Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-08-16

Last Modified: 2024-04-04

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 Bengaluru 17.4.1a release:

- c8000v-universalk9.17.04.01a.ova
- c8000v-universalk9.17.04.01a.iso
- c8000v-universalk9.17.04.01a.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.
17.04.01a	Indicates that the software image is mapped to the Cisco IOS XE Bengaluru 17.4.1a 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 in Cisco IOS XE Bengaluru 17.6.x

New and Changed Software Features in Cisco IOS XE 17.6.7

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.6a

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 17.6.6

There are no new software features in this release.

Note See the End-of-Sale and End-of-Life Announcement for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map Feature in IOS XE page for information about the end-of-life milestones for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map feature.

New and Changed Software Features in Cisco IOS XE 17.6.5a

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 17.6.5

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.3a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.2

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.1a

Note Cisco IOS XE Bengaluru 17.6.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE Bengaluru 17.6.1 release series.

The following are the new Cisco Catalyst 8000V software features for Cisco IOS XE Bengaluru Release 17.6.1a:

Table 2: Software Features in 17.6.1a

Feature	Description
AWS Metadata Version 2	Earlier, when you deployed Cisco Catalyst 8000V on Amazon Web Services, only version 1 or V1 was applicable for the **Metadata Accessible** field. Starting from Cisco IOS XE Release 17.6.1a, metadata version 2 or V2 is also supported. Now, you can either select the V1 and V2 (token optional) option or the V2 (token required) option. When you select either of these options, the instance uses session-oriented requests by creating tokens. The tokens are then used to fetch all the required metadata for your instances.

Feature	Description
Automatic Mapping of Cisco CSR 1000V or Cisco ISRv Licenses to DNA Tier Licenses	The Cisco Smart Software Manager (CSSM) manages licenses of all the Cisco devices including Cisco CSR 1000V and Cisco ISRv, which have an end-of-life milestone of year 2022. To continue to keep your Smart Account active, it is mandatory to move to Cisco DNA tier-based licenses. After you activate your Cisco DNA license, CSSM automatically maps the device licenses (CSR 1000V or Cisco ISRv) to your Cisco DNA tier license.
Support for ESXi 7.0	Cisco Catalyst 8000V supports ESXi 7.0 and 6.7 from Cisco IOS XE 17.6.1a. Note that support for ESXi 6.5 has been deprecated.
Zone-Based Firewall Policy Reclassification	The Zone-Based Firewall (ZBFW) Policy Reclassification feature is an enhancement to the Zone-Based Firewall feature. With this enhancement, any changes you make to the policy configuration on an existing firewall session is immediately enforced.
Asymmetric Lease for DHCPv6 Relay Prefix Delegation	This feature allows you to manage or change the lease renewal. It provides options to force renewal of lease and also detects when the lease is nearing the expiry date.
Upgrade to pyang version 2.x	The updated pyang plugin version 2.x fixes existing issues such as XPATH validation and upstream pyang issues. Additionally, this version reports all errors in the YANG models to the users and enforces a strict model validation.
WebSocket Based Forking for Cloud Speech Services in CUBE	From Cisco IOS XE Bengaluru 17.6.1, CUBE can use WebSockets to handle media forking in a Cisco Unified Contact Center Enterprise (UCCE) solution deployment with Cloud Speech Services. WebSockets transport multiple media streams over a single reliable TLS connection that may traverse firewalls without the need for special policies. WebSocket traffic is also compatible with HTTP load balancers and proxies.
Support for OPUS Codec Transcoding in CUBE	From Cisco IOS XE 17.6.1 onwards, CUBE can transcode Opus encoded media streams. Because Opus codecs perform very well over the Internet, this feature is particularly beneficial when routing calls between the PSTN and Cloud calling services. See also https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_transcoding.html.

Feature	Description
Class of Restriction YANG Configuration Model updates:	YANG models were developed for the following CLIs as part of the Class of Restriction configuration: • dial-peer voice <tag> pots/voip corlist • dial-peer voice vad • dial-peer cor custom name <string> • dial-peer cor list <string> member <string> • voice num-exp <string1> <string2> • voice register pool <string> [no] cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}

Table 3: Software Features in 17.6.2

Feature	Description
Snapshots for PAK Licenses	The library that manages product activation key (PAK) licenses is being deprecated from the software image. To continue supporting and honouring any existing PAK licenses you may have, the system automatically takes a snapshot of the PAK license and triggers a Device-Led Conversion process, to convert the PAK license to a Smart License. For the system to take the snapshot, the software version running on your device must be one of the required releases. For information about the releases in which the system can take a snapshot, and the options that are available with respect to the device and the license, see Snapshots for PAK Licenses.

Note From Cisco IOS XE Bengaluru 17.6.x, configuring a weak crypto algorithm generates a warning. But this warning can be safely ignored and does not impact the working of the crypto algorithms. For more information on weak crypto algorithms, see Supported Standards.

Resolved and Open Bugs for Cisco IOS XE Bengaluru 17.6.x

Resolved Bugs - Cisco IOS XE 17.6.7

Identifier	Headline
CSCwh73350	Device keeps crashing when processing a firewall feature

Identifier	Headline
CSCwh99399	FