Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-26

Last Modified: 2024-02-29

Full Cisco Trademarks with Software License

Cisco Catalyst 8000V Edge Software Overview

About Cisco Catalyst 8000V

Cisco Catalyst 8000V Edge Software or Cisco Catalyst 8000V is a software-based, virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in on-prem branches, data centers, colocation data centers, and public clouds.

Cisco Catalyst 8000V supports NIM modules on Cisco ENCS platforms, runs on any x86 platform, and is supported on ESXi, KVM, NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

When you deploy Cisco Catalyst 8000V as a VM, the Cisco IOS XE software behaves similar to a traditional Cisco router (hardware platform). You can configure different features depending on the Cisco IOS XE software version.

Features

- **Hardware independence**: The Cisco Catalyst 8000V router uses the benefits of virtualization in the cloud to provide hardware independence. Since the Cisco Catalyst 8000V runs as a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of host hardware resources**: The host server hardware resources such as CPU cores, memory, and disk are managed by the hypervisor, and these resources are shared among the guest VMs. You can regulate the amount of hardware resources assigned to a specific Cisco Catalyst 8000V VM instance.
- **Flexibility in deployment**: You can easily move a VM from one server to another. Thus, you can move a Cisco Catalyst 8000V instance from a server in one physical location to a server in another physical location without moving any hardware resources.
- **Enhanced software security - Secure Object Store**: In Cisco Catalyst 8000V, storage partitions for NVRAM, licensing, and other data are created as object stores. The individual object stores are encrypted to ensure data security, and this product is Cisco Secure Development life cycle (CSDL) compliant. Further, Cisco Catalyst 8000V supports a 16G disk cycle profile.

Hardware Requirements

For hardware requirements and installation instructions, see the Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.

Software Images and Licenses

The following sections describe the licensing and software images for Cisco Catalyst 8000V.

Cisco Catalyst 8000V Software Licenses

The Cisco Catalyst 8000V is licensed based on throughput, feature-set, and the licensing term. This product supports Cisco Smart Licensing Usage Policy as well as Cisco DNA Licensing. Based on whether you want to go for purchased licenses that go with the Cisco Catalyst 8000V instance, or a subscription-based license, choose one of the following options:

Subscription-Based Licensing via Cisco DNA

You can purchase a subscription license for Cisco Catalyst 8000V through the following three licenses that are available via Cisco DNA:

- Cisco Catalyst 8000V - Network-Premier
- Cisco Catalyst 8000V - Network-Advantage
- Cisco Catalyst 8000V - Network-Essentials

For more information on Cisco Catalyst 8000V DNA licensing, see Cisco DNA Software for SD-Wan and Routing Ordering Guide.

Bring-Your-Own-Licensing

You also have an option to purchase and use licenses with Cisco Catalyst 8000V as a Bring-Your-Own-License (BYOL) instance or as a Pay-As-You-Go (PAYG) instance.

To use a Cisco Catalyst 8000V - BYOL license, see Licenses and Licensing Models to know to how install and configure your license.

If you have upgraded to Cisco Catalyst 8000V from a Cisco CSR 1000V or a Cisco ISRV, you must use Smart Licensing Using Policy (SLP). Traditional licenses do not work after the upgrade.

Pay-As-You-Go Licensing

Cisco Catalyst 8000V supports the PAYG Licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace. Cisco Catalyst 8000V hourly-billed AMI or Pay As You Go licensing model allows you to consume an instance for a defined period of time. In this licensing model, you can directly launch the instance from the AWS or Azure Marketplace and start using the instances. The licenses are embedded in the image.

