Release Notes for Cisco Catalyst SD-WAN, Release 26.1.x

Cisco Catalyst SD-WAN Release, 26.1.x 3
New software features 4
Changes in behavior 9
Resolved issues 12
Open issues 16
Compatibility 19
Supported hardware 20
Related resources 20
Legal information 20

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

Cisco Catalyst SD-WAN Release, 26.1.x

Cisco Catalyst SD-WAN Release 26.1.x is a major update focused on expanding cloud integration, strengthening security posture, and improving sustainability and operational observability.

- **Cloud & SaaS Optimization**: Enhanced Azure Cloud Gateway support for multi-tenant and multi-subscription environments, new telemetry controls for Webex and Microsoft 365, and refined DNS resolver prioritization.
- **Security & Compliance**: Introduced centralized remediation for insecure configurations, improved visibility into Identity Provider settings, and automated IP allocation for Unified Threat Defense (UTD).
- **Energy & Observability**: Launched a comprehensive Energy Management Dashboard (including carbon metrics and reporting) and added new CPU, Memory, and Energy reports alongside proactive Node Latency alarms.
- **System & Operational Efficiency**: Streamlined web server certificate installation, updated cluster management workflows, optimized app-list processing, and expanded support for ISR 4461 devices.

End-of-Life Notice for Cloud OnRamp for IaaS

Cloud OnRamp for IaaS is reaching End of Life (EOL) effective with the next SD-WAN release. Cisco Catalyst SD-WAN Release 26.1.x is the final version that supports this feature. To maintain service and support, customers are required to set up their connectivity to their cloud infrastructure using Cloud OnRamp for Multicloud.

Catalyst SD-WAN Recommended Computing Resources Matrix

What's new

We have introduced the Recommended Computing Resources Tool to streamline the process of identifying recommended computing resources for Cisco Catalyst SD-WAN deployments. Enter your deployment requirements to receive recommendations in seconds.

Why use the Recommended Computing Resources Tool

The tool eliminates manual analysis of recommendation tables and deployment scenarios by generating computing resource recommendations based on your deployment requirements.

Transition

To provide a smooth transition, this guide and the Recommended Computing Resources Tool will both remain available for the next two releases after Cisco Catalyst SD-WAN Manager Release 26.1.x. After this transition period, the Recommended Computing Resources Tool will become the primary source for recommended computing resource information.

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.

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

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 26.1.1 and Control Components 26.1.1.1

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

Product Impact	Feature	Description
Software reliability	Resilient Infrastructure	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • ·Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in

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

Product Impact	Feature	Description
		a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption. For more information, refer this document Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing
Cloud OnRamp Configuration Guide		
Ease of use	Multiple Resource Groups and Subscriptions for Azure Cloud Gateways	This feature enables tagging and discovery of vNets from Cisco SD-WAN Manager across subscriptions and tenants different from the one hosting the virtual WAN (vWAN). It also provides flexibility to use either the same or different resource groups for each region when creating a cloud gateway. Additionally, you can create cloud gateways or virtual hubs within the same virtual WAN, even if they reside in different subscriptions.
Ease of use	Cloud OnRamp for SaaS Telemetry Settings	This feature provides setting options for enabling and disabling Webex and Microsoft 365 telemetry from the Cloud OnRamp for SaaS monitoring dashboard in Cisco SD-WAN Manager.
Software Reliability	DNS resolver prioritization	Refinement of the DNS resolver prioritization for application traffic subjected to Cloud OnRamp for SaaS, when using Cisco Umbrella Connector or data policy Redirect DNS.
Upgrade	Secure Service Edge Support for Cloud OnRamp for SaaS	This feature extends Cloud OnRamp for SaaS support to Secure Service Edge (SSE) tunnel. With this feature you can access SaaS applications securely, and automatically select the best SSE tunnel for accessing the SaaS applications.
Getting Started Guide		
Ease of setup	Web server certificate installation	SD-WAN Manager uses an authentication certificate for secure browser connections. This release provides new installation options for web server certificates.

