Release Notes for Cisco Catalyst SD-WAN, Release 26.2.x

Cisco Catalyst SD-WAN Release, 26.1.x 3
New software features 3
Changes in behavior 6
Resolved issues 9
Open issues 17
Compatibility 19
Supported hardware 19
Related resources 19
Legal information 19

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst SD-WAN Release, 26.2.x

Cisco Catalyst SD-WAN Release 26.2.1 strengthens security and infrastructure resilience while improving high availability, operational visibility, and ease of network management.

- **Security & resilience:** Introduced secure-by-default enhancements across Cisco IOS XE, including disabled Proxy ARP by default, stronger password-hashing controls, warnings for insecure protocols, and real-time visibility into insecure services. The release also adds Secure Router NGFW, IKEv2 support, and post-quantum encryption options.
- **High Availability & reliability:** Added a resilient SD-WAN data plane that maintains IKEv2/IPsec tunnels and per-VRF BGP routing during extended SD-WAN control-component outages. Safety barrier enhancements and packet-order preservation during tunnel underlay reassembly further help prevent system failures and maintain traffic integrity.
- **Monitoring & troubleshooting:** Expanded operational visibility with upgrade pre-check and Link SLA Change reports, filter support across alarm and event heatmaps, sub-interface statistics, enhanced admin-tech logging, and FQDN support for High Speed Logging and external syslog servers.
- **Network intelligence & connectivity:** Enhanced NBAR with recognition for key Operational Technology protocols, including DNP3, IEC104, MMS, NTCIP, and OPC-UA. IPv6 day-0 onboarding now supports DHCPv6 prefix delegation alongside stateful DHCPv6 and SLAAC.
- **Configuration & management flexibility:** Added support for non-contiguous IPv4 subnet masks in network object groups and NGFW policies, providing greater flexibility when defining security rules and data-prefix variables.

From Cisco Catalyst SD-WAN Release 26.2.1 support for SD-Branch is discontinued as it reaches end-of-life (EOL).

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 IOS XE Catalyst SD-WAN 26.2.1 and Control Components 26.2.1

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

Product Impact	Feature	Description
Software reliability	Resilient Infrastructure	As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: • Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the **ip proxy-arp** command explicitly if required.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		• Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (telnet, ftp, tftp, http) are enabled in the configuration. • Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance.
Cisco Catalyst Network Monitoring		
Software reliability	Safety barriers enhancements	This feature adds support to enable safety barriers by default to prevent system failures.
API experience	OT Application Recognition in NBAR	This feature enhances the NBAR engine to identify a foundational set of Operational Technology (OT) protocols, including DNP3, IEC104, MMS, NTCIP, and OPC-UA.
Cisco Catalyst SD WAN High Availability		
Software reliability	Resilient data plane for Cisco Catalyst SD-WAN	Provides IKEv2/IPsec tunnels and per-VRF BGP routing that operate independently of the Cisco SD-WAN Control Components during an extended Cisco Catalyst SD-WAN outage.
Cisco Catalyst SD WAN Monitor Maintain		
Ease of use	Filters apply to Alarms and Events heatmap views	You can efficiently isolate critical network issues through advanced alarm and event filtering, which supports the application of up to five concurrent criteria. This enhanced filtering capability is reflected across both the tabular data and the intuitive heatmap view, empowering you to rapidly visualize alarms and events of interest to significantly streamline troubleshooting and monitoring workflows.
Ease of use	Sub-interfaces supported in SD-WAN Manager statistics	This feature enables you to monitor sub-interfaces in Cisco SD-WAN Manager's statistics, providing better visibility and control over your network performance. You can view detailed data on traffic and resource utilization per sub-interface, making it easier to troubleshoot and optimize your network resources effectively.
Cisco Catalyst SD WAN Network Hierarchy Configuration		
Ease of use	Support of FQDN for High Speed Logging and Syslog	You can enhance your security logging capabilities by configuring High Speed Logging (HSL) and external syslog servers. You set up the destination IP addresses or Fully Qualified Domain Names (FQDNs) of log servers, allowing collection of syslogs for up to four servers. This streamlined logging process enables effective monitoring and management of security-related events across your Cisco IOS XE Catalyst SD-WAN devices.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
Cisco Catalyst SD WAN Network Monitoring		
Upgrade	Upgrade Pre-check Report	This feature introduces a new upgrade pre-check report in addition to the preexisting reports.
Ease of use	Link SLA Change Report	The Link SLA Change Report tracks historical SLA metric changes and identifies if events were caused by packet loss, latency, or jitter.
Cisco Catalyst SD WAN Policy Groups		
Ease of use	Discontiguous Subnet Mask Support for IPv4 Network Object Groups	Adds support for discontiguous subnet mask entries in IPv4 data prefixes and IPv4 network object groups used by NGFW Policy. You can use discontiguous subnet mask entries in IPv4 source and destination match conditions, rule sets, object groups, and data prefix variables.
Cisco Catalyst SD WAN Security		
Upgrade	Secure Router NGFW	This feature introduces Secure Router NGFW, a new security-application container for supported Cisco Catalyst 8000 Series Secure Routers. In Cisco IOS XE Catalyst SD-WAN Release 26.2.1 and Cisco Catalyst SD-WAN Manager Release 26.2.1, it provides workflows to install the container and migrate supported settings from V1 Engine to V2 Engine. IPS and IDS retain their existing detection and prevention behavior while using Talos Lightweight Security Package (LSP) content. The release also adds Encrypted Visibility Engine (EVE) for encrypted-flow analysis without payload decryption and Snort ML inspection for supported threats. The V2 Engine replaces the UTD community/subscriber signature-package workflow with independently managed LSP and Vulnerability Database (VDB) packages. LSP provides Talos rules and detectors, while VDB provides application, fingerprint, and enrichment information.
API experience	SD-WAN IKEv2 and post-quantum encryption	Enables Cisco IOS XE Catalyst SD-WAN devices to use Internet Key Exchange Version 2 (IKEv2) to establish and refresh encryption keys directly with each other for IPsec data-plane tunnels. The feature also supports two post-quantum encryption options: post-quantum cryptography (PQC) and post-quantum preshared keys (PPK).
Cisco Catalyst SD WAN Troubleshooting		
Software reliability	Include Log Settings Output in an Admin-Tech File	This feature enhances the admin-tech file by including verbose logs from the application server and its internal components, such as the configuration database, statistics database, and other services. You can select the log categories required for debugging, including

