devices.	Refer to Activate Cisco IOx on devices section for more details.
You can adjust the TCP Maximum Segment Size (MSS) even for a TCP packet encapsulated in an MPLS label. You can set the TCP MSS per the Path Maximum Transmission Unit (PMTU) with 30 bytes to account for Layer 2 headers, such as Ethernet, VLAN tags and MPLS headers.	Refer to the Information About Layer 2 VPN Support within the Cisco Catalyst SD-WAN Overlay Network.
Limitation for enabling Cloud Services.	While a Protocol Pack upgrade for devices in the network is in process, or is scheduled and pending, you cannot enable Cloud Services. Refer to Enable Cloud Services.
Disk Quota Checks at Admin Tech Generation and Image Upload.	Ensures disk space limits are not exceeded during admin tech generation and image uploads on Manager, with checks for disk usage across scenarios and nodes in a cluster. Refer to Information About Admin Tech for Collecting System Information..

© 2026 Cisco and/or its affiliates. All rights reserved.

Behavior change	Description
Certificate Expiration Dates	Cisco SD-WAN Manager uses epoch time for certificate expiration dates, ensuring time zone consistency. Refer to Information About Expired Certificate Indication and Quarantine.
Sequential Upgrade for Devices on the Same Site.	Upgrades within the same site are halted if a device fails, skipping subsequent devices. Refer to Software Upgrade in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.
CPU and Memory ranges in tooltips for Cisco IOS XE Catalyst SD-WAN Devices are accurately displayed on Cisco SD-WAN Manager.	View WAN Edge Health Pane for more details.
Log message for throttling throughput due to license entitlement	The Quick Connect workflow supports up to 500 devices at a time. Refer to Restrictions for Quick Connect workflow.
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.
Quick Connect workflow device limit.	The Quick Connect workflow supports up to 500 devices at a time. Refer to Restrictions for Quick Connect workflow.
The attachfeature API now requires the isEdited and isMasterEdited flags to be set to 'True' as appropriate when attaching a Device Template. Set isMasterEdited to 'True' for Master Template edits and isEdited to 'True' for Feature Template edits to ensure changes are correctly applied.	Refer to Feature Template for more details.
From SD-WAN Manager 20.18.1, custom applications are supported in multitenant environments.	Refer to Multitenancy.

Changes for 20.18.2

Behavior changes	Description
QoS actions like bandwidth, priority, random-detect, policing, and child-level shaping are supported and displayed in the statistics. Fair-queuing is not supported.	Refer to the Restrictions for QoS statistics section.
You can disable Cisco Catalyst SD-WAN Analytics directly from the Cisco SD-WAN Manager. This allows for self-service management of the SD-WAN Analytics feature without needing to contact TAC.	Refer to the Information About Converged Dashboard section.
A Skip configuration button has been added to the quick connect workflow.	Earlier, customers would need to enter required information like Hostname, System-IP, Site Name in order to onboard a device. From 20.18.2, users can directly onboard a device without needing to enter the same information, by using the Skip configuration button. Access the quick connect workflow

© 2026 Cisco and/or its affiliates. All rights reserved.

Behavior changes	Description
When importing or exporting CSV files in the Quick Connect workflow, the Site column now uses Site Name instead of Site ID.	Refer to Access the Quick Connect Workflow.
You can configure DNS settings either in common control component settings or device-specific settings; device-specific DNS settings override common settings when configured, otherwise common settings apply.	Refer to the Common Control Component Network Settings section.
To display the Identity Manager status for its connections to SD-WAN Manager, use the **show idmgr status** command.	Refer to the show idmgr status command.
Supported Characters in Variable Values	Semicolons (;) are not supported in variable values. To separate multiple CLI lines, use the newline character (\n) instead.

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 20.18.1

Bug ID	Description
CSCwd58323	Cisco SD-WAN Manager Azure AD SSO maxAuthenticationAge is fixed at 7200 seconds
CSCwm14592	Cisco SD-WAN Manager UI Password create or update
CSCwm45553	Time format was changing in API body in Cisco SD-WAN Manager in 20.14/20.15
CSCwp12663	No restrictions have been applied to upload files under diagnostic log capture.
CSCwm83954	Unable to enter AS-Path list longer than 32 characters
CSCwm92001	Underlay Measurement and Tracing Services modelling is not correct
CSCwm97086	Configuration Group: deleted feature parcel remains in list view
CSCwn04371	Neo4j does not remove DR Cisco SD-WAN Manager chassis-id once DR configuration is removed
CSCwn18532	Cisco SD-WAN Manager - Configuration Group service profile: Switchport is not responding
CSCwn24493	Unable to update edited copied feature template **Default_BootStrap_Cisco_System_Template** on Cisco SD-WAN Manager

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwn26880	When using cli based centralized policy, config-db doesn't remove commented lines from the config
CSCwn33483	Policy Group Deployment: ambiguous **Failed to deploy device with Policy Group** error message
CSCwn34053	Need to include pointers on the configurations to add Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller in Cisco SD-WAN Manager UI
CSCwn41014	Enabling **Per-tunnel QoS Aggregator** on cellular interface results in error on preview
CSCwn51488	Multiple active userSessions exist on Cisco SD-WAN Manager even after controller upgrade transaction completes
CSCwn51590	Error not handled in UI - Invalid TG API Key generates no UI error
CSCwn55852	**NullPointerException** error seen if a CSG with port-channel is configured with a PG with Zscaler
CSCwn56891	**show alarm history** gives exception ValueError(" time data %r does not match format %r")
CSCwn61388	A space is required for custom application defined in IPv4
CSCwn69650	Follow up on Lodash upgrade
CSCwn75393	Tunnel Configuration on GRE (or IPSec) Profile parcel under the Service VPN Parcel cannot be changed
CSCwn81322	SSO Single Logout is not working
CSCwn81610	Local user with expired password is redirected to SSO Login
CSCwn88445	Cisco SD-WAN Manager does not generate **snmp-server trap-source Port-channel xx** configuration using feature template
CSCwn96141	Cisco SD-WAN Manager configuration-group template incorrectly sets interface MTU and IP MTU on 40G interfaces.
CSCwn96853	Cisco SD-WAN Manager role access issues to Monitor > Devices > Troubleshooting
CSCwo00101	Cisco SD-WAN Manager 20.16.1 : cannot use custom port for alarm email notification.
CSCwo12125	SD-WAN Validator restarts due to " got signal 11"
CSCwo20628	API call to /dataservice/device/reachable returns empty[]
CSCwo26043	MT Cisco SD-WAN Manager: tenant admin is unable to modify an alarm notification rule
CSCwo32490	Fabricated Reboot Event is generated after Control Connection Flap

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwo32576	Unified Security Policy -Ruleset causing deployment failure due to object or group not configured.
CSCwo44239	Dropdown for Service Chain in Policy Configuration does not display any of the configured Service Chain
CSCwo45368	Include email in subject, not SAN, in Cisco SD-WAN Manager Web Server Certifcate CSR
CSCwo52495	Cisco SD-WAN Manager gives error **Input Json Payload validation failed** for service chain
CSCwo52922	License not found in Cisco SD-WAN Manager DB although it is present
CSCwo72101	Port List in Manager GUI doesn't allow adding ports higher than 65530
CSCwo76533	Configuring VPN Interface T1/E1/Serial template, the interface name cannot be defined as a variable
CSCwo93942	Facing multiple issues under Alarm UI in monitoring tab.
CSCwp12653	Unable to display interface details. Diagnostic log capture failed.
CSCwo96831	Unable to schedule upgrade for devices using later/now.
CSCwo99545	Error retrieving: ('Connection aborted.', RemoteDisconnected('Remote end closed connection without response'))
CSCwp02180	Object groups cannot be referenced under Cisco SD-WAN Manager Configuration -> Security -> Define Lists -> Rule Set after an upgrade
CSCwp11066	Cisco SD-WAN Manager reloads due to ConfD got signal 9 due to clickhouse memory exhaustion
CSCwp11220	Cisco SD-WAN Manager 20.15.3 does not decrypt type 6 password for TACACS+ server using CLI Template
CSCwp18519	Experiencing issues with Cisco SD-WAN Manager RBAC (Role-Based Access Control) permissions related to Configuration Groups, Feature Profiles, and Policy Groups.
CSCwp28358	Cisco SD-WAN Manager: Alarms do not get generated even though event is generated.
CSCwp32081	Cisco SD-WAN Manager Configuration Groups -> System -> OMP -> ecmp limit should show error if above threshold
CSCwp32515	Cisco SD-WAN Manager: Alarm filter with STATE(Active/Cleared) not available in 20.12 release
CSCwp38011	Support replication of File System Data as part of DR