Note For demo or evaluation licenses, contact your Cisco Account Team if you have a direct purchase agreement with Cisco, or your Cisco Partner or Reseller.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Software Image Nomenclature for Installation Files

The Cisco Catalyst 8000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Cupertino 17.9.1a release:

- c8000v-universalk9.17.09.01a.ova
- c8000v-universalk9.17.09.01a.iso
- c8000v-universalk9.17.09.01a.qcow2

The following table lists the filename attributes along with its properties:

Table 1: Installation Filename Attributes

Filename Attribute	Properties
universalk9	Specifies the package that you are installing.
17.09.01a	Indicates that the software image is mapped to the Cisco IOS XE Cupertino 17.9.1a release.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Enhanced Features for Cisco IOS XE Cupertino 17.9.x

New and Changed Software Features in Cisco IOS XE 17.9.5a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

New and Changed Software Features in Cisco IOS XE 17.9.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.3a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.2a

There are no new software features in this release.

New and Enhanced Features for Cisco IOS XE 17.9.1a

Note Cisco IOS XE Cupertino 17.9.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE Cupertino 17.9.x release series.

Table 2: Software Features

Feature	Description
Support for ConnectX-5VF vNIC	Cisco Catalyst 8000V now supports the ConnectX-5VF Virtual Network Interface (vNIC) card for deployments in ESXi, KVM, and NFVIS (CSP) environments. This enhancement provides multiple benefits including advanced hardware offloads to reduce CPU resource consumption and enhanced drive for high packet rates and throughput. See also Requirements for KVM Installation and Installing Cisco Catalyst 8000V in NFVIS Environment.
Support for c5n.18xlarge instance type	Cisco Catalyst 8000V running on Amazon Web Services (AWS) now supports the c5n.18xlarge instance type for deployment. This instance type supports Elastic Fibre Adapter (EFA) that enhances performance especially in network intense solutions.
AWS Enhancements	Cisco Catalyst 8000V running on AWS supports performance enhancements with higher number of queues, thereby increasing the packet processing rate.
Support for Unicast-to-Multicast Destination Reflection	This feature introduces support for configuration of unicast-to-multicast destination reflection to facilitate unicast-to-multicast destination translation and unicast-to-multicast destination splitting. It also provides the capability for users to translate externally received unicast destination addresses to multicast addresses.
Support for BGP additional paths with label-unicast unique mode	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured.

Feature	Description
ACE Scale Limit Per OGACL	This feature provides the capabilities to increase the Common Adaptive Classification Engine (CACE) scale limit per ACL and object group (OG) ACL. Currently, the CACE supports only 64K ACEs per ACL and it can have 64K networks in the source and destination OGs per policy.With the increase in CACE limit to 256K, Cisco Catalyst 8000v Edge Software can now support 150K ACE entries per ACL with 270K ACEs per system across five ACLs. Additionally, the device can support 3000 ACE entries per OGACL and 2400 OGs with 100 networks per OG.Cisco Catalyst 8000v must have 8 GB memory to support this configuration.

Table 3: Cisco Unified Border Element (CUBE) Features

Feature	Description
CUBE: End-to-end Secure Calling for Courtesy Call Back and Unified Contact Center Survivability	With the Cisco Voice Portal (CVP) application, a caller may request an automatedcallback, rather than wait in a queue for an extended period. When an agent becomes available, CVP sends a request to place a call to the original caller. When the call is answered, the agent is connected. With this update, outbound calls over a secure SIP PSTN trunk are possible.
CUBE: Load Balancing for DNS SRV Host	This enhancement to the DNS session target feature, provides effective call distribution and load balancing of calls based on the preference, priority and availability of hosts provided in DNS SRV Resource Records. This feature further simplifies configuration by allowing effective call distribution with a single dial-peer.
CUBE: Options Ping for DNS SRV Hosts	Previously, CUBE (Local Gateway) had to be configured with separate dial-peers to monitor the availability of individual proxies used in services such as Webex Calling. To simplify this configuration, all targets resolved from a DNS SRV record may now be monitored using a common Options Ping policy defined for a single dial-peer. If a remote server becomes unresponsive, CUBE will busy out that destination, allowing calls to be sent to alternative destinations.
Transfer of Call Detail Records Using SFTP	Cisco IOS gateways can use FTP and now SFTP servers to transfer call accounting files.

