Release Notes for Cisco Catalyst 8000V, Release 17.18.x

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

Cisco Catalyst 8000V Edge Software, Release 17.18.x 3
New software features 3
Resolved issues 9
Open issues 15
Related resources 17
Legal information 17

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

Cisco Catalyst 8000V Edge Software, Release 17.18.x

The key highlights of this release include:

- Support for deployments in Oracle Cloud Infrastructure
- Support for N4 and N2 compute instance families in Google cloud Platform (GCP)
- Support for D[s]_v5 compute instance family in Microsoft Azure
- Support for SR-IOV connectivity with Nvidia Mellanox ConnectX-7 and ConnectX-6 NICs for on-premise deployments
- Support for Ubuntu 22.04 LTS and RHEL 9.6 hypervisor
- Hosted Edge Services manages Cisco IOx applications
- Certificate Management unifies device certificates
- MVPN Ingress Replication over SRv6 simplifies multicast
- SRv6 Path MTU Discovery prevents fragmentation
- SRv6 Flex-Algo improves network resilience

New software features

This section provides a brief description of the new software features introduced in this release.

New software features in Cisco IOS XE 17.18.5

There are no new software features for this release.

New software features in Cisco IOS XE 17.18.4

There are no new software features for this release.

New software features in Cisco IOS XE 17.18.3a

Table 1. New software features for Cisco 8500 Series Secure Routers, Release 17.18.3a

Product impact	Feature	Description
Ease of set up	Support for Microsoft Azure on MANA Enabled Hosts	Starting with 17.18.3a, Cisco Catalyst 8000V Edge Software supports Microsoft Azure Network Adapter (MANA), enabling Catalyst 8000V Network Virtual Appliances (NVAs) on Azure VM series to run on MANA-capable hardware while maintaining compatibility with Azure's accelerated networking evolution. For more information, see Remediate: Advisory – Catalyst 8000V Running in Microsoft Azure on MANA Enabled Hosts.

New software features in Cisco IOS XE 17.18.2

Table 2. New software features for Cisco 8500 Series Secure Routers, Release 17.18.2

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

Product impact	Feature	Description
Ease of set up	Support for Microsoft HyperV on Azure Local certified servers	Cisco IOS XE 17.18.2 supports the deployment of Cisco Catalyst 8000V virtual router on Microsoft HyperV hypervisor in Microsoft HCI OS version 23H2 operating system software that runs on Microsoft Azure Local (formerly also known as Azure Stack HCI) certified servers. The deployment support includes network connectivity via NetVSC driver. Use the Cisco Catalyst 8000V .iso image and Microsoft HCI OS PowerShell CLIs for these deployments. Support for deployment on Azure Local is also enabled for Cisco Catalyst 8000V running Cisco IOS XE 17.15.5 release. For more information, see Azure Local.
Ease of set up	Support for Nutanix AHV Hypervisor	Cisco IOS XE 17.18.2 supports the on-premises deployment of Cisco Catalyst 8000V virtual router on Nutanix AHV (Acropolis Hypervisor) bundled in Nutanix AOS version 7.3 (Acropolis Operating System). Nutanix AHV is a type-1 bare-metal hypervisor based on Linux KVM technology. Support includes SR-IOV fast-path connectivity for Nvidia Mellanox ConnectX-6 NICs. For other NICs you can use VirtIO connectivity. Use the Cisco Catalyst 8000V .iso image or the .qcow2 image for these deployments. You can perform the deployment by using Nutanix Prism Central dashboard, Nutanix Prism Element dashboard, Nutanix AOS REST APIs, or Nutanix AOS CLIs. Support for deployment on Nutanix AHV is also enabled for Cisco Catalyst 8000V running Cisco IOS XE 17.15.5 release. For more information, see Nutanix support. For more information, see Nutanix support.
Ease of use	Support for RHEL 9.6 hypervisor for KVM hosts	Cisco IOS XE 17.18.2 release supports the deployment of Cisco Catalyst 8000V on Red Hat RHEL 9.6 operating system with KVM hypervisor.
Ease of use	Support for Nvidia Mellanox ConnectX-7 network interface cards	Cisco IOS XE 17.18.2 release supports SR-IOV connectivity for Nvidia Mellanox ConnectX-7 Network Interface Cards (NICs) that deliver higher throughput and performance for the supported hypervisors.
Security	Resilient Infrastructure	Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives. This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release: • **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files. *Recommendation*: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials. • **SSHv1** *Recommendation*: Use SSHv2.