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwp38115	OMP Graceful Restart timer default value is set to 120 for Cisco Catalyst 8000V Azure Template
CSCwp55823	Configuration Group variables removed when unassigned device is deployed and then removed
CSCwp65998	Rate limit value for URL non bulk api will be reset to default 100 after reboot in 20.12 / 20.15
CSCwp83222	Cisco SD-WAN Manager: IP Route realtime table does not display multiple next-hop entries for ECMP routes
CSCwp85929	Cisco SD-WAN Controller: Changing sequence of the rules in centralized policy causes mis programming.
CSCwp87365	Data Prefix validation does not work.
CSCwp97237	20.12.4.1 - If one IDP enabled and one IDP is disabled, it causes an Internal Server Error
CSCwp98827	Embedded Security Rules fail to load due to high number of service profiles
CSCwp99414	Post DR switchover, certificate workflow cannot reach Cisco Catalyst SD-WAN Validator
CSCwq15493	Group of Interests, including the pre-defined ones, get deleted. by CISCO
CSCwq23889	attachfeature API does not process devices when multiple entries share the same **templateId** in **deviceTemplateList**
CSCwq27461	Cisco SD-WAN Manager: Unable to reorder application priority & SLA rules using sequence dropdown
CSCwq28772	On Cisco SD-WAN Manager 20.15.3 **preferred remote color restrict** does not work in UX2.0
CSCwq61556	Validation checks are failing while onboarding the Catalyst 8000 vEdge to the Manager device.
CSCwp14077	Unable to load the view details for security events details in security dashboard.
CSCwp84371	Unwanted error popup for adding new profile.

Resolved issues for 20.18.2

Bug ID	Description
CSCWq21361	vManage GUI upgrade from 20.15.2 to 20.15.3 fails, need to perform the CLI upgrade
CSCWq57458	Upgrade Coordinator Reports Success Even When it Fails to Clear MW Flag

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCWq69370	Unable to load vManage UI due to excessive size of Angular module files
CSCWq74763	vManage timeouts while actively working in vmanage
CSCWq84033	Incorrect Disk Space Recommendation for Controller and Validator OVAs in Release 20.16.x and 20.18.x
CSCWq86617	High CPU Utilization on Neo4j Leader Node Triggered by Network Rediscovery
CSCWq98192	vmanage high CPU utilization because of vdaemon-message processes leaking on socket 'CLOSE_WAIT'
CSCWr06729	vManage | Unable to push template due to device duplicate entry
CSCWr14063	vDaemon process crashes when trying to parse vmanage-system-ip
CSCWr85293	Topology Hub and Spoke not getting deployed|| failed Not able to find config-group
CSCWq56333	Policy Preview Fails with 'Duplicate Mapping' Error due to UI/Backend Race Condition
CSCWq57146	There is no button to block the https service in the Dialer feature template
CSCWq61950	Vmanage is not allowing to configure 0.0.0.0/0 le 32 ge 32 as a prefix list within groups of interest (policy groups)
CSCWq65340	vManage | 20.12.5 | Incorrect behavior in cancelling a change to Centralized Policy after " Topology" is added
CSCWq68126	IPV4-Device-Access-Policy Sequences not displayed in Firefox browser.
CSCWq70818	ip source-route' enabled unexpectedly after pushing config group
CSCWq84802	Not possible to add more than 2000 characters on a Prefix List inside Configuration > Configuration Groups > Policy Profile > Add New Feature > Prefix, in Manager version 20.15.3.1
CSCWq84823	vManage Remote Repo: cEdge software download fails with " Image Repository Access Check: Failed to recv file"
CSCWq86700	Centralized Policy page not loading up - 20.12.5
CSCWq97540	IPv4 Route not installed after upgrade in AWS with IPv4/IPv6 Dual Stack enabled resulting in failed upgrade
CSCWr00709	Configuring PPPOE using config group is limiting number of char for usernames to 32 char
CSCWr13670	API returns 204 for configuration group that was deleted

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCWr14030	Post DR switchover, some SD-WAN Validators unable to connect to new active cluster
CSCWr37975	vManage - RADIUS or TACACS VPN ID variable doesn't exist in AAA profile
CSCWr61736	Centralized policy taking too long to load.

Resolved issues for 20.18.2.1

Bug ID	Description
CSCws33583	Cisco Catalyst SD-WAN Manager information disclosure vulnerability.
CSCws33584	Cisco Catalyst SD-WAN Manager arbitrary file overwrite vulnerability.
CSCws33586	Cisco Catalyst SD-WAN Manager arbitrary file overwrite vulnerability.
CSCws93470	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.
CSCws52722	Cisco Catalyst SD-WAN Controller authentication bypass vulnerability.