Note Customers using the CUBE WebSocket forking feature with the Cisco Agent Answers solution should not use the Cisco IOS XE Cupertino 17.9.1a release. We recommend that you use the Cisco IOS XE Bengaluru 17.6.x release for this feature.

Table 4: Smart Licensing Using Policy Features

Feature	Description
Managed Service License Agreement (MSLA) Support with Smart Licensing Using Policy.	For Cisco Catalyst 8000V running in the autonomous mode, you can now implement a post-paid model for licenses, where you pay for the actual usage of a license instead of pre-paying for the licenses you may require. This model requires an MSLA with Cisco, and licenses with subscription ID. (Licenses with subscription IDs to be ordered on Cisco commerce workspace (CCW). The licenses are deposited in the specified Smart Account and Virtual Account in CSSM, with the corresponding subscription IDs. To complete licensing workflows, you can implement a topology where the product instance interacts directly with Cisco Smart Software Manager (CSSM), via Cisco Smart Licensing Utility (CSLU), or via Smart Software Manager On-Prem (SSM On-Prem), or it can operate in a disconnected mode. A product instance that uses licenses with subscription IDs must also enabled with a "utility mode". Communication to and from the product instance is flagged to indicate that it is in the utility mode. A product instance in the utility mode requires a Resource Utilization Measurement Acknowledgement (RUM ACK) installed every 30 days. You are billed based on the throughput and the Cisco DNA subscription tier that is activated and in-use.

Feature	Description
New mechanism to send data privacy related information	A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy {all | hostname | version}** command in global configuration mode), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in an offline file. For more information, see license smart (global config).
Hostname support	Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, and SSM On-Prem. It is then displayed on the corresponding user interface. For more information, see license smart (global config). With the introduction of this enhancement, the hostname limitation which existed from Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Cupertino 17.8.x – is removed. In these earlier releases, hostname information is not sent or displayed on various licensing utilities (CSSM, CSLU, and SSM On-Prem).

Feature	Description
RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.
Virtual Routing and Forwarding (VRF) Support	On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem. **Note** When using a VRF, the supported transport types are **smart** and **cslu** only. For more information, see license smart (global config).

Resolved and Open Bugs - Cisco IOS XE 17.9.x

Resolved Bugs - Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwh71278	Appx license boot level config lost in running-config after upgrade

Identifier	Headline
CSCwe90501	Upgrade fails due to advertise aggregate with VRF
CSCwf74668	HSEC licenses incrementing
CSCwh73350	Device keeps crashing when processing a firewall feature
CSCwf70596	Fix VLAN replay for SRIOV i40e interface after link flap
CSCwf67564	Device observes memory leak at process SSS Manager
CSCwf23291	Write or Do Write saves configuration but RSA keys /SSH lost after reload
CSCwc79115	Policy commit failure notification and alarm from vsmart
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP
CSCwh68508	Unexpected reboot occurs after establishing control plane of EVPN MPLS and receiving packets
CSCvo01546	NHRP reply processing may dequeue an unrelated request
CSCwf03193	Device crashes and crashinfo files generated with segmentation fault, process IPSEC key engine
CSCwh08434	OMP route is being advertised although the route is not available
CSCwf24164	Netflow stops working when flow monitor reaches cache limit
CSCwf65540	Running more than four tests on ThousandEyes Agent causes tracebacks on device running TE in docker container
CSCwi28227	NAT HSL logging vrf-filter not working
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwh49644	CSDL compliance failure : Use of 3DES by IPSec is denied
CSCwh32386	Unexpected reload on device due to critical process fman_fp_image
CSCwe30514	Device reboots with sslproxy and utd are enabled
CSCwh30377	Device data plane crashes in Umbrella/OpenDNS processing due to incorrect UDP length
CSCwf34171	The **configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices
CSCwf96980	Unexpected reboot after configuring application redundancy
CSCwe64779	IOS XE router software forced reset during high IPC congestion with IPsec