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

Product impact	Feature	Description
		• **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption** *Recommendation*: Use SNMPv3 with authentication and encryption (authPriv). • **MD5 (authentication) and 3DES (encryption) in SNMPv3** *Recommendation*: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption. • **IP source routing based on IP header options** *Recommendation*: Do not use this legacy feature. • **TLS 1.0 and TLS 1.1** *Recommendation*: Use TLS 1.2 or later. • **TLS ciphers using SHA1 for digital signatures** *Recommendation*: Use ciphers with SHA256 or stronger digital signatures. • **HTTP** *Recommendation*: Use HTTPS. • **Telnet** *Recommendation*: Use SSH for remote access. • **FTP and TFTP** *Recommendation*: Use SFTP or HTTPS for file transfers. • **On-Demand Routing (ODR)** *Recommendation*: Use a standard routing protocol in place of CDP-based routing information exchange. • **BootP server** *Recommendation*: Use DHCP or secure boot features such as Secure ZTP. • **TCP and UDP small servers (echo, chargen, discard, daytime)** *Recommendation*: Do not use these services on network devices. • **IP finger** *Recommendation*: Do not use this protocol on network devices. • **NTP control messages** *Recommendation*: Do not use this feature. • **TACACS+ using pre-shared keys and MD5** *Recommendation*: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1

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

Product impact	Feature	Description
Software Reliability	High availability for DHCP servers	In a high availability set up DHCP servers are deployed in an active/standby deployment model where two Cisco IOS XE DHCP servers synchronize DHCP bindings (IP address records). This synchronization ensures that if the active device fails, the standby device seamlessly assumes the Active role, preserving IP address records and maintaining uninterrupted network service.
Ease of Setup	IPv6 Rule and Rule Set Support in Security Policies	From Cisco IOS XE 17.18.2, you can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager.
Upgrade	IPv6 GRE-TP tunnel as protected link support for SRv6 TI-LFA with IS-IS	From Cisco IOS XE 17.18.2, this feature extends IPv6 GRE-TP tunnel as protected link support for SRv6 TILFA with ISIS.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with OSPFv2	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPFv2.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with IS-IS	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with ISIS.
CUBE FEATURES		
Upgrade	Directional attribute compliance for SIPREC responses	From Cisco IOS XE 17.18.2 onwards, for a recorder response with INACTIVE SDP attributes, CUBE stops media packets transmission towards that recorder.
Security	Security warnings for usage of legacy TLS and associated weaker ciphers – CUBE and SRST	From Cisco IOS XE 17.18.2 onwards, CUBE and SRST display warning messages during handshake for configurations with legacy TLS (v1.0, v 1.1) and associated weaker cipher.

New software features in Cisco IOS XE 17.18.1a

This section provides a brief description of the new software features introduced in this release.

Table 3. New software features for Cisco Catalyst 8000V Edge Software, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Support for deployment of Catalyst 8000V in Oracle Cloud Infrastructure	Oracle Cloud Infrastructure (OCI) is a cloud service that enables you to build and run a range of applications and services in a hosted environment. OCI provides high-performance compute capabilities as physical hardware instances and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network. From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V is supported for deployments in OCI on VM.Standard.E5.Flex compute instances for Bring Your Own License (BYOL) consumption.