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		Authentication, Cloud, and Configuration Database logs. The selected option increases the logging verbosity for the corresponding component of the application server.
Interfaces Configuration		
API experience	IPv6 day-0 onboarding with DHCPv6 prefix delegation	Adds DHCPv6-PD as an IPv6 address-discovery option in the ZTP/PnP workflow for Cisco IOS XE Catalyst SD-WAN devices. ZTP runs IPv4 and IPv6 address discovery in parallel, and IPv6 discovery can use stateful DHCPv6, SLAAC, or DHCPv6-PD.
Ease of use	Port settings for speed, duplex, and auto-negotiation	Configures speed, duplex, and negotiation auto in a single command.
Network Configuration		
Software reliability	Packet Order Preservation during Tunnel Underlay Reassembly	Packet-order preservation for reassembly ensures that a tunnel endpoint forwards completed, reassembled packets from the same traffic flow in correct order. The feature operates with packet reassembly boost mode on supported Cisco IOS XE Catalyst SD-WAN devices and SD-WAN Manager.

Changes in behavior

Changes for Cisco IOS XE Catalyst SD-WAN 26.2.1 and Control Components 26.2.1

Behavior change	Description
DNS packet routing now follows standard device configuration and route lookups.	Previous Behaviour: DNS packets were forced through the NAT DIA route, unavailable. New behaviour: DNS routing follows standard route lookups. NAT routes r otherwise, traffic defaults to standard paths (e.g., overlay). The Umbrella F and symmetric routing is maintained. Refer to the Umbrella Integration sec
From Cisco IOS XE 26.2.1, the show sdwan control CLI command's local-properties option shows more helpful information about expired certificates. In case of an expired certificate, the certificate-validity field in the command output shows Valid-Expired. In earlier releases, it shows only Expired.	Refer to show sdwan control.
The account lockout customization feature is not supported in a multitenant environment.	Refer to the documentation of Account lockout.
For multi admin tech generation requests, if certain nodes are down, it shows the failure in UI and continues the loop, allowing admin tech generation to proceed for other available nodes.	Refer to the Collecting system information using an admin-tech file sectio

© 2025 Cisco and/or its affiliates. All rights reserved.