Resolved issues for 20.18.2.2

Bug ID	Description
CSCwt50498	Cisco Catalyst SD-WAN Controller authentication bypass vulnerability.
CSCwt38739	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.
CSCwt55544	Cisco Catalyst SD-WAN Manager XML external entity injection vulnerability.
CSCwt38767	Cisco Catalyst SD-WAN Manager privilege escalation vulnerability.

Resolved issues for 20.18.2.3

Bug ID	Description
CSCws79979	Disaster recovery configuration fails in SD-WAN Manager standalone with 400 Bad Request due to replication interval parsing error.
CSCwt40948	Memory corruption with inbound policy + show omp routes CLI.
CSCwr88750	SD-WAN Manager generates guest-ipaddress and VirtualPortGroup ip adress from different subnets.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt12783	VTY IPv6 access list rejects all SSH traffic in VRF for SD-WAN cEdges.
CSCws68934	Network Hierarchy for MRF does not show associated devices when selecting single site.
CSCwt02491	Unable to upgrade Arbitrator from 20.15 to 20.18 due to stats migration check.
CSCwt49861	SD-WAN Manager - zScaler SSE - device specific option is missing.
CSCws24275	Unable to deploy Configuration Group when its site type is " Dual Router" .
CSCws38767	SD-WAN Manager triggers false alarms indicating High /tmp directory usage despite it being low.
CSCws94878	View / edit the topology policy with 250 rules causes the UI to hang.
CSCws94132	Unable to sync SA for users.
CSCwr96258	TACACS Secret Key is showed in plain text in SD-WAN Manager syslog even when template is pushing as encrypted.
CSCwt26594	Add Custom Applications button in Discovered Applications tab does NOT work.
CSCwr87014	Cisco Catalyst IOS XE device missing " tunnel mode ipsec ipv4" after deploying policy group.
CSCwr87767	After upgrade to 20.15.4 the ifDescr mib (OID 1.3.6.1.2.1.2.2.1.2) is providing incorrect interface name.
CSCws03309	Verification failed- After upgrade, updating Smart account username on license management fails.
CSCwt40320	GUI fails to load properly for SD-WAN Manager node due to 429 rate limits seen.
CSCws49871	Unable to select more than 100 devices from workflow > Quick Connect > Sync your device inventory.
CSCwq80027	Unable to create new prefix list from route policy parcel in CG in MT SD-WAN Manager setup.
CSCwq48395	SDWAN Controller has stuck exported routes after policy change.
CSCwr51442	Report-link utilization fails
CSCws93417	SD-WAN Manager MFA integration with DUO now requires API calls use Python version 5.5.0.
CSCwr79876	SD-WAN Manager removes NAT bypass from policy group.
CSCwt36429	SD-WAN Manager UI slowness.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr57474	SD-WAN Manager is unable to sync license with offline file, GUI shows " Smart Account licenses synced" while SD-WAN Manager-server logs through errors " Exception - java.lang.Exception: " Error while creating SA VA node:[Ljava.lang.StackTraceElement.
CSCwr75344	Redirect-dns umbrella configuration missing after saving Application Priority & SLA changes in Policy Groups.
CSCws75823	Licensing overview page not updated to exclude perpetual licenses.
CSCwr33423	SD-WAN: Static NAT Entry Limitation in Firewall HA Service Profile.
CSCws94961	SD-WAN Manager bootstrap configuration generate ip host configuration which is ignored by device.
CSCws70210	Cannot edit or delete local users Cisco SD-WAN Manager.
CSCwq14387	Configuration group lost variable values.
CSCwr92492	ISR1100 and CG522 quick connect workflow doesn't go through completely.
CSCwt73216	Usernames can include the special character “@”.
CSCws65191	SSO Single Logout not working on Chrome and Edge but works fine on Firefox browser.
CSCwt16575	License assignment failure for mixed platform-class device selection in SD-WAN Controller Mode.
CSCwq37648	UC upgrade is not working when there are special characters in the neo4j password.
CSCwt62820	SD-WAN Manager monitoring Interface utilization graphs shows in 'k kbps' instead of 'mbps' unit notation.
CSCws36801	MT upgrade fails due to application-server failure.
CSCws52923	The username cannot be created with the period - " ." : Name should not start with a number, characters (except underscore, hyphen) and uppercase not allowed.
CSCwp27018	Aggregation for BFD Summary wrong for Full BFD connectivity:Not considering any site having ENCS and SDWAN Device.
CSCwt68746	Unable to configure send-path-limit on Cat SDWAN Controller from Configuration > Control Components Settings.