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

Product impact	Feature	Description
Ease of Use	Support for N4 and N2 compute instance families in Google cloud Platform	Cisco Catalyst 8000V supports the N2 compute instance family as well as the N4 compute instance family with gVNIC driver support for Google Cloud Platform (GCP) deployment.
Ease of Use	Support for D[s]_v5 compute instance family in Microsoft Azure	Cisco Catalyst 8000V supports the D[s]_v5 compute instance family for Microsoft Azure deployments from Cisco IOS XE 17.18.1a release.
Software Reliability	Support for Nvidia Mellanox ConnectX-6 network interface cards	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V supports the Nvidia Mellanox ConnectX-6 Network Interface Cards (NICs) with port speeds of up to 40 GbE. Also, the supported VNIC drivers for SR-IOV connectivity is expanded to include CX6VF.
Ease of Use	Support for Ubuntu 22.04 LTS	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V supports Ubuntu 22.04 LTS version open-source OS on Linux.
Software Reliability	Throughput performance optimizations	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V delivers higher throughputs for both encrypted and unencrypted traffic. We recommend you benchmark your unique traffic profiles prior to production. The performance improvements will depend on your feature set, packet sizes, and the number of vCPU cores.
Licensing Process	Licensing compliance, reporting, and notification enhancements	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Ease of Use	Hosted Edge Services for SD-Routing Devices	From Cisco IOS XE 17.18.1a release, Cisco Catalyst SD-WAN Manager supports deployment of IOx applications such as Cyber Vision, Thousand Eyes, UTD, and so on. The support to monitor these applications is introduced through Hosted Edge Services monitoring dashboard which offers a simplified user experience for overseeing IOx container applications across multiple devices. The Hosted Edge Services monitoring dashboard is introduced on Cisco Catalyst SD-WAN Manager version 20.18.x.
Ease of use	Managing NGFW Policies from Security Cloud Control	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Security	Custom IPS signature sets	From Cisco IOS XE 17.18.1a release, Custom IPS signature sets are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets. This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS

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

Product impact	Feature	Description
		signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	Certificate Management on SD-Routing Devices	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Upgrade	MVPN Ingress Replication (IR) over SRv6	This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	SRv6 Path MTU Discovery	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.
Upgrade	SRv6 Flex-Algo with TI-LFA and uLoop Avoidance	From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Upgrade	MVPN Ingress Replication (IR) over SRv6	This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Licensing Process	Product Analytics for routers	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
CUBE FEATURES		
Ease of Use	Enhanced support for serviceability in SIP recording	From Cisco IOS XE 17.18.1a onwards, serviceability is enhanced to display consolidated information on forked and associated anchor call legs.
Upgrade	Third-Party GUID capture for correlation between call transfers and SIP-based recording	From Cisco IOS XE 17.18.1a onwards, the Third-Party GUID capture for correlation between calls and SIP-based recording is extended to support transmission of globally unique identifiers (GUIDs) to the recording server during call transfers.
Upgrade	IOS UC apps reports smart licensing flex subscription entitlement tag	From Cisco IOS XE 17.18.1a onwards, CUBE and SRST smart licensing reports flex subscription entitlement tag on all the supported platforms.

© 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 bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Resolved issues in Cisco IOS XE 17.18.5