Behavior change	Description
The SEA gateway provisioning includes VRF information for management and asset-access networks. This update ensures that the correct SEA gateway configuration is generated and applied to each configured VRF.	Refer to the Secure Equipment Access (SEA) section. Cisco Secure Equipment Access
BGP New Format is enabled by default.	Refer to the Global section
SAML Security Rejection Alarm	Cisco SD-WAN Manager now raises a SAML Security Rejection alarm whe potential security risks or validation failures. For more information, refer to Alarms Guide.
Link SLA Report Renamed	From Cisco Catalyst SD-WAN Manager Release 26.2.1, the Link SLA Rep For more information refer to the Reports section in Cisco Catalyst SD-WA
In a configuration group, in the Transport and Management profile, the Cellular Interface feature includes a field for specifying an interface name. To prevent configuration errors, the field validates the input to ensure this format: Cellular0/x/y. x: 0 through 9 y: 0 or 1 Example: Cellular0/0/1	Refer to the Cellular Interface section. Celular Interface
The existing logic that deleted admin tech files from disk after 24 hours is removed. Now, the files will not be deleted after 24 hours, the files will remain on disk untill the user manually deletes it.	Refer to the Collecting system information using an admin-tech file sectio
New role permission, SSH Terminal access is added	Refer to the Manage user group permissions section
When you deploy a policy group, Cisco SD-WAN Manager excludes controllers from the CLI preview if no CLI differences exist for the controllers.	Refer to Cisco SD-WAN Controller tasks for policy group deployments se
Changed behavior regarding an authentication issue when using an on-prem license server: When using the on-prem license server option, an error may occur when you first attempt to synchronize licenses between the server and SD-WAN Manager. This can occur if the license server is using a certificate not signed by a known certificate authority (CA). In earlier releases, addressing this required either having the certificate signed by a known certificate authority, or a workaround of manually loading a root certificate authority (CA) certificate onto SD-WAN Manager. If you are using an earlier version and require this workaround, contact Cisco TAC for details. In SD-WAN Manager 26.2.1 and later, this behavior has been changed. The change requires using software version 10-202606 or later for the on-prem license server.	Refer to Configure the License Reporting Mode for the procedure for setti on-prem license server.
Validation of vBond Orchestrator remote servers is limited to a single IP address or FQDN.	Refer to the vbond command.

© 2025 Cisco and/or its affiliates. All rights reserved.

Behavior change	Description
The POST /dataservice/alarms/markviewed API is updated to improve batch processing efficiency. The update includes the following changes: Partial Success: If the request contains a mix of valid and invalid UUIDs, the system updates all valid alarms and returns a response identifying the specific invalid UUIDs. Error Handling: If all provided UUIDs are invalid, no alarms are updated, and the system returns an INVALID_UUID error.	Refer to Alarm Fields in the Alarms Details section.
When you configure tenant-managed notification rules using the /dataservice/notifications/rule API, the VPN and VPN IP Subnet fields are mandatory if source VPN is set to 512. For more information, see Update Notification Rule.	Refer to the Send Alarm Notifications section.
Changed the behavior of the tools nping command. From 26.2.1, the options keyword and all of the sub-options are no longer supported. A new set of command options are supported.	Refer to the tools nping CLI command reference for details.
Any changes made to the location from the Zscaler portal are preserved. However, the configuration defined in Cisco SD-WAN Manager takes precedence for location attributes configured in Cisco SD-WAN Manager. Cisco SD-WAN Manager synchronizes with Zscaler using the Zscaler API, ensuring that only attributes managed through Cisco SD-WAN Manager are updated for existing locations.	Refer to Create tunnels to Zscaler using policy groups.
For a site-list, a region, or a region-list, mixing apply data-policy in direction all with from-service or from-tunnel is rejected. Use direction all by itself or use from-service and/or from-tunnel. Unsupported configurations are blocked. One data policy for from-service and another for all at the same site. One data policy for from-tunnel and another for all at the same site.	Refer to the Restrictions for Data Policy section
SD-WAN Manager's password expiration handling is enhanced, including extended configurable ranges for expiry and warning ages.	Refer to before you begin in the Reset a locked user using SD-WAN Mana
From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, the maximum length of the policy name is 128 characters. Cisco SD-WAN Manager UI and API validation reject values longer than 128 characters.	Refer to Configure traffic policy
You cannot use the deprecated configuration-db update-admin-user command to update the configuration database administrator credentials. Instead, use the standard Cisco SD-WAN Manager upgrade workflow. When you upgrade Cisco SD-WAN Manager, the system automatically updates the configuration database administrator credentials.	Refer to the Update the configuration database login credentials section.

© 2025 Cisco and/or its affiliates. All rights reserved.