Identifier	Headline
CSCwh01425	ITU channel configuration not working
CSCwh20577	Crashed by TRACK client thread at access invalid memory location
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot
CSCwf82676	CPU usage mismatch in **show sdwan system status** vs **show proc cpu platform**
CSCwh36801	Crash in IP Input process during tunnel encapsulation
CSCwh96415	Cannot disable DMVPN logging
CSCwe85301	Crypto PKI-CRL-IO_0 process crashes when PKI trustpoint is being deleted
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwc97579	Spoke-spoke cache refresh does not work correctly in case of multiple cache entries for same next hop
CSCwf11394	IOS XE - Vdaemon debug log should mention port-hop and reason prior to DISTLOC
CSCwf04866	Keyman process crash seen while re-generating SSH key
CSCwh00332	B2B NAT: When configring IP nat inside/outside on VASI intereface,ack/seq number is abnormal

Open Bugs - Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwh74249	IPv6 PMTUD packet is fragmented at 1494 bytes
CSCwi40603	Memory leak in the crypto IKMP process
CSCwi34858	VLAN sub interfaces do not pass traffic after upgrade
CSCwh18120	The IKEv2 Diagnose feature is taking 11% CPU during session bring up
CSCwh22414	Warning and critical CPU utilization thresholds are not recomputed when using data-plane-heavy mode
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason
CSCwh12093	Enable SoS/ROC feature for DSL
CSCwi06843	Endpoint tracker triggers a CPU hog
CSCwi53306	Unknown appID in ZBFW HSL log
CSCwi06404	PKI crashes after failing a CRL Fetch

Identifier	Headline
CSCwi46997	NAT command not readable after reloaded
CSCwi33168	DSP reporting out of range utilization values in SNMP
CSCwi08171	Router may crash due to crypto IKMP process
CSCwi53951	Packets with Unicast MAC get dropped on a port channel L2 Sub-intf after a router reboot
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI
CSCwh50510	Router crashes with 'Segmentation fault(11), Process = NHRP' when processing NHRP traffic
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK number'
CSCwh91136	Traffic not encrypted and droped over IPSEC SVTI tunnel
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error
CSCwi51326	CPP CP SVR crashes after decoding all packets to text (using l2 copy) on fia trace
CSCwi04547	SDWAN Custom Application is marked as invalid
CSCwi16111	IPv6 TCP adjust-mss does not work after delete and reconfigure
CSCwi63042	Packet drops observed between LISP EID over GRE tunnel
CSCwj01508	After upgrade, device continuously crashes and crash file is not generated

Resolved Bugs - Cisco IOS XE 17.9.4a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Bugs - Cisco IOS XE 17.9.4a

Identifier	Headline
CSCwd39257	IOS-XE cpp crashes when entering no ip nat create flow-entries
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is deleted

Identifier	Headline
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites
CSCwf34171	**Configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices
CSCwd17272	UTD packet drops due to fragmentation for ER-SPAN traffic
CSCwf41450	Device reloads changing the resource profile
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface
CSCwf52751	CLI template fails to attach to the device with the access-denied error message
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine
CSCwf11394	IOS XE - Vdaemon debug log should mention port-hop and reason prior to DISTLOC
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwf60120	Static NAT entry gets deleted from running config but remains in startup config
CSCwe51910	SNMPL ifindex persist does not work
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwd61988	Output packet bytes calculation bias when we enable QoS on port channel

Resolved Bugs - Cisco IOS XE 17.9.4

Identifier	Headline
CSCwf48808	FlexVPN: stale client routes stuck in RIB on FlexServer
CSCwe54089	ZTP process does not work
CSCwf02225	Device freezes during **show sdwan** commands
CSCwf47796	NHRP cache entries flood matching a /32 default route
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance
CSCwf08698	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail