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

Product Impact	Feature	Description
Ease of use	Access to Cisco Support Assistant	Cisco Support Assistant is a support tool that integrates TAC support functions directly into SD-WAN Manager. In previous releases, using Support Assistant required installing a browser extension. This is no longer needed. With Support Assistant, you can open TAC cases, record screens, and upload logs directly from SD-WAN Manager.
Monitor Maintain Guide		
Ease of use	Elimination of reports passwords	To eliminate the burden of managing system-generated passwords, password requirement is removed for Executive Summary and Application Summary Reports. This is applicable to both new and existing scheduled reports.
Ease of use	CPU, Memory and Energy Report	This feature introduces a new CPU, Memory and Energy Report in addition to the preexisting reports.
Ease of use	Energy Management Dashboard	The Energy Management dashboard in Cisco SD-WAN Manager has the following enhancements: • Energy management reporting • Offline-mode support • Carbon intensity metrics • Time period comparison • Site-to-Site comparisons
Ease of use	Insecure configuration management	Provides centralized visibility and actionable remediation for insecure feature configurations to strengthen network security in Cisco Catalyst SD-WAN.
Ease of use	Cisco SD-WAN site-to-site speed test with private address	This feature introduces the use of private IP addresses (10.1.x.x) for site-to-site speedtest instead of 11.1.x.x. A new CLI command is provided to disable 11.1.x.x.
Software reliability	One Minute Granularity for Interface Statistics	With this feature you can collect granular interface statistics for the devices for every minute. This feature ensures optimal performance along with real-time troubleshooting.
Upgrade	Firmware Upgrade on Selective Devices with Cellular or Wi-Fi modules	SD-WAN Manager supports choosing specific devices with Wi-Fi or cellular modules for firmware upgrade.
Ease of use	Energy Management Enhancements	This feature enhances the support on IR platforms.
Policies Guide		

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

Product Impact	Feature	Description
Ease of use	Packet duplication on more than one additional tunnel	This feature allows you to generate multiple copies for each original packet on more than one additional tunnel using the CLI.
Software reliability	Policy validation in Cisco SD-WAN	This feature ensures network reliability and operational efficiency by automatically validating Cisco Catalyst SD-WAN policies for accuracy, platform compliance, and alignment with network requirements before deployment.
Configuration Group Guide		
Ease of use	Device Tagging for Dual Device Site Configurations	With this feature you can add devices to a dual devices site configuration in the configuration groups workflow using tags.
Policy Groups Guide		
Ease of use	Enhancements for NGFW in Policy Groups	The following enhancements are introduced with this release: • Display rule hit count. • Import and export of the firewall policies. • Drag and drop rules in a policy to update the priority. • Display policy and object usage reference in the NGFW policy dashboard. • Rule and policy name retention in the running CLI configuration.
Upgrade	Increase in FQDN Scale	With this feature the FQDN entries are increased to 256.
Upgrade	Increase in Local Domain Bypass Scale	With this feature the local domain bypass entries are increased to 256.
Upgrade	DNS Security with Cisco Secure Access	This feature monitors and controls the DNS requests by blocking access to unauthorized domains and applies consistent DNS-based security policies across devices. DNS security fallback ensures that dns security policy routing is determined by device routing configurations. In the event of a failover where the NAT Direct Internet Access (DIA) route is unavailable, connectivity is maintained by service vpn routing, ensuring continued reachability.
Ease of use	Device Tagging for Policy Groups	With this feature you can add devices to a policy group configuration workflow using tags.