Behavior change	Description
As part of a security enhancement to the coordination server used for SD-WAN Manager cluster operations, additional validation steps may cause a one-time boot-up delay immediately after the upgrade. This delay occurs only during the first startup after the upgrade.	Refer to the SD-WAN Manager cluster upgrade section.
From Cisco Catalyst SD-WAN Release 26.2.1, variable values support semicolons. Earlier releases did not support semicolons.	Refer to the Create a CLI Add-On Profile section.
Newer UTD IPS signature packages with different filenames can replace existing packages when they use the same Snort version.	In Cisco Catalyst SD-WAN Manager releases 26.2, a newer remote UTD I rejected as a duplicate solely because it uses the same Snort version. If th replaces the existing package, so users do not need to delete the existing Packages with the same filename or a different Snort version continue to b packages.
From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, aux parameter is unsupported. During an upgrade, SD-WAN Manager handles this command automatically.	Refer to the line command.
IPv6 high-priority packets that are destined to the local router follow the same policy behavior as IPv4 high-priority packets. Such packets are skipped by policy processing and are not dropped even when the policy action or default action is set to Drop. This behavior applies only to packets consumed by the local router. If the packets are forwarded to another device, policy processing still applies.	Refer to Action conditions section of Application Priority and SLA chapter.
To configure the maximum number of active outgoing connections from a device, use the crypto ikev2 limit command in global configuration mode.	Refer to crypto ikev2 limit.
DHCPv6-PD day-0 onboarding includes vendor information for device identification.	For DHCPv6-PD day-0 onboarding, use these commands: • ipv6 dhcp client vendor-class mac-address — supplies the device MAC a • ipv6 dhcp client request vendor — requests vendor-specific information i Refer to IPv6 day-0 onboarding with DHCPv6 prefix delegation.
You can provide either an IPv4 or IPv6 address or a Fully Qualified Domain Name (FQDN) to specify a destination server.	Refer to Configure security logging.

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Resolved issues for Cisco IOS XE Catalyst SD-WAN, 26.2.1

Bug ID	Description
CSCwt10887	The Cisco IOS XE Catalyst SD-WAN device crashes after the system attempts to push a configuration group.
CSCwv02836	The Cisco IOS XE Catalyst SD-WAN device upgrade process reports an incorrect " Required space" value.
CSCws50867	The system sets the tracker probe ID to 0 when users change an invalid DNS endpoint to an endpoint IP.
CSCwt54094	Fails to adjust queue limits in the C8kv policy-map after administrators install an HSEC license.
CSCwu03035	Cisco IOS XE Catalyst SD-WAN device silently drops large, fragmented RADIUS packets when UTD is active.
CSCwv34598	A PuntInject Keepalive timeout triggers a reset on the Cisco Catalyst SD-WAN edge router.
CSCwu03372	An FTMD fault triggers an unexpected reload on Cisco Catalyst SD-WAN edge routers using On-Demand tunnels.
CSCwv23165	BFD echo packet counters report a false 50% packet loss after administrators enable Enhanced Application Aware Routing.
CSCwu39202	A power reset during the boot process forces the Cisco IOS XE Catalyst SD-WAN device into ROMMON.
CSCwt47734	The endpoint-tracker HTTP probe sends an IP address instead of an FQDN.
CSCwt25835	The C8455-G2 router crashes during an IPsec scale periodic rekey.
CSCwv61185	The C8000V vdaemon process causes control connection flaps with HWCERTREN when multiple Cisco Catalyst SD-WAN Manager-signed certificates share identical Not Before timestamps.
CSCws66553	Executing the " clear sdwan omp events" command triggers an fpmd crash on the 17.12.6B respin image.
CSCwu21490	Deletes kernel core files from flash when it generates an incomplete Admin Tech.
CSCwt70932	An ARP resolution failure prevents BFD session establishment.
CSCwt44263	Configuration fails to maintain the VPN ID after users enable the UTD feature, causing ZBFW to evaluate traffic against an incorrect policy.
CSCwv25887	Concurrent NAT translation creation and timeouts cause allocator contention and high QFP utilization.
CSCwu53168	A confd Phase 0 failure causes the Cisco IOS XE Catalyst SD-WAN device upgrade to fail with a timeout
CSCwu34418	A qfp-ucode-mirabile error causes a C8235-G2 QFP crash.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv08826	Cisco IOS XE Catalyst SD-WAN device fails to perform BOW in EAAR when tunnels exceed SLA and variance thresholds.
CSCws68686	A basic policy with a default drop action causes IPv6 BGP neighborship failures in the application policy.
CSCwt16689	The QFP command displays an incorrect App-Probe-Class (APC) queue assignment.
CSCwt46462	Failure in generating alerts when the EC Genet server dies or times out.
CSCwu10100	The endpoint tracker fails to determine the next-hop for DNS name resolution from a Dialer interface.
CSCwu43078	Software triggers a stats cache bad address error in the CPP cpp_cp_svr process. %STATS_CACHE-3-BAD_ADDR: F0: cpp_cp_svr: id=1104077742 bad_addr=0xb6db0968 uidb=Tunnel91(in) fia=IPV4_INPUT_WCCP oce=0x0 oce_type=UNKNOWN OCE TYPE - Traceback=1#d8af1020c39c03a6d18baae61e21
CSCwt92911	The OMP process crashes during endpoint tracker teardown.
CSCws98086	displays an incorrect state change reason in the BFD syslog.
CSCwt02712	The Curie (Radium) platform exhibits CP CPU degradation on the 26.1 Cy3 Relops image.
CSCwv74258	High traffic rates cause infra timer expiry on the C8500 platform.
CSCwu71258	The entSensorScale and entSensorPrecision values return incorrect results for the PEM compared to the "show environment" command.
CSCwv07339	Upgrading to 26.2.1 causes an unexpected increase in IOX application persistent disk size.
CSCwv09160	The HTTP SIG tracker resolves the endpoint-api-url IP address via DNS following an upgrade to 17.15.05.
CSCwu67470	Changing the security policy to "none" in a template causes an unexpected reload on the Cisco Catalyst SD-WAN edge router.
CSCwu86821	Configuration fails to delete old TLOC list actions during local service-chain configuration modifications, causing packet drops.
CSCwu53407	The Cisco Catalyst SD-WAN edge router intermittently fails to generate a standalone endpoint-tracker UP recovery syslog.
CSCwu32769	CPP stuck threads in the BFD Cisco Catalyst SD-WAN transmit path cause the Catalyst 8500 router to reload.
CSCwr76176	A dbg2:1 event causes BFD Cisco Catalyst SD-WAN PMTU to converge unexpectedly to 970 bytes.