Identifier	Headline
CSCwf09758	Watchdog crash while importing a large CRL file into the device
CSCwe41946	DTMF is failing through IOS MTP during call on-hold
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates
CSCwd49309	Ucode crash seen on device with traffic pointing to segfault in coff handler
CSCwe33793	Memory allocation failure with extended antireplay enabled
CSCwe66318	NAT entries expire on the standby router
CSCwe37002	C8000V is not taking 2 day 0 files configuration in OpenStack
CSCwa96399	Configuring the entity-information xpath filter causes syslogs to print, does not return data
CSCwe20008	SNMP MIB OID changing its last index
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair
CSCwe18058	Unexpected reload with IPS configured
CSCwd73783	Observed qfp-ucode-wlc crash
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured
CSCwe89404	No way audio when using secure hardware conference with secure endpoints
CSCwc89823	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info
CSCwe32862	Router IOS-XE crashes while executing AES crypto functions
CSCwf37888	Device Packet Duplication: Duplicate packets are counted on primary tunnel interface statistics
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console, te1 interface until router reloads
CSCwd49177	IPv6 prefix delegation is not reachable when packets are switched
CSCwe18124	Macsec remains marked as SECURED but the traffic stops working randomly
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP
CSCwd34941	NAT configuration with no-alias option is not preserved after reload

Identifier	Headline
CSCwd87195	NAT configuration with redundancy, mapping id, and match-in-vrf options with no-alias support
CSCwe70374	Platform punt-policer is not configurable
CSCwe37123	Router uses excessive memory when configuring ACLs with large object groups

Open Bugs - Cisco IOS XE 17.9.4

Identifier	Headline
CSCwd39257	IOS-XE cpp crashes when entering no ip nat create flow-entries
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is deleted
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites
CSCwf34171	**Configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices
CSCwd17272	UTD packet drops due to fragmentation for ER-SPAN traffic
CSCwf41450	Device reloads changing the resource profile
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface
CSCwf52751	CLI template fails to attach to the device with the access-denied error message
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine
CSCwf11394	IOS XE - Vdaemon debug log should mention port-hop and reason prior to DISTLOC
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwf60120	Static NAT entry gets deleted from running config but remains in startup config
CSCwe51910	SNMPL ifindex persist does not work
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwd61988	Output packet bytes calculation bias when we enable QoS on port channel
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs - Cisco IOS XE 17.9.3a

Bug ID	Headline
CSCwd45402	MSR Unicast-To-Multicast does not work if Dst and Src are the same in Service Reflect configuration
CSCwd90168	Unexpected reload after running 'show voice dsp' command while an ISDN call disconnects
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry is not in the ARP table
CSCwc27307	Service Engine YANG Support for ZBFW
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA
CSCwd81357	QoS Classification does not working for DSCP or ACL + MPLS EXP
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for the same client
CSCwc99823	fman crash seen in SGACL@ fman_sgacl_calloc
CSCwd25107	Interface VLAN1 is placed in "shutdown" state when configured with "ip address pool"
CSCwd61255	Data Plane Crash on the device when Making Per-Tunnel QoS configuration changes with scale
CSCwe01015	IKEv2/IPSec - phase 2 rekey fails when peer is behind NAT
CSCwd03869	CEF DPI Load-Balancing causes out of order packets
CSCwc65697	Device crashes and restarts during call flow with the new image
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
CSCwe03614	CWMP : MAC address of ATM interface is not included in Inform message
CSCwd38943	GETVPN: KS reject registration from a public IP
CSCwd06372	Unconditional excessive logging in eogre tunnel error handling case
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M)
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface
CSCwd06923	Stale IP alias left after NAT statement got removed
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply
CSCwc77981	C8000V crash - track the fman-fp's memory leak caused by cond-debug
CSCwd72312	GETVPN : Traffic drops seen on GM after rekey installing policies on 17.11.1 image
CSCwc14688	Single WAN Interface subslot 0/0 timing
CSCwd62953	C8000V: error platform provided UDI list has invalid values: ; udi_sn is empty
CSCwd07516	Memory leak under linux_iosd-imag related to SNMP