CSCws44011	Controller and Validator upgrade should fail if they are being upgraded to a higher release than SD-WAN Manager.
CSCwt06042	Save option is not available after modifying the parameters in Prisma tunnel configuration.
CSCwr07079	Crash file generated on SD-WAN Manager and GUI became unreachable for sometime.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt07060	Controller fails to push preferred-color-group-options to the device if the preferred-color-group reference is modified in policy.
CSCws60895	DR seeing issues after registration on cluster setup.
CSCwt27474	The hardcoding of the AS number 64512 needs to be removed and changed to autodetect.
CSCws66278	Unable to install Cisco PKI controller certs on MT overlay.
CSCwr94642	Failed policy group push leads to Controller out of sync.
CSCwt44817	Adding SD-Routing devices will fail in quick connect workflow.
CSCwr73205	Omp_ro_opt: Assert @ cfgmgr - vconfd_sub_cb with threadid as optimized out.
CSCws11167	IPv6 Routes cannot be advertised to OMP using a Device Specific Route Policy inside an SD-WAN Manager VPN Feature Template.
CSCwq56228	Datastore corruption causes coordination server to restart continuously.
CSCws46075	Missing TLOC_UP alarm from SD-WAN Manager.
CSCws05835	Topology Group creation fails with the reason " Feature Profile failed" at first attempt.
CSCwt78921	SD-WAN Manager: Random Forbidden Request: API calls may fail with HTTP error 403.
CSCwq29080	Newly created Group of Interest not visible in configuration-group policy.
CSCwr47582	SD-WAN Manager: Neo4j OOM seen on the first replication after DR is registered.
CSCwt25808	Misalignment and incorrect time format in exported csv for wanedge under software upgrade.
CSCws09295	On SD-WAN Manager, copying a Security → Lists → Rule Set does not work.
CSCwp00753	Collapsible common banners for > 2 banners.
CSCws33783	Unable to create/edit the allow/block URL list [Objects and Profiles -> Security Profiles -> URL Filtering -> Advanced].
CSCwq10559	Network Hierarchy Page Unavailable Due to Missing SD-WAN Controllers in User Scope.
CSCws99348	UC- post activation commit failed and rollback also failed.
CSCwr55335	Configuration preview fails with error " Invalid Format Attributes" when LAN vpn id is configured as a device variable.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt19263	After performing an upgrade, the 'Upload WAN Edge List' function does not work when using a role-based user account.
CSCwt00896	GUI tasks fail due to app-server not connecting to Vault service.
CSCws91077	When selecting Area for Match Sites hitting NPE.
CSCwq79825	Errors encountered when applying new Policy Group due to PSK issues on SIG tunnels due to restriction ';' character.
CSCwr43054	Unreachable Cisco Catalyst IOS XE device invalidate and delete causes the SD-WAN Manager-system ip to persist on device causing mismatch and re-onboarding issue.
CSCwt54915	Stale sshd_config in RW filesystem cause:DeviceEventListener NETCONF client creation failed post 20.18 activation-Pre-check to be implemented in UC.
CSCwo62038	SD-WAN Manager SSO with Azure: Incorrect Resource/Scope Assignment for Remote Users.
CSCwp03901	SD-WAN Manager SSO Login fail with F5 APM IDP.
CSCwp35976	Intermittent login issues on devices with aaa accounting enabled.
CSCwt97004	When adding match site in topology (policy group) and searching for a site and tick, not only the site is selected. global will be selected (all other sites).
CSCwt40951	Cisco Catalyst SD-WAN Controller crash during admin-tech collection.
CSCwr74862	Two routers with the same Site IDs on two different policy groups.
CSCwt97799	Configuration-group CLI generation fails with duplicate tracker ID when the same tracker group is reused across multiple VRRP-enabled service VPN interfaces.
CSCws66441	Notification rule matching fails due to incorrect query generation with OR conditions.
CSCwt97874	SD-WAN Manager crashed with reason of vdaemon-x got signal 11.
CSCws91663	Multiple topology group bugs when selecting Folders, inconsistent behaviors, lack of diagnostic error messages.
CSCwq97113	SD-WAN Manager on-prem: Daily backups are wiped from SD-WAN Manager disk.
CSCwo44963	After enabling the debugs, cannot directly disable the debugs from device running Viptela OS.
CSCws02678	Tunnel Stats are Not being Converted to Site Health Summary.
CSCwt91646	After upgrading SD-WAN Manager delete the non-active virtual images together doesn’t work : " only one is deleted" .