© 2025 Cisco and/or its affiliates. All rights reserved.

Resolved issues for Cisco Catalyst SD-WAN Control Components, 26.2.1

Bug ID	Description
CSCws89886	Cisco Catalyst SD-WAN Manager Release 20.15.4 continuously refreshes the DNS Security page for custom role users.
CSCwu40662	Cisco Catalyst SD-WAN Manager partially loads feature template drop-down options in device templates that contain over 400 options.
CSCwt59126	Cisco Catalyst SD-WAN Manager fails to create and save Network Design Profiles.
CSCwu15737	[Enhancement][20.18.2] Enable automatic renewal when the Cisco Catalyst SD-WAN edge device or hardware edge runs in Enterprise mode.
CSCww00334	Cisco Catalyst SD-WAN Manager fails to generate the Next-Generation Firewall (NGFW) CLI for SD-Routing during policy group preview or deployment.
CSCws90426	Centralized policy lists display a reference count of 0 after upgrading Cisco Catalyst SD-WAN Manager from Release 20.12 to 20.15.
CSCwu49363	Single Sign-On (SSO) login to Cisco Catalyst SD-WAN Manager fails when the IdP SAMLResponse root element uses the default xmlns namespace instead of the saml: or samlp: prefix.
CSCws30298	Cisco Catalyst SD-WAN Manager prevents users from modifying an Application-Aware Routing (AAR) policy due to the error: " Failed to acquire lock for template type policy_definition with policy" .
CSCws70834	In Release 20.15.5 UX 2.0 CLI Add-On, the variable creation workflow in the user interface prevents users from entering spaces and unsupported special characters.
CSCwt53078	Configure individual OSPFv3 settings within Configuration Groups in Cisco Catalyst SD-WAN Manager.
CSCwv56552	The Cisco Catalyst SD-WAN Controller VPN 512 IPv6 interface does not display its link-local address.
CSCwu08319	Cisco Catalyst SD-WAN Manager synchronizes the in-memory AVL tree for valid Cisco Catalyst SD-WAN Controller lists that the application server transmits.
CSCwv00709	The Cisco Catalyst SD-WAN Manager user interface pushes unsupported data policy configurations to devices.
CSCwv33808	On Disaster Recovery (DR) nodes, the DR page displays Data Center (DC) nodes as down despite active replication.
CSCwu78405	The Cisco Catalyst SD-WAN Controller Identity Manager (IDMGR) advertises invalid Cisco Identity Services Engine (ISE) pxGrid IP-to-user sessions with empty usernames or missing Active Directory domain data.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu02280	Cisco Catalyst SD-WAN Manager does not support configuring the Cisco ThousandEyes Enterprise Agent on Cisco Catalyst 8500-20X6C devices through Configuration Groups.
CSCwv98654	The Cisco Catalyst SD-WAN Manager user interface cannot reach Cisco Catalyst SD-WAN edge devices on multitenant setups, even though control connections remain active.
CSCwt53968	Cisco Catalyst SD-WAN Manager does not display TACACS+ authenticated users in the User Sessions view.
CSCwt49418	Editing a policy automatically disables the Fallback to Routing option for the catch-all rule.
CSCwt55758	The Cisco Catalyst SD-WAN Manager Speedtest tool displays the error " Invalid request Invalid deviceId" .
CSCwu99502	User Scopes do not function properly across a Cisco Catalyst SD-WAN Manager cluster.
CSCwu67471	Tenant creation fails in Cisco Catalyst SD-WAN Manager due to an NCS MAAPI transaction conflict during template pushes to the Cisco Catalyst SD-WAN Controller.
CSCwv64209	Cisco Catalyst SD-WAN Control Components generate a Certificate Signing Request (CSR) with a 2048-bit key instead of the selected RSA 4096-bit key in Releases 20.15.x and 26.1.1.
CSCww19672	Removes character restrictions to permit special characters such as @ and & in the organization name
CSCwt99082	Cisco Catalyst SD-WAN Manager upgrades fail because the container manager encounters an error.
CSCwv91041	Admin was removed from the internal NACM netadmin group, causing cfgmgr crash in all cluster nodes
CSCwu78416	Configuration-db password appears as plain-text in Cisco Catalyst SD-WAN Manager UC logs
CSCwt87655	Cisco Catalyst SD-WAN Manager fails to authenticate with TACACS on VPN 512 loopback after upgrade to 20.15.5.
CSCwu25921	Interface statistics do not update on Cisco Catalyst SD-WAN Manager UI.
CSCwt47459	App Usage Dashboard fails when app list contains appFamily entry type.
CSCwv40786	NWPI trace start on cEdge fails after control-connection loss during trace stop.
CSCwv38934	Unable to save changes in SVI interface using configuration groups without assigning IP.
CSCwv77379	CSV export in Dual Router Configuration Group fails to populate certain router1 device variables.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt79338	RBAC user limited to one site can browse to deep URLs such as /apidocs and /logsettings.html.
CSCwv06053	Unable to modify AAA authentication order in Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller AAA feature templates.
CSCwu17506	Unable to add new devices via serial file upload because internal management IP address pool is exhausted.
CSCwu72186	Multiple API calls generate in Cisco Catalyst SD-WAN Manager 20.15.4.2 causing policy preview or activation issues.
CSCwv27877	Lack of input validation for client session timeout using API requests
CSCws74603	Enabling port channel on Ethernet interface in service VPN removes tunnel configuration when using configuration group.
CSCwu25012	Custom applications are lost from application list after upgrading from 20.12 to 20.15.