Table 4. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 17.18.5

Bug ID	Description
CSCwu97838	RADSEC TLS peer validation fails when unrelated trustpoints share a common PKI Root CA
CSCwv41991	Device w/C-NIM-2T XE - Link is not advertising its AUTONEG capability which results in link down/down state
CSCwv55092	Upgrade rollback due to recursive SNMP BGP trap deprecated-model migration
CSCwq96185	SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak
CSCwu97716	Unexpected Device Reload Triggered by DHCP Service Failure During Lease Conflict Scenarios
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.
CSCwu99434	Unexpected Device Reload During Rapid Trustpoint Deletion and Creation Events Resulting in Core File Generation
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwu12631	Posture redirection not working on SD-WAN router switch module
CSCwt81568	Route-replicate command is present in configuration but is not taking effect after reload.
CSCww06413	PKCS12 re-import silently fails to install a CA certificate
CSCwt42293	IR8140: Cellular interface flap causing crypto enrollment failure
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwt98537	QoS unsupported configuration makes route processor crash
CSCwq08386	Device platform Tier 3 throughput clarification
CSCwt75037	Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwr69095	DNS requests for vBond fail
CSCwu00043	LSC certificate failure " CRYPTO_PKI: Failed to add ca req pool entry 538" in scale environment

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

Bug ID	Description
CSCwu61766	SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration
CSCws92932	Unexpected reload due to Segmentation Fault on TPS IPC Process
CSCwt44596	Router fails to bring up BFD over IPSEC Tunnel when underlay path is using switching module instead of on-board interface.
CSCwu27937	system-report handling has a conflict - unrelated processes may dump core after a cpp/ucode fault.
CSCwt66413	ncsshd process fails to terminate after " no netconf" and netconf refuses connection
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface
CSCwt13176	Memory leak detected in TLS testcase
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router
CSCwv37592	Unable to configure no exec under async line or async range IOS-XE SDWAN 17.15
CSCwu21682	Segmentation Fault at Process = SASCheckInit (or other process)
CSCwu93056	Device may reload after remove an endpoint.
CSCwt51797	[IOS XE] RIPv2 will stop sending multicast routing updates after interface flap
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header
CSCwr74339	vman crashed @ __GI___clock_nanosleep in router reload and power cycle test
CSCwr47230	Upgrade failed " Install operation not allowed because verification of image is in progress."
CSCwt69544	QFP Ucode device crash
CSCwv39390	IOS-XE router generates FMANRP_ESS-3-ERREVENT logs with tracebacks
CSCwu97638	IOS-XE unexpected reload due to ACL pointer corruption with SNMPv3
CSCwt51754	Router reloaded after adding voice related configuration
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwu45273	LISP ITR sources locally-originated control-plane packets from the numerically lowest configured RLOC IP instead of the outbound interface address
CSCwu11498	show interface counter become abnormal
CSCws26006	Device SFP EN LED light green when no SFP inserted

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

Bug ID	Description
CSCwu76495	SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwt34226	SSH Connectivity Issue with On-Demand Next Hop in Segment Routing Traffic Engineering (SR-TE)
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on the device
CSCwu01733	Rapid memory leak in ompd after ISE integration with vManage
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)
CSCwv41407	BGP updates that should be suppressed are advertised with incorrect attribute after RPSO
CSCwu21682	Segmentation Fault at Process = SASCheckInit (or other process)
CSCwv61185	Device daemon may flap SD-WAN control connections with HWCERTREN when multiple vManage-signed edge certificates have identical Not Before timestamps.
CSCwu93056	Device may reload after remove an endpoint.
CSCwt51797	[IOS XE] RIPv2 will stop sending multicast routing updates after interface flap
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header
CSCwr74339	vman crashed @ __GI___clock_nanosleep in router reload and power cycle test
CSCwr47230	Upgrade failed " Install operation not allowed because verification of image is in progress."
CSCwt69544	QFP Ucode C8500L crash on 17.15.4c
CSCwu97638	IOS-XE unexpected reload due to ACL pointer corruption with SNMPv3
CSCwt51754	Router reloaded after adding voice related configuration
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwu45273	LISP ITR sources locally-originated control-plane packets from the numerically lowest configured RLOC IP instead of the outbound interface address
CSCwu11498	show interface counter become abnormal
CSCwv39390	IOS-XE router generates FMANRP_ESS-3-ERREVENT logs with tracebacks
CSCwu76495	SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwt34226	SSH Connectivity Issue with On-Demand Next Hop in Segment Routing Traffic Engineering (SR-TE)
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on the device