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

Product Impact	Feature	Description
Routing Guide		
Software reliability	OMP vDiagnostics	This feature introduces a diagnostic tool designed for Cisco SD-WAN to troubleshoot OMP peering failures. When OMP peering is lost, the system automatically captures a snapshot of essential data.
Rugged Series Router Configuration Guide		
Ease of use	Wireless monitoring in Cisco SD-WAN Manager	Wireless monitoring in Cisco SD-WAN Manager provides real-time visibility into the status and operating mode of the Wi-Fi module installed in Cisco Catalyst IR1800 Rugged Series Routers. This feature enables you to monitor the health, operational mode, and firmware version of the Wi-Fi module.
Security Guide		
Software reliability	Custom DNS Configuration for UTD	This feature introduces custom DNS server configuration for Unified Threat Defense (UTD) on Cisco IOS XE Catalyst SD-WAN devices. Configuring custom DNS servers using the ip name-server CLI command under the utd global submode allows you to specify primary and secondary IP addresses. This overrides the default OpenDNS and IOSd-configured name-servers, thus ensuring optimized URL resolution and filtering performance.
Ease of use	Unified Threat Defense Support for Cisco Catalyst IR8100 Heavy Duty Series Router	IR8140 supports selective activation of Unified Threat Defense (UTD) capabilities, specifically Intrusion Prevention System (IPS) and Intrusion Detection System (IDS).
Software reliability	IPSec Interworking Re-architecture for Cisco IOS XE Catalyst SD-WAN devices	This feature streamlines the security infrastructure of Cisco IOS XE Catalyst SD-WAN devices by relocating IPSec logic from the Forwarding Table Manager (FTM) to the IOS daemon (IOSd). By removing the Security Association (SA) database from FTM and establishing a direct communication channel for updates, the system ensures that security states are managed centrally. This leads to enhanced system stability, faster security operations (such as rekeying and Pairwise Key generation), and improved serviceability and reliable session management.
Ease of use	Unified Threat Defense Support for Cisco 8100 Series Secure Routers	UTD extends support on next-generation Cisco 8100 Series Secure Routers: C8131-G2, C8151-CVAI-G2, C8151-CVAP-G2.
Upgrade	Cisco Secure Access integration extended to Cisco Catalyst SD-WAN for Government	Cisco Catalyst SD-WAN for Government can integrate with a federally authorized Cisco Security Service Edge (SSE) server to enable Cisco Secure Access integration.
Interfaces Configuration Guide		

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

Product Impact	Feature	Description
Ease of use	Per packet load balancing	With this feature, Cisco SD-WAN sends packets from a single flow across multiple WAN links, maximizing bandwidth and maintaining performance by reordering packets at the destination.
Multitenancy Guide		
Ease of use	Support for Controlling Tenant's Access to SD-WAN Manager	Allows service providers to temporarily suspend or restore a tenant's access to SD-WAN Manager without affecting network traffic, monitoring, or alerts. Suspended tenants cannot log in to SD-WAN Manager or configure changes, while providers retain full visibility and control.
SD-WAN Portal Guide		
Ease of use	Open Cisco SD-WAN Manager directly from the Portal	The Fabric Details page in the SD-WAN Portal includes a browser link to launch the SD-WAN Manager without re-entering credentials.

Changes in behavior

Changes for Cisco IOS XE Catalyst SD-WAN 26.1.1 and Control Components 26.1.1.1

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, risking blackholes if the route was unavailable. New behaviour: DNS routing follows standard route lookups. NAT routes now require a tracker to ensure availability; otherwise, traffic defaults to standard paths (e.g., overlay). The Umbrella FIA no longer forces global VRF traversal, and symmetric routing is maintained. Refer to the Umbrella Integration section.
For a network with specific conditions, 26.1.1 introduces a restriction of vRoute (OMP route) advertising to improve efficiency by not advertising vRoutes that are incompatible due to color. An SD-WAN Controller only advertises vRoutes to devices whose TLOC color is compatible with the TLOC color of the ultimate TLOC color.	Refer to the TLOC color filtering section.
Support for Cyber Vision includes monitoring L2 and L3 interfaces simultaneously on IR8340 platforms.	Refer to Cyber Vision Integration Cyber Vision Integration with Cisco Catalyst SD-WAN
From SD-WAN Manager 20.18.1, custom applications are supported in multitenant environments.	Refer to Multitenancy.
The clear aaa login command, on an SD-WAN Manager, Controller, or Validator host, closes a user CLI session opened by Telnet or SSH.	Refer to clear aaa login.