CSCwv46950	Monitor topology view drilldowns ignore selected site and list all sites regardless of health status (20.18 & 26.1.1.2).
CSCwv25542	Cisco Catalyst SD-WAN Manager shows only 25 devices when more than 25 devices have version mismatch or incompliance.
CSCwt98623	Unable to delete images from MT Cisco Catalyst SD-WAN Manager image repository.
CSCwt44516	Cisco Catalyst SD-WAN Manager : Auto-generated zone name in NGFW does not follow 32-character constraints.
CSCwv43223	Cellular link shows increased bandwidth usage.
CSCwv18532	Valid centralized policy fails with error: " Invalid policy: Assembly failed. Duplicate mapping detected for <site-list>#<policy-type> in VPN <vpn-name>" .
CSCww00001	AWS GovCloud Cloud OnRamp configuration removed after upgrade because legacy CGW is missing cloudGatewayMode. `
CSCwt40661	Cluster-oracle process terminates after reboot.
CSCwu99447	Cisco Catalyst SD-WAN Manager 20.18.3 does not show routers in step 5 " deploy" when deploying configuration group.
CSCwu08422	Cisco Catalyst SD-WAN Manager UI check for special characters bypassed via API.
CSCwt68160	UX 2.0 single device configuration group variable values lost when device disassociates.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt09625	Cisco Catalyst SD-WAN Controller experiences high memory usage due to IDMGR process on 20.15.
CSCwu50939	Failed to update variables and failed to edit security policy.
CSCwt24351	Cisco Catalyst SD-WAN Manager requires RBAC granularity so only specific tools can be accessed.
CSCwt80056	Cisco Catalyst SD-WAN Manager application server restarts continuously after interrupted disaster recovery database import.
CSCwv17579	On-prem ZTP device upload fails using .viptela file when configuring Cisco Catalyst SD-WAN Validator as ZTP server.
CSCwv84273	Leaking other tenants' serial numbers into another tenant when MT-E is enabled and conflicting IP addresses exist.
CSCwu37175	Hardened edge serial parsing scripts to limit impact of corrupt data/empty string sent by Cisco Catalyst SD-WAN Manager.
CSCwt71863	Long interval of disaster recovery in pause state causes large files to be written to disk from last successful replication.
CSCwt51589	Post upgrade from 20.9.8 to 20.15.4.2, IOS-XE cEdges fail to sync root certificate.
CSCwu77155	Post upgrade from 20.9.8 to 20.15.4.2, IOS-XE cEdges fail to sync root certificate.
CSCwu53690	Login banner is missing when logging into Cisco Catalyst SD-WAN Controller.
CSCwu09062	Neo4j user password not updated in Neo4j database when username and password contain special characters.
CSCwu14629	Device selection issue with configuration group.
CSCwv62413	Deploy configuration group and show license management display blank screen.
CSCwv30205	IPSEC parcel save operation fails with error: " Address is invalid" when tunnel mode is set to ipv4-v6overlay.
CSCwv17013	Operator role can edit or invalidate controllers on Cisco Catalyst SD-WAN Manager 20.18.3.1.
CSCwv40868	Cisco Catalyst SD-WAN Manager: Editing DNS redirect action on any policy edit results in error.
CSCwv04385	Audit log flooded with session timeout logs from Cisco Catalyst SD-WAN Validator device user
CSCwu00420	VLAN ID not found error during NGFW policy group deployment with zone security on Cisco Catalyst SD-WAN Manager.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv71074	Show users command fails for every CLI user when active GUI session contains multiple addresses from HTTP X-Forwarded-For header.
CSCwv12043	TACACS secret key shows in plain text in configuration group.
CSCwt35522	Cisco Catalyst SD-WAN Manager 20.15.4.1 unable to push policy group on one of the Cisco Catalyst SD-WAN Controllers.
CSCws08530	Deploying two sub-policies with same variable names in 26.1 should show sub-policy names correctly.
CSCwt91627	Cisco Catalyst SD-WAN Manager API stopped working after upgrade from 20.12 to 20.15.
CSCwu33078	Historical CPU and memory usage graphs in security monitoring graphs for IPS are empty.
CSCww07892	Cflowd centralized policy save or activation fails when using a subinterface as collector source interface.
CSCwv33920	Cisco Catalyst SD-WAN Manager displays duplicate variables in policy groups and CLI configuration groups.
CSCws45978	Policy/topology group push may fail due to unreferenced VPN profile error.
CSCwv03618	Cisco Catalyst SD-WAN Manager crashes with multiple processes aborted
CSCwt98267	Unexpected " Enforce Software Version (ZTP)" warning during cEdge upgrade.
CSCwv41952	Cisco Catalyst SD-WAN Manager does not generate alarms and shows incomplete events for OSPFv3 neighbor up/down.
CSCwt62850	Device-specific option missing when configuring service node IP addresses for App QoE in service profile.
CSCwv87005	Offline smart licensing loses license assignments when new sync file uploaded after communication issue
CSCwt95401	HSEC installation succeeds on c8000v router but Cisco Catalyst SD-WAN Manager reports failure with timeout error post system-IP change.
CSCwu39601	Upgrading Cisco Catalyst SD-WAN Manager Li image from confd_cli fails due to wrong image name parsing.
CSCwv23305	Custom role with minimal permissions can view WAN Edge inventory in Cisco Catalyst SD-WAN Manager 20.15.5.2.
CSCwu59830	Config preview fails when no value is given to more than one optional static/default route in service profile.
CSCwv89588	Editing a centralized policy fails with error " Policy contains invalid control or l"

