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

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Upgrade	Log files cleanup during software upgrade	The Cisco IOS-XE software upgrade has been improved to clean outdated files from flash before upgrade.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. 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 17.18.1, see Changes in 17.18.1

Changes for 20.18.1

Behavior change	Description
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.	See 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.

Behavior change	Description
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.
Multitenancy support: Multitenant environments support integration with Cisco Secure Equipment Access (SEA) and third-party custom applications only at the tenant level.	See 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.	See 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.	See Configure Cisco Catalyst SD-WAN Validator for more details.
The default OMP hold time is reduced to 300 seconds.	See 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.	See 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, see 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.	See 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.	See 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.	See 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.	See 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. See Enable Cloud Services.

Behavior change	Description
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. See Information About Admin Tech for Collecting System Information..
Certificate Expiration Dates	Cisco SD-WAN Manager uses epoch time for certificate expiration dates, ensuring time zone consistency. See 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. See 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. See 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. See 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.	See Feature Template for more details.

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

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.

Bug ID	Description
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
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 >

Bug ID	Description
	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
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.

Bug ID	Description
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
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.

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

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

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

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.