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

Behavior change	Description
Change in controller entity names for alarms.	Previous behaviour: Alarms in Cisco SD-WAN Manager were called vManage alarms, vBond alarms, and vSmart alarms New behaviour: From from Cisco Catalyst SD-WAN Control Components Release 26.1.x, the, alarms will appear as Manager alarms, Validator alarms, and Controller alarms. Refer to the Cisco IOS XE Catalyst SD-WAN Alarms Guide.
NAT DIA fallback and redirect-dns IP actions are supported at the same time in data policy beginning with Cisco IOS XE Catalyst SD-WAN Release 26.1.1.	Refer to NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices section.
Starting from Cisco IOS XE Catalyst SD-WAN Release 26.1.1, export and import of topology is not supported because the sites can be added with site id and tag rules.	Refer to Create topology section.
You can redistribute nat DIA route (inside and outside) to BGP before 26.1.1. From 26.1.1, you can choose to redistribute nat DIA outside route to BGP by new UI knob.	Refer to BGP Routing in Service profile section.
Functionality for Configuration conversion tool is updated.	Refer to the Configuration conversion tool section.
ISR 4461 devices are supported and compatible.	Refer to Device version compliance section.
The FNF default cache size will dynamically adjust according to the FNF flow defined length. For example, if enable more optional features, The FNF default cache size will reduce accordingly.	Refer to the Configure Global Flow Visibility section
Update the software version of your router to the latest to prevent unintended boot failures. This update ensures that the previous_packages.conf file remains aligned with the configured default software version that you have set using the CLI command request platform software sdwan software set-default or through Cisco SD-WAN Manager.	Refer to Router Loads the Previous Software Version After Booting
When creating configuration groups, SD-WAN Manager provides interface suggestions for Industrial Router (IR) devices.	Refer to the Add Devices to a Configuration Group section
After completing the migration from single-tenant overlay to multitenant overlay, perform this additional step if the destination setup connects to SD-AVC SaaS. Run the specified API from the destination multitenant environment for a seamless integration with SD-AVC. API: `HTTP POST: /dataservice/sdavc/saas/publish-tenants`	Refer to the Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment section
You can edit the Secure Equipment Access (SEA) API key in the Secure Equipment Access Cloud window for external services.	Refer to the Configure a connection to a Cisco Secure Equipment Access portal in the Network Hierarchy section

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

Behavior change	Description
Starting with Cisco IOS XE Catalyst SD-WAN Release 26.1, the new scepencrypt CLI command provides the flexibility to define the SCEP encryption algorithm. This command supports various AES standards (128, 192, and 256) and maintains specific defaults based on the operational mode (FIPS vs. non-FIPS)	Refer to the crypto pki trustpoint command.
In Cisco SD-WAN Manager, both the VirtualPortGroup and guest interface IP addresses for Unified Threat Defense (UTD) are automatically allocated from the same /16 subnet. This update eliminates the need for manual configuration and ensures consistent communication between the gateway and the application, resolving previous connectivity issues related to /24 subnet assignments.	Refer to the Configure the Unified Threat Defense Resource Profiles Using Cisco SD-WAN Manager section.
Cisco SD-WAN Manager Node Latency State	Cisco SD-WAN Manager raises this alarm when it detects potential latency issues within the Cisco SD-WAN Manager cluster. For more information refer to Cisco IOS XE Catalyst SD-WAN Alarms Guide.
Device limits app-list processing to 10 entries.	The device processes only the first 10 app-families in a app-list. For more information, refer to the Application section.
Policy group deployment triggers Cisco SD-WAN Controller tasks during the subsequent deployments.	Refer to the Cisco SD-WAN Controller tasks and Policy groups for multitenant environments section.
In the administration settings for identity provider settings, you can view the details such as status, expiration date, certificate information, and so on, for the installed certificates.	Refer to the Enable an Identity Provider in Cisco SD-WAN Manager section.
VPN 0 transport interface IP address is not supported in the Edit Manager screen of Administration > Cluster Management.	Refer to Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server section.
Transition of UTD alarms to event-based notifications for improved monitoring.	Refer to the Cisco IOS XE Catalyst SD-WAN Alarms Guide.
From Cisco Catalyst SD-WAN 26.1.1, when executing the Register Disaster Recovery procedure, the Start Time field is no longer available.	Refer to Register Disaster Recovery.
Source interface field is introduced to use its IP address to export the flow records to the collector.	Refer to Configure cflowd section.
Cisco SD-WAN Manager generates a new syslog message when the device reaches the maximum number of bfd sessions.	Refer to System Message Guide.
Supported characters in variable values	Semicolons (;) are not supported in variable values. To separate multiple CLI lines, use the newline character (\n) instead.