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt97002	After upgrade to 20.15.5, olap-db shows MEMORY_LIMIT_EXCEEDED exception.
CSCwv95244	SD-WAN upgrade from 26.1.1.2 to 26.1.2 via upgrade workflow in disaster recovery setup gets stuck
CSCwu50841	Configuration groups missing administrative distance field for DHCP-based static routes in transport VPN profiles.
CSCwu93858	DCA does not send monitoring files when Cisco Hosted setting is false.
CSCwt62906	Cisco Catalyst SD-WAN Manager site topology shows '0 kbps' inaccurate TX and RX rates.
CSCws82756	NAT mapping-ID conflict occurs during HA configuration deployment in 20.15/17.15.5.
CSCwv36012	Unified policy push fails to push Umbrella secret or token.
CSCwu24260	Cisco Catalyst SD-WAN Validator vdebug flooded with failed to send DTLS packet IPC errors.
CSCwu60884	Smart-PxGrid connect fails with Cisco Catalyst SD-WAN Manager 20.18 and ISE nodes
CSCwv38668	REST API calls and Cisco Catalyst SD-WAN Manager GUI display only 5 OMP routes instead of full route set shown in Cisco Catalyst SD-WAN Controller CLI.
CSCwt70545	TACACS authentication fails on Cisco Catalyst SD-WAN Validator after upgrade to 20.18.2.
CSCwv26731	Cisco Catalyst SD-WAN Manager builds remote syslog (syslog-ng) as IPv6 by default when logging server is configured by FQDN.