Open Bugs - Cisco IOS XE 17.9.3a

Bug ID	Headline
CSCwd39257	IOS-XE cpp crashes when entering 'no ip nat create flow-entries'
CSCwd63783	Memory leak on vdaemon process caused router reload
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe09805	OID for SNMP monitoring of DSP resources is not working as expected
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby
CSCwd17272	UTD Packet drops due to fragmentation for ER-SPAN traffic
CSCwd07580	Azure: C8000V QFP uCode crashes due to MLX4 driver
CSCwe32862	Router crashes while executing AES crypto functions
CSCwe33793	Memory allocation failure when extended antireplay is enabled
CSCwd68994	Unable to match on customer profile based on certificate-map
CSCwc06327	PFP policy in SRTE, RIB resolution in FC brings down ipsec tunnel interface- stuck at linestate down
CSCwe37002	C8000V does not allow multiple day0 configuration files in Openstack deployments
CSCwd97676	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
CSCwe38732	IP CEF load sharing command is being changed by the device
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs - Cisco IOS XE 17.9.2a

Bug ID	Headline
CSCwc94230	C8000V secondary disk not mounted in AWS
CSCwb52324	C8000V unexpected reload due to QFP ucode crash
CSCwc21739	Nat not requesting further for low ports after initial allocation when cli knob "reserved-ports" set
CSCwc39012	Crash saving tracelogs after "Too many open files" error
CSCwc03478	Vtcp does not support L2 correctly
CSCwc82140	QFP Crash When ZBFW configuration features "log dropped-packets" configuration
CSCwd12591	Ucode crash during FW classification, session frees
CSCwc99668	Routes added by ikev2 getting deleted at responder

Bug ID	Headline
CSCwc23077	Firewall drop seen stating Firewall L4
CSCwc78528	DSPware 60.1.1 Release targeting v179_throttle
CSCwc96444	Device is not programming the correct next-hop for unicast prefix with multicast config present
CSCwc49715	Carsh @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwmp configs
CSCwd06118	IKEv2 Cert-based IPSEC does not work between IOS-XE and AWS
CSCwc77183	Packet duplication is causing drops in payment transactions.
CSCwb89958	Unified Policy HSL not sending sccurate NBAR application information.
CSCwc52538	Flows are not distributed and load-balanced evenly and consistently on the device
CSCwc45950	ZBFW self zone policy drops ssh session on Mgmt-intf 512 ports
CSCwc43794	VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
CSCwc79145	Throughput degrades when Local TLOC specified in Data Policy goes down
CSCwc32595	BFD session remains down if interface flap form up/down/up
CSCwb65396	CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found)
CSCvz89354	Router crashes due to CPUHOG when walking ciscoFlashMIB
CSCwc39865	Subscriber session getting stuck and needs manual clearance
CSCwb48953	Device speed test fails with "Device Error: Speed test in progress" error
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication
CSCwd13352	SSH from device shell gets closed after update
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy
CSCwd56336	BFD sessions are not coming up after flapping the interface due to low ftm rate
CSCwd56015	UTD skipped when interface UTD config is used to enable/disable UTD