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

Bug ID	Description
CSCwu01733	Rapid memory leak in ompd after ISE integration with vManage
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)
CSCwu31545	Device control connections/basic ping fail after CSCwt77501 fixed image due to incomplete autoinstall suppression in controller mode
CSCwv69412	1.3.6.1.4.1.9.9.86.1.6.4.1.13.x value keep stale value until execute show dspfarm all
CSCwt88212	Untagged packets dropped with non-default native VLAN on ISR4K
CSCwq98154	[XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwr24042	[SDWAN-Mcast]:Traffic going to all CEDGES without receivers where Replicator stuck in P MDT
CSCwu49303	Memory Leak in cpp_sp_svr due to Classification Objects
CSCwv25890	Support for GRE+MPLS on tunnel transport mode

Resolved issues in Cisco IOS XE 17.18.4

Table 5. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 17.18.4

Bug ID	Description
CSCwt76906	C9K: Continuous increase in holding memory for CTS CORE
CSCwt47516	WLC crash due to corrupted length field during AAA processing
CSCwt94106	Pubd core generated for C9300
CSCwu04279	System instability and potential service disruption after invalid GPM load
CSCwu03804	C9000: Randomly during operation - Interface VLAN / SVI go missing from "show run" but remain up. Configs are lost upon reload.
CSCwu21451	C9250/C9350: Cluster manager crash for stacked devices with specific mac address combination
CSCwt51443	Controller crashed due to CPUHOG under DBAL_EVENTS
CSCwt86654	IOS-XE: IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to C8570-G2/C8500-12x4QC in SDWAN and SD-Routing
CSCwn80721	Unexpected Reboot in Process Sessmgrd
CSCwt87294	mDNS Cache-Flush behavior not consistent

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

Resolved issues in Cisco IOS XE 17.18.3a

Table 6. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 17.18.3a

Bug ID	Description
CSCwr42574	C8Kv MLX5 main interface ping fails if subinterfaces are configured
CSCws72902	C8200/C8300/C8500L: Overrun drops due to uneven GRE traffic distribution across data plane cores
CSCwr90843	SD-WAN Edge: Device may reload unexpectedly under heavy IPSec Traffic Load
CSCwr72709	Router crash in TDM-TDM call when debug voip fpi enabled
CSCws66278	Unable to install Cisco PKI controller certs on MT overlay
CSCws68039	C8200: Unable to configure HSRP Groups up to the maximum limit
CSCws28994	CPP crash while processing QoS rate profile
CSCwr95551	c8kv crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT
CSCwr84985	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
CSCws32991	C1100TGX does not honor jumbo MTU on WAN ports after reboot
CSCws95993	Seeing T1 license in use even after configuring T2.
CSCws30718	Dataplane Crash Observed on CGN NAT Scale Router after " clear ip nat translation *"
CSCwt18839	Segmentation Fault in cpp_cp_svr while Printing FIA Trace Data
CSCws77372	Software crash with fman_fp core due to NAT-related show commands
CSCwr44547	SDWAN Manager: Reporting abnormal loss value for tunnel stats in the UI
CSCws80232	SD-WAN Edge: Zone-Based Firewall Not Programmed Correctly Resulting in Class-Default Match
CSCwt46335	MAP-E: stop sending IPv4 traffic during MAP rule refresh
CSCwq60752	Catalyst 8000 FP Crash After Clearing NAT Translations
CSCws58529	When the name server is specified using IPv6, half entries are created due to unintended NAT.
CSCws76668	Memory leak udner " fman_fp_image" on CAT8500 routers when NAT is enabled.
CSCwt22873	High QFP Caused by " all-host" Limit in - Carrier Grade NAT mode