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu08266	During Controller certificate installation, Netconf failure shouldn't update the SD-WAN Manager database without verifying Controller certificate.

Resolved issues for 20.18.3.1

Bug ID	Description
CSCwu18563	Cisco Catalyst SD-WAN Controller Authenticated Privilege Escalation Vulnerability

Resolved issues for 20.18.4

Bug ID	Description
CSCwt97002	Upgrading the Cisco Catalyst SD-WAN Manager to 20.15.5 triggers a MEMORY_LIMIT_EXCEEDED exception in the olap-db.
CSCws91663	Selecting folders causes multiple topology group bugs, inconsistent behaviors, and a lack of diagnostic error messages.
CSCwv05945	The ThousandEyes workflow fails because the thousand_eyes_token.value does not match the regex pattern ^[0-9a-z]{32}$.
CSCws83671	Following the MT cluster upgrade from 20.15.306 to 20.15.403, the Cisco Catalyst SD-WAN Manager and the Cisco Catalyst SD-WAN Validator lose device serial numbers.
CSCwt97004	Searching for and selecting a site within a topology policy group incorrectly selects all other sites globally.
CSCwr51442	The system fails to report link utilization in version 26.1.999-4821.
CSCwt87655	The Cisco Catalyst SD-WAN Manager fails to authenticate with TACACS on the VPN 512 loopback after the upgrade to 20.15.5.
CSCwt02221	The system produces inconsistent policy compilations for the CoR SaaS sequence.
CSCws93417	The Cisco Catalyst SD-WAN Manager MFA integration with DUO now requires API calls to use Python version 5.5.0.
CSCwu76358	Existing and new Cisco Catalyst SD-WAN Manager alarm notifications disappear after the upgrade to 20.18.3.
CSCwt00896	GUI tasks fail because the application server cannot connect to the Vault service.
CSCwu19341	Blocked NotificationsConsumer workers prevent the Cisco Catalyst SD-WAN Manager from sending webhook notifications, which causes webhook executor queue saturation and task rejection.
CSCwu83609	The Cisco Catalyst SD-WAN Manager (versions 20.18.3 and 20.18.3.1) fails to save BGP route-policies that include a sequence with an " accept" action.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt62820	The Cisco Catalyst SD-WAN Manager displays interface utilization graphs in 'k kbps' instead of 'mbps' unit notation.
CSCws99393	Navigating the topology page causes the Inbound and Outbound site entries to disappear.
CSCwp03901	The Cisco Catalyst SD-WAN Manager fails to perform SSO login with F5 APM IDP.
CSCwt40320	429 rate limits prevent the Cisco Catalyst SD-WAN Manager GUI from loading properly.
CSCwu08266	A NETCONF failure during the Cisco Catalyst SD-WAN Controller certificate installation should not update the Cisco Catalyst SD-WAN Manager database before the system verifies the Cisco Catalyst SD-WAN Controller certificate.

Resolved issues for 20.18.4.1

Bug ID	Description
CSCww79570	Cisco Catalyst SD-WAN Manager API authentication bypass vulnerability.