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

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 Cisco IOS XE Catalyst SD-WAN, 26.1.1

Bug ID	Description
CSCwr30573	Module boot-up timing prevents the TLOC extension from programming.
CSCwr44921	Memory pressure causes the Cisco Catalyst IOS XE Catalyst SD-WAN device to crash due to high CPU usage.

Resolved issues for Cisco Catalyst SD-WAN Control Components, 26.1.1.1

Bug ID	Description
CSCwt48865	Unable to delete root-certificate from GUI.
CSCwt40661	Cluster-oracle terminated after reboot.
CSCwq48395	SD-WAN Controller has stuck exported routes after a policy configuration change.
CSCws12781	SD-WAN Manager displays duplicate devices for custom roles.
CSCwr74178	Preview CLI is not loading on the service chain configuration when using the workflow.
CSCwt40948	An inbound policy and the show OMP routes CLI command cause memory corruption.
CSCwr88750	SD-WAN Manager generates the guest IP address and VirtualPortGroup IP address from different subnets.
CSCws09544	SD-WAN Manager fails to generate the IP NAT DIA command when using the device-specific value in the configuration group.
CSCws68934	The network hierarchy for MRF fails to show associated devices when a user selects a single site.
CSCwr73205	omp_ro_opt : Assert @ cfgmgr - vconfd_sub_cb with threadid as optimized out.
CSCwr70696	Users are not able to attach DIA sites on Cloud OnRamp with the Office365 application.
CSCwr63220	An NGFW Policy created from automation fails to push with a NullPointerException.
CSCws10645	The policy-groups region drop-down list does not display secondary regions for MRF.
CSCwq24066	" show omp routes|tlocs received|advertise detail" show the same results.

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

Bug ID	Description
CSCwr57474	SD-WAN Manager fails to sync the license with the offline file despite the GUI indicating success.
CSCwq79825	Errors appear when applying a new policy group due to PSK restrictions involving the ';' character on SIG tunnels.
CSCwr47027	All traces of embargo are removed from logging and other tracing mechanisms.
CSCws84334	Setting TLOC preference change using a configuration group will not be configured if the change value is default.
CSCws75823	The licensing overview page fails to exclude perpetual licenses.
CSCwq08068	PSK issues on SIG tunnels cause errors when applying a new policy group.
CSCwr94642	A failed policy group push causes the SD-WAN Controller to become out of sync.
CSCwt40951	SD-WAN Controller crashes during admin-tech collection.
CSCwq37551	SD-WAN Manager fails to apply the FQDN syslog configuration.
CSCws70210	Users cannot edit or delete local users in Cisco SD-WAN Manager.
CSCwt18938	PSK restrictions involving the ';' character cause errors when applying a new policy group in configuration groups.
CSCwq14387	The configuration group loses variable values.
CSCwo62038	SD-WAN Manager SSO with Azure assigns incorrect resources or scopes to remote users.
CSCws62586	The site availability report incorrectly displays information for all sites to users scoped to a single site.
CSCwr08232	The VPN group view details page lists unrelated devices.
CSCwq27187	No graphs for device monitoring on several devices.
CSCws11167	IPv6 routes not advertised to OMP using a device-specific route policy within an SD-WAN Manager VPN feature template.
CSCws98207	SD-WAN Manager fails to push the template due to an error retrieving the configuration template type from the lock record.
CSCwq56228	Datastore corruption causes the coordination server to restart continuously.
CSCwq46523	The dashboard underlay monitoring page incorrectly displays the alarm as active.
CSCwp35976	AAA accounting causes intermittent login issues on Viptela devices.