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 Cisco IOS XE Catalyst SD-WAN, 26.2.1

Bug ID	Description
CSCww46621	The ISR1K platform repeatedly fails to initialize primary and backup NVRAM.
CSCww34162	NAT type changes after a Cisco IOS XE Catalyst SD-WAN device upgrade to 17.15.6, causing TLOC extension registration to the Cisco Catalyst SD-WAN Validator through local egress.
CSCwv84068	Code changes in 17.12.6 cause control connection failures on Cisco IOS XE Catalyst SD-WAN device.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCww51727	A Gi sub-interface stays stuck in "DELETING - FEATURES" within the QFP on C8200-1N-4T edge routers with CTS (cpp_cts) bound, preventing AOM pending object drainage and causing VRRP/InjectErr drops and subnet gateway black-holing.
CSCwv71872	CoR-SaaS probes custom-app endpoint URLs on a free configurable port.
CSCwv95062	A CPP traceback occurs in the UTD interface-create path when tunnel app-id lookup fails.
CSCww46523	ZTP interface configuration fails to deploy on module interfaces for 8500 platforms.
CSCww36048	Cisco IOS XE Catalyst SD-WAN device LTE GPS standalone state prevents committing ms-based configuration through CLI or Cisco Catalyst SD-WAN Manager.
CSCww43760	SGT information disappears on SIA auto tunnels with IP-to-SGT bindings.
CSCww45867	Hubs drop a surviving Cisco Catalyst SD-WAN peer after NAT tuple reuse.
CSCwv65418	The ICMP interface tracker reports "up" every time the Cisco IOS XE Catalyst SD-WAN device resolves the configured DNS name.
CSCwv91764	Cisco Catalyst SD-WAN Manager displays incorrect public IP addresses for tunnels when using 26.2 Zscaler SSE GRE.
CSCww49105	FTMD fails to retry non-OnDemand TLOCs after transient BFD resource exhaustion.
CSCww20413	Updates to the GeoDB address outdated records in 17.18.x.
CSCwu24210	The .sdwaninstaller script on the Cisco IOS XE Catalyst SD-WAN device incorrectly accounts for rollback files during disk space calculation.
CSCww00586	The UTD context remains in Divert mode without inspection features enabled, causing traffic black-holing at the memif interface.
CSCww02502	Umbrella tunnels stay down while reporting a cdb-validate-info failed state with a 401 authentication error.

Open issues for Cisco Catalyst SD-WAN Control Components, 26.2.1

Bug ID	Description
CSCww37814	Cannot save BGP route-policy when the sequence contains only the action "accept."
CSCwv97506	Cisco Catalyst SD-WAN Multi-tenant cannot validate devices that were previously invalid in the tenant.
CSCwv91051	Cisco Catalyst SD-WAN Manager version 20.15.5.2 does not display spoke sites and prevents editing of existing Hub-Spoke topology.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt61835	Configuration group deployment fails due to an SNMP-related error.
CSCww08123	Cisco Catalyst SD-WAN Manager's Configuration Group page loads slowly when many Service VPN entries exist.
CSCwv99325	Cisco Catalyst SD-WAN Manager generates invalid DHCP pool names when VLAN variables contain spaces, causing configuration failure.
CSCwv49366	Policy group deployment fails at Preview CLI with error "Vpn Id for vpn name 0 not found" when the VPN feature parcel name is not numeric.

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.

© 2025 Cisco Systems, Inc. All rights reserved.