Resolved issues for 20.18.5

Bug ID	Description
CSCwv07438	Quick Enable On Demand Troubleshooting displays the full Moment.js object JSON in the Data Backfill.
CSCwt99082	A container manager failure interrupts the Cisco Catalyst SD-WAN Manager upgrade process.
CSCww07892	Cflowd Centralized Policy fails to save or activate when you use a subinterface as the collector source interface.
CSCwv91041	Removing the admin user from the internal NACM netadmin group triggers a configuration manager crash in all cluster nodes.
CSCwv87005	Offline Smart Licensing loses license assignments when you upload a new sync file after communication starts.
CSCwv37287	The CDCS MT upgrade fails during activation.
CSCww42552	A race condition occurs during the second base-config exchange with a Cisco Catalyst SD-WAN Edge device in the Cisco Catalyst SD-WAN Manager.
CSCwv68062	Configuration Group deployment fails after you import device-specific configuration containing an encrypted BGP neighbor password.
CSCwt80633	Removing the set preference in the route leaking sequence via control policy causes misprogramming in the Cisco Catalyst SD-WAN Controller.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCww06973	Redesigning OMP readiness timeouts on a few edge peers rolls back the entire centralized policy deployment.
CSCwu17151	Multitenant Cisco Catalyst SD-WAN Manager CPU graphs display discrepancies.
CSCww56326	Adding a site in a UX 2.0 configuration group deployment creates a new site list.
CSCwv84273	Other tenant serial numbers leak when you enable multi-tenant and there are conflicting IP addresses.
CSCws44162	Several services fail to run or enable after you upgrade from 20.15 to 26.1.
CSCwt71863	A long interval of Disaster Recovery in a pause state causes large files to write to the disk from the last successful replication.
CSCwq37551	FQDN Syslog configuration fails to apply through the Cisco Catalyst SD-WAN Manager.
CSCwv06053	You cannot modify the AAA authentication order in the Cisco Catalyst SD-WAN Edge and Cisco Catalyst SD-WAN Controller feature templates.
CSCww10934	The Cisco Catalyst SD-WAN Manager fails the centralized-policy CLI preview when the Cflowd source interface uses a lowercase loopback name.
CSCwt51589	Cisco IOS-XE edge devices fail to sync the root certificate after you upgrade from 20.9.8 to 20.15.4.2.
CSCwu77155	The policy edit process removes all match policy object sequences if any policy object GET API errors out or times out.
CSCwu17506	You cannot add new devices via serial file upload because the internal management IP address pool is exhausted.
CSCwt53078	You encounter issues with individual configuration settings for OSPFv3 in a configuration group within the Cisco Catalyst SD-WAN Manager.
CSCws30298	A lock for the template type policy definition fails to acquire when you modify an AAR policy in the Cisco Catalyst SD-WAN Manager.
CSCws35953	The Cisco Catalyst SD-WAN Manager displays duplicate devices in custom roles.
CSCwu59830	Configuration preview fails when you do not provide a value to more than one optional static or default route in the service profile.
CSCws32376	The daemon crashes in the Cisco Catalyst SD-WAN Controller after you create or place a tenant.
CSCww19672	You can now request the removal of restrictions for special characters like at symbols and ampersands in organization names.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu09062	The Neo4j user password fails to update when the username and password contain special characters.
CSCwv33920	The Cisco Catalyst SD-WAN Manager displays the same variable more than once in policy groups and CLI configuration groups.
CSCwt49973	You encounter errors during the CLI preview when you attempt to configure dual-router high availability from the Cisco Catalyst SD-WAN Manager.
CSCws67054	The TLOC chart on the device page fails to display data.
CSCwv25542	The Cisco Catalyst SD-WAN Manager only shows 25 devices when you have more than 25 devices that report version mismatch or version incompliance.
CSCwt44516	The auto-generated zone name in the NGFW fails to follow 32-character constraints.
CSCwv17046	The policy group UI displays a device list from a different policy group until you refresh the page.
CSCwu93858	The DCA fails to send any monitoring files when the Cisco Hosted setting is false.
CSCwv57173	The controller upgrade fails for the multi-tenant topology.
CSCwu49012	You encounter an internal error when you create or fetch a storage account during Azure CGW creation.
CSCwu02280	ThousandEyes Enterprise Agent configuration remains unsupported on C8500-20X6C devices via configuration groups.
CSCwv98654	The edge remains reachable through control connections but not through the Cisco Catalyst SD-WAN Manager UI on multitenant setups.
CSCwv43223	Cellular links report incorrect bandwidth usage.
CSCwu00420	You receive a VLAN ID not found error during NGFW policy group deployment with zone security on the Cisco Catalyst SD-WAN Manager.
CSCwv89588	Editing a centralized policy fails with an error indicating that the policy contains an invalid control or local sequence.
CSCwt49418	Any editing of the policy disables the fallback to routing option for the catch-all rule.
CSCwt18938	You encounter errors when applying a new policy group due to PSK issues on SIG tunnels caused by the semicolon character restriction.
CSCwv38668	REST API calls and the Cisco Catalyst SD-WAN Manager GUI display only 5 OMP routes instead of the full route set visible in the Cisco Catalyst SD-WAN Controller CLI.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwq61556	Validation checks for onboarding the C8KV to the manager device fail.
CSCws82756	A NAT mapping-ID conflict occurs during HA configuration deployment.
CSCwt79278	TLOC lists disappear from a policy group after you save the policy.
CSCws45978	A policy or topology group push fails due to an unreferenced VPN profile error.
CSCwu24260	The Cisco Catalyst SD-WAN Validator debug logs flood with failed to send the DTLS packet IPC errors.
CSCwq32633	The RSA-4K-CSR option appears greyed out on the validator or controller on release 20.15.3.
CSCws37849	You cannot generate a web server certificate CSR with a wildcard SAN DNS name.
CSCwt68160	Single device configuration group variable values are lost when you disassociate a device in UX 2.0.
CSCws15644	The Cisco Catalyst SD-WAN Manager disaster recovery control connection drops after failover when managers are signed by Cisco PKI.
CSCwu50939	Variables fail to update or the security policy fails to edit.
CSCwv36012	Unable to push the umbrella secret or token while pushing the Unified policy.