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

Bug ID	Description
CSCwp38316	There is a discrepancy between the WildFly active session count and the logged-in user session count in the configuration database.
CSCws05835	Users are unable to create a topology group on the first attempt due to a feature profile error.
CSCws09295	SD-WAN Manager fails to copy security rule sets.
CSCws67054	The TLOC chart on the device page fails to display data.
CSCwq37648	The UC upgrade fails when the neo4j password contains special characters.
CSCws38767	SD-WAN Manager triggers false alarms for high /tmp directory usage.
CSCwt26594	The Add Custom Applications button fails to function in the discovered applications tab.
CSCwr74862	The system allows two routers with the same site IDs to exist in two different policy groups.
CSCwo81500	OMP shut and no-shut commands on spokes cause rib-cache memory bloat on the controller.
CSCwt00896	A connection pool timeout to the vault causes the configuration group deployment to fail.
CSCws42389	Enabling tagging causes the configuration WAN edge list to freeze.
CSCws36801	An application-server failure causes the MT upgrade to fail.
CSCwr33423	The firewall HA service profile enforces a static NAT entry limitation.
CSCws17553	SD-WAN Manager fails to consistently redirect the applications, sites, and circuits tabs to SD-WAN Analytics.
CSCwr77759	The olap-db container fails to start after upgrading the SD-WAN Manager.
CSCwr60082	A " Resource group does not exist" error message on the standby DR node.
CSCws04241	SD-WAN Analytics causes high CPU and memory usage on SD-WAN Manager.
CSCws91663	Selecting folders causes multiple topology group bugs, inconsistent behavior, and a lack of diagnostic error messages.
CSCwp03901	F5 APM IDP causes the SD-WAN Manager SSO login to fail.
CSCwq97113	SD-WAN Manager deletes daily backups from the local disk.
CSCwo44963	Users are unable to disable debugs directly on devices running Viptela OS.

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

Bug ID	Description
CSCwq51748	The standby running-configuration fails to reflect edits to a custom role after a switchover in a DR setup.
CSCwp27018	The BFD summary aggregation fails to consider sites containing ENCS and the SD-WAN Device.
CSCwr83042	An error is generated when a user renames the cellular controller profile.
CSCwq32145	Upgrade fails due to the legacy unused neo4j-tx-listener component.
CSCws52923	A username cannot be created with the period - " ." : Name should not start with a number, characters (except underscore, hyphen) and uppercase not allowed.
CSCws70771	SD-WAN Manager lacks proper input validation for the web server certificate.
CSCwr87767	The ifDescr MIB provides an incorrect interface name after upgrade.
CSCwq32633	The RSA-4K-CSR option is greyed out on the validator and controller.
CSCwr05920	The cluster management page fails to display all options, showing only the connected device.
CSCws02678	Tunnel statistics are not getting converted into the site health summary.
CSCwr79876	SD-WAN Manager removes NAT bypass from the policy group.
CSCws36240	Feature needs to be enabled for custom role configuration group deployment.
CSCws44011	Controller and Validator upgrades should fail if the release version is higher than that of the SD-WAN Manager.
CSCws99348	The post-activation commit fails during upgrade and rollback.
CSCws49871	Users cannot select more than 100 devices in the Quick Connect device inventory sync workflow.
CSCwr76299	The configuration diff preview incorrectly merges the add-on CLI policy and centralized GUI policy changes.
CSCws24275	Configuration Group does not get deployed when its site type is " Dual Router" .
CSCwr87340	The validation check fails and throws an unrelated error while creating and deploying the configuration group.
CSCws42991	Unable to generate a report with the user name under the Email setting, even though the API call succeeds with the user name.