Resolved issues in Cisco IOS XE 17.18.2

Table 7. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 17.18.2

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

Bug ID	Description
CSCwr42950	On-demand tunnels in SD-WAN do not expire when Universal Mobile Telecommunications System (UMTS) is enabled.
CSCwq51935	A NAT64 static entry is removed when a command to delete a non-existent entry is applied.
CSCwe19394	The device may boot up with the previous packages configuration file due to a power outage.
CSCwr77958	Network-Based Packet Inspection (NWPI) is not capturing self-generated syslog traffic.
CSCwj61730	The router may crash when Security Group Tag (SGT) caching is removed from an interface.
CSCwq77322	The router sends a 2-byte packet for the FLOW_SAMPLER_RANDOM_INTERVAL field instead of a 4-byte packet.
CSCwr24031	After an upgrade, the SD-WAN service tracker in a VRF instance may select the source IP address from the global routing table when Multiprotocol Label Switching (MPLS) Inter-AS Virtual Private Network (VPN) option B is configured.
CSCwr49794	Integrated Services Router (ISR) exporters with Encrypted Traffic Analytics (ETA) enabled generate invalid template data errors in Secure Network Analytics (SNA).
CSCwq98206	The Enhanced Policy-Based Routing (EPBR) set interface action is missing after a reboot.

Resolved issues in Cisco IOS XE 17.18.1a

Table 8. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 17.18.1a

Bug ID	Description
CSCwn42496	Devices lose all BFD sessions while control connections remain up
CSCwn69868	Unable to come up with control connections with controllers after controllers added and down/up
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them
CSCwo84428	Memory leak under vdaemon process with DTLS on SNMP polling
CSCwp24639	Device reloads after VPN configuration changes
CSCwm72336	CXP with data policy redirect-DNS via overlay causes blackhole
CSCwn26353	BFD sessions via TLOC-ext do not come up when IPv6 is dynamically changed
CSCwo05703	VFR is not dynamically disabled after ZBFW removal
CSCwo75657	Maximum control connection is not equal to maximum OMP sessions
CSCwp91064	FTMD zero pointer dereference is seen leading to crash
CSCwp23487	SGW offline with SSH error Unable to open socket while establishing netconf session

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

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. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Open issues in Cisco IOS XE 17.18.5

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

Open issues in Cisco IOS XE 17.18.4

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

Open issues in Cisco IOS XE 17.18.3a

Table 9. Open issues for Cisco Catalyst 8000V Edge Software, Release 17.18.3a

Bug ID	Description
CSCwq96185	SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak

Open issues in Cisco IOS XE 17.18.2

Table 10. Open issues for Cisco Catalyst 8000V Edge Software, Release 17.18.2

Bug ID	Description
CSCws30834	The router ignores the keepalive command under the Secure Internet Gateway (SIG) tunnel interface when pushed by the management platform.
CSCws13857	Incorrect NAT occurs from the service Virtual Routing and Forwarding (VRF) to the global table for self-generated Internet Control Message Protocol (ICMP) Time Exceeded (Type 11) packets
CSCwq77458	The forwarding manager process crashes after Flexible NetFlow (FNF) configuration changes.
CSCwr87083	The router is unable to onboard SD-Routing devices using a generic bootstrap file stored on a USB drive.
CSCwo42664	Periodic service restarts on the edge device may generate crash files
CSCws18137	Configuration is out of sync when a CLI template is attached, due to a missing authentication element in the configuration).
CSCwr64075	During extended testing, a core dump related to the QFP microcode was observed, indicating an issue within a thread responsible for managing memory ring operations.
CSCwr76580	Unexpected behavior occurs with Secure Internet Gateway (SIG) tunnels configured from the management platform to the Umbrella service.
CSCwr60310	Template push or CLI configuration updates may fail due to duplicate VTY or asynchronous lines in the configuration.
CSCwr30573	TLOC extension cannot be programmed due to module boot-up timing issues.