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 20.18.1

Table 3. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.1

Bug ID	Description
CSCwq91481	DR: Scale configuration causes neo4j to crash and restart in secondary when deleting & importing SYSTEMDEVICESNODE
CSCwq21361	Cisco SD-WAN Manager GUI upgrade from 20.15.2 to 20.15.3 fails, need to perform the CLI upgrade
CSCwq54162	Unable to copy or import several configuration groups with System, Transport, Management profile.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwq33835	DR replication fails with large configuration - Neo4j OOM on standby

Open issues for 20.18.2

Table 4. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.2

Bug ID	Description
CSCwr42574	Megaport ICGWs are stuck in LIVE state with CG being in OUT of Sync after connection creation
CSCwr44657	SD-Routing-SIT : Cli config group attaching is failing due to XML character (Unicode: 0x8)
CSCwr47027	Remove all traces of embargo from logging and other tracing mechanisms.
CSCwr47582	vManage 20.18.2 Neo4j OOM seen on the first replication after DR is registered.
CSCwr73205	omp_ro_opt : Assert @ cfgmgr - vconfd_sub_cb with threadid as optimized out
CSCwr94748	26.1 SD-Routing: PG re-deploy failed with previous deployed successful rule having IPv6 data prefixes
CSCwr98987	20.18: OMPD process crashed on Cisco Catalyst SD-WAN Controller.
CSCwp35976	Intermittent login issues on Viptela devices with AAA accounting enabled.
CSCwr31886	Quick Connect - Failed to authenticate Smart Account credentials. - Unexpected char.
CSCwr49368	SSE Tunnels with Cisco Secure Access are stuck in SD-WAN Configuration Database

Open issues for 20.18.2

There are no open bugs for this release.

Open issues for 20.18.2.1

Table 5. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.2.1

Bug ID	Description
CSCwt40948	Memory corruption with inbound policy + show omp routes CLI.

Open issues for 20.18.2.2

There are no open bugs for this release.

© 2026 Cisco and/or its affiliates. All rights reserved.

Open issues for 20.18.3

Table 6. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.3

Bug ID	Description
CSCws94961	SD-WAN Manager bootstrap configuration generates IP host configuration which is ignored by device.
CSCws83671	After the MT cluster upgrade, SD-WAN Manager and Validator lose the device serial.
CSCwj13394	SD-WAN Manager flushes active user sessions within 10 minutes of login, causing abrupt UI logouts.
CSCwh81860	Transport interface parcel with the default " Auto negotiate" option fails on C8500L-8S4X platforms.
CSCws04241	SD-WAN Manager experiences high CPU and memory utilization due to SD-WAN Analytics.
CSCwm26607	SD-WAN Manager removes the NAT egress-interface option from the Device configuration.
CSCvr12395	SD-WAN Manager pushes " media-type rj45" while configuring duplex on ISR1k.
CSCwq57801	SD-WAN routing becomes inconsistent when the same MPLS label is allocated to both VPN 10 and VPN 65528 (SIG VPN), as identified through NWPI insights during EFT.
CSCvp11416	Cisco Catalyst IOS XE device template attachment fails on a device when a central policy with Cflowd is activated.
CSCwt40661	Cluster-oracle terminates after reboot.
CSCvu53340	Template push fails because SD-WAN Manager tries to disable link recovery for the cellular controller.

Open issues for 20.18.4

Table 7. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.4

Bug ID	Description
CSCwv80117	Software edge devices renew certificates signed by the Cisco Catalyst SD-WAN Manager..

Open issues for 20.18.4.1

There are no open bugs for this release.

Open issues for 20.18.5

Table 8. Open issues for Cisco Catalyst SD-WAN Control Components 20.18.5

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv75389	27.1 Controller upgrade preparation fails with an NPE in EventManager.shutdown while setting the maintenance-window flag.

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, 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.

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

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)

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 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.

© 2026 Cisco Systems, Inc. All rights reserved.