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

Bug ID	Description
CSCwt53505	Cannot apply any restriction to the file upload under the banner settings.

Resolved issues for Cisco Catalyst SD-WAN Control Components, 26.1.1.2

Bug ID	Description
CSCwu18563	Cisco Catalyst SD-WAN Controller authenticated privilege escalation vulnerability.

Resolved issues for Cisco Catalyst SD-WAN Control Components, 26.1.2

Bug ID	Description
CSCws83671	Following the Multitenant cluster upgrade from 20.15.306 to 20.15.403, Cisco Catalyst SD-WAN Manager and Cisco Catalyst SD-WAN Validator lost the device serial numbers.
CSCwt19263	After an upgrade, a role-based user account fails to execute the 'Upload WAN Edge List' function.
CSCwt78921	Cisco Catalyst SD-WAN Manager triggers random Forbidden Requests, causing API calls to fail with HTTP error 403.
CSCwt54915	A stale sshd_config in the RW filesystem causes the DeviceEventListener to fail the NETCONF client creation during the post-20.18 activation pre-check in the Cisco Catalyst SD-WAN Control Components.
CSCwu18441	An arbitrary file write vulnerability affects Cisco Catalyst SD-WAN Manager.
CSCwt50498	An authentication bypass vulnerability affects Cisco Catalyst SD-WAN Controller.
CSCwt27474	Developers must remove the hardcoded AS number 64512 and implement autodetection in the 20.18.2 Cisco SPA.
CSCwu76358	Existing and new alarm notifications disappear from Cisco Catalyst SD-WAN Manager after the upgrade to 20.18.3.
CSCwu18563	An authenticated privilege escalation vulnerability affects Cisco Catalyst SD-WAN Controller.
CSCwt06042	The system hides the Save option after a user modifies parameters in the Prisma tunnel configuration.
CSCwr07079	A crash file generation on Cisco Catalyst SD-WAN Manager causes the GUI to become unreachable temporarily.
CSCws99353	The Cisco Catalyst SD-WAN Manager application server reports timeouts for NETCONF sessions to Cisco XE SD-WAN Router following a burst of SSH connections from the stats-processor.

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

Resolved issues for Cisco IOS XE Catalyst SD-WAN, 26.1.2

Bug ID	Description
CSCws74808	The switch module shows the SVI link status inconsistently.
CSCwt66009	Upgrading the C8kv from 17.9 to 17.12 creates a duplicate VPN label 1003.
CSCws82489	Memory corruption in the timer wheel on IOS-XE SD-WAN causes a crash during policy detach/reattach.
CSCwu24891	TLS control connections flap every 30 seconds with the Cisco Catalyst SD-WAN Controller.
CSCwo90776	Race conditions during connrent and eagain states prevent the system from draining messages in the MQIPC buffer queue.
CSCwn63596	The system observes a vdaemon process crash in the SDWAN-SIT.
CSCwt71977	Enabling the " endpoint-tracker-settings name-lookup-over-sig" command causes the DIA tracker to remain down after a reload, while the SIG tracker remains up.
CSCwt59219	A memory leak in the cEdge vdaemon process causes a crash.
CSCwt79452	The system experiences OMP flaps with the device-ACL-policy configuration.
CSCws35252	Corruption in NVRAM causes the cEdge to lose its interface IP configuration.
CSCwt07060	The Cisco Catalyst SD-WAN Controller fails to push preferred-color-group-options to the cEdge if the preferred-color-group reference undergoes modification in the policy.
CSCwu42856	Application-Aware Routing (AAR) fails to function as expected.
CSCwt28048	The data policy fails to honor the preferred-color-group restriction.
CSCwt07572	The UTD silently consumes RADIUS packets.
CSCwt65192	SELinux blocks O365 and Webex CoRSaaS telemetry functionality.
CSCwt79239	The system observes a Crestone ucode crash at fnf_confd_oper_flow_cache_walk_sdwan while collecting cflowd stats/DPI.
CSCwt22006	Invalid configuration causes a Web UI bootstrapping failure, leading to persistent config merge errors despite subsequent corrections.
CSCws95387	The system fails to delete the PCG configuration from the data plane after removing the configuration.
CSCws86262	The Cisco IOS XE Catalyst SD-WAN device IPv4 GRE Tunnel API endpoint-tracker incorrectly uses IPv6 DNS.
CSCwu23624	OMP crashes with a SIGSEGV in the 17.18.2 Cisco IOS XE Catalyst SD-WAN device code.