Open Bugs - Cisco IOS XE 17.9.2a

Bug ID	Headline
CSCwc99038	C8000V (Autonomous) stuck in Day-0 prompt with the customdata having invalid syntax
CSCwd44006	Control connection on the device doesn't come-up with reverse proxy using Enterprise Certificate
CSCwd33966	Unable to configure the local BGP as-path-list
CSCwd23810	IOS-XE: High CPU utilization caused by NHRP
CSCwd17579	Router crashing with reason CPU Usage due to Memory Pressure exceeds threshold (Reboot)
CSCwa14636	Device stopped forwarding traffic. Suspect OMPd is busy
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= ""
CSCvz55282	Serviceability enhancements for config migration failures between releases
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side
CSCwd13050	After an upgrade, the device moved into Out of Sync status
CSCwd12955	NAT translation is not correctly sent to the hub router from branch when SSNAT and UTD are configured
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same
CSCwd36621	CERM may kick in due to IPSec sessions initiated for on-demand tunnels
CSCwd44586	Login banner config is changed after upgrade
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy
CSCwc28468	Device always fails to push any template if it is running in the FIPS mode
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc
CSCwd29334	Upgrade failures due to inability to establish netconf connection from the device to upgrade-confirm
CSCwd45508	Device does not form BFD across Serial link when upgrading
CSCwa96399	Configuring "entity-information" xpath filter causes syslogs to print, does not return data
CSCwd34941	NAT configuration with the no-alias option is not preserved after reload
CSCwd12330	Invalid TCP checksum in SYN flag packets that pass through the router
CSCwd18131	Device not reachable after configuring platform resource service-plane-heavy
CSCwd18028	After deleting CSP, New CCM bringup on existing CSP is stuck in "Initializing CCM" on MT cluster

Resolved Bugs - Cisco IOS XE 17.9.1a

Bug ID	Headline
CSCvz65764	Peer MSS shows incorrect value
CSCwa95092	When Object-group used in an ACL is updated, it takes no effect
CSCwb39822	MLX5 Driver error on a C8000V in Microsoft Azure causes excessive debug printing
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions
CSCwb49857	Memory leaks on keyman process when key is not found
CSCwa65728	Large number of DH failures
CSCwb11389	NAT translation stops suddenly (ip nat inside doesn't work)
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA
CSCwb39098	Router crashed after new IPv6 address assigned when router used specific configuration
CSCwa69101	Initiator unclassified ip-address LQipv4 command has no effect
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop
CSCwb27486	New Key for NBAR app and NBAR category without OGREF optimized
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post upgrade
CSCwa49101	OMP origin protocol comparison cleanup
CSCwb17282	Router crashes when clearing a VPDN session
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route
CSCwa98617	Memory leak in AEM chunks related to firewall
CSCwb18223	SNMP v2 community name encryption problem
CSCwb31587	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests
CSCwb51238	Router unexpectedly reloads two times when netflow show commandis executed
CSCwb12647	Router crashes for stuck threads in cpp on packet processing
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCwa78348	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager
CSCvz81664	Enabling or Disabling OMP Overlay AS Prevents Connected Routes from Being Advertised in OMP
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwb15331	Keyman memory leak using public keys

Bug ID	Headline
CSCwb34625	C8000V auto mode: static ip from bootstrap config overwritten by dhcp on fresh install
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address.
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
CSCwb51595	Missing IOS config (voice translation rule) on upgrade
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
CSCwb13850	License boot level not detected with Day0 after C8000V boots on NFVIS platforms

Open Bugs - Cisco IOS XE 17.9.1a

Bug ID	Headline
CSCvz65764	Peer MSS shows incorrect value
CSCwb11389	NAT translation stops suddenly(IP nat inside doesn't work)
CSCwa84919	"Revocation-check crl none" does not failover
CSCwb42807	After Enforce Software Version (ZTP) completes successfully, it automatically rolls back
CSCwb04815	NHRP process takes more CPU when IP nhrp redirect is configured
CSCwa72273	ZBFW drops return packets post device upgrade
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb18223	SNMP v2 community name encryption problem
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored
CSCwb12647	Device crashes for stuck threads in cpp on packet processing
CSCwb24123	Registration of spoke fails with dissimilar capabilities
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwb45422	Crash due to IPv4 reassembly
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address
CSCwb29362	Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection
CSCwa68540	FTP data traffic broken when UTD IPS is enabled in both the service VPN
CSCwb27900	WebSocket forking connection failed for Voice VRF scenario
CSCwa48122	SIP OAuth http request to fetch keys from CUCM fails after bootup as interface is down
CSCwc65697	Router crashes with CUBE WebSocket forking flows

Related Documentation

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

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.