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

Bug ID	Description
CSCws25557	Only Transport Layer Security (TLS) 1.2 cipher suites are supported for control connections.
CSCwr95551	The router fails when configuring SSL VPN with PBR and NAT.
CSCwr08462	There is an issue where the NAT router does not respond to Address Resolution Protocol (ARP) requests.
CSCwr44921	The router fails due to high CPU usage when memory pressure exceeds the threshold.
CSCwr97784	Slow performance is observed on Network Configuration Protocol (Netconf) Remote Procedure Call (RPC) with stateless static NAT translation.
CSCwr55240	The router experiences a critical process fault in the Operations, Management, and Policy Daemon (OMPD) on the route processor.
CSCwr84985	The authentication process daemon (dmiauthd) crashes, causing the configuration to become unsynchronized between the startup and running configuration files.
CSCwq24119	A traceback is seen when detaching customer configurations for a railway client.
CSCwm97460	The control connection to the management platform is only attempted over the highest priority Transport Locator (TLOC).
CSCwr00088	A CLI option is needed to change the query interval for per-Multiprotocol Label Switching (MPLS) label Cisco Express Forwarding (CEF) statistics on the forwarding manager
CSCwr88206	The Forwarding Information Base (FIB) table routes have a corrupted Next Hop (NH) ID 0, which is assigned to a value other than blackhole
CSCwr72709	The router fails during Time-Division Multiplexing (TDM) calls when debug Voice over IP (VoIP) Forwarding Path Interface (FPI) is enabled
CSCws12946	Port forwarding issues occur on the router when using multiple Internet Service Providers
CSCwq98154	Multicast traffic is not forwarded over point-to-point Dynamic Multipoint VPN (DMVPN) phase 1 tunnel.
CSCwr49475	BFD sessions flap and do not recover because the symmetric NAT (SYMNAT) port is not updating to the data plane.
CSCwq59240	The Gigabit Ethernet interface does not consistently obtain an IP address from Dynamic Host Configuration Protocol (DHCP)
CSCwr64257	The router experiences an unexpected reload due to the forwarding and traffic management daemon.
CSCws26373	The router unexpectedly reboots due to NAT in the data plane after a policy is pushed.
CSCwm71868	Stopping the virtual router in a cloud environment results in a device reload, followed by a shutdown after 10 minutes
CSCwr46263	Interface counters do not increment when using the 'show interfaces' command on the virtual router
CSCwp97178	Flapping NAT causes BFD session loss, and the IPSec session is shown as down.

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

Bug ID	Description
CSCwr76176	Path Maximum Transmission Unit Discovery (PMTUD) for BFD over SD-WAN converges unexpectedly to 970 bytes after a diagnostic event.
CSCws30834	The virtual router fails in the cryptography library

Open issues in Cisco IOS XE 17.18.1a

Table 11. Open issues for Cisco Catalyst 8000V Edge Software, Release 17.18.1a

Bug ID	Description
CSCwp12196	Router unexpectedly reloads due to memory corruption on a notification queue in FTMd
CSCwq27426	BFD session down due to unencrypted outbound BFD packets despite active IPsec SA
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwo42664	Keyman core files on device
CSCwp01089	EPFR-High latency times are observed on the hub device
CSCwp81539	Memory leak under cfgmgr process on SNMP polling
CSCwq20326	Device does not install service-side static route to CEF after upgrade
CSCwq40026	Unexpected reboot occurs due to Process FTMD
CSCwq68385	TLOC disabled after link is down; no automatic tunnel recovery after link restores and TLOC state is Up

Related resources

- Cisco Catalyst 8000V Edge Software Product Page
- Cisco Catalyst 8000V Edge Software Data Sheet
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide
- Cisco Catalyst 8000V Edge Software High Availability Configuration Guide
- Troubleshooting Guide for Cisco Catalyst 8000V Edge Software
- Configure Licenses and Throughput for Cisco Catalyst 8000V Edge Software

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: www.cisco.com/go/trademarks. 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. (1110R)

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 included 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.