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

Resolved issues for Cisco IOS XE Catalyst SD-WAN, 26.1.2.1

Bug ID	Description
CSCww79570	Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability.

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, 26.1.1

Bug ID	Description
CSCwt65192	SELinux violation logs relating to CXPD appear after configuration pull spamming logging buffer.
CSCws66553	Longer soak and clearing SD-WAN OMP events cause an fpmd crash.
CSCwt20467	Enabling the UTD feature causes an unexpected reboot on the Cisco Catalyst IOS XE Catalyst SD-WAN device.
CSCws35252	Corruption in NVRAM causes the Cisco Catalyst IOS XE Catalyst SD-WAN device to lose interface IP configuration.
CSCwt39760	NAT-DIA on a color based on a loopback fails to work.
CSCwt07572	UTD silently consumes the RADIUS packet.
CSCwt43938	The policy-map fails to match traffic, preventing QoS counters from incrementing the ISR1100X-4G.
CSCwt44263	The VPN ID is not maintained after enabling the UTD feature, causing ZBFW to evaluate an incorrect policy.
CSCwr76176	A dbg2:1 event causes the BFD SD-WAN PMTU to converge unexpectedly to 970 bytes.
CSCws98086	The " reason for state change: MAX" in the BFD syslog is updated.
CSCwt21819	The cfgmgr process causes a memory leak on the Cisco Catalyst IOS XE Catalyst SD-WAN device.
CSCwt28048	The data policy fails to honor the preferred-color-group restriction.
CSCws95387	PCG configuration is not deleted from the FP.
CSCwt02712	The 26.1 Cy3 Relops image on the Curie platform causes CPU degradation in the control plane.
CSCwt22006	Invalid configuration causes a web UI bootstrapping failure, leading to persistent configuration merge errors despite subsequent corrections.

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

Bug ID	Description
CSCwt27474	The removal of the hardcoded AS number 64512 Cisco SPA is required. Needs to be replaced with an autodetect mechanism.

Open issues for Cisco Catalyst SD-WAN Control Components, 26.1.1.1

Bug ID	Description
CSCwu18031	Breakage found in online/offline reporting for license inventory synchronization between SD-WAN Manager and CSSM.
CSCwt49624	UTD service failed to refresh the token, and UTD signature update doesn't occur.
CSCwt40320	429 rate limits prevent the GUI from loading properly for the SD-WAN Manager node.
CSCwt30535	SD-WAN Manager enforces non-repetitive character usage in strings.
CSCwt31445	An unhelpful message is displayed when the IOx application version fails to match the expected version.
CSCwr49368	SSE tunnels with Cisco Secure Access remain stuck in the SD-WAN configuration database.
CSCwt46293	An incorrect token in the sdavc-gw.conf file prevents SDAVC from starting.
CSCwr07079	A generated crash file causes the SD-WAN Manager GUI to become temporarily unreachable.

Open issues for Cisco IOS XE Catalyst SD-WAN, 26.1.2

Bug ID	Description
CSCwv84776	Intermittent crash from memory corruption in IOS-XE SD-WAN during repeated policy detach/reattach.

Open issues for Cisco Catalyst SD-WAN Control Components, 26.1.2

There are no customer impacting bugs that were identified in this release.

Open issues for Cisco Catalyst SD-WAN Control Components, 26.1.2.1

There are no customer impacting bugs that were identified in this release.

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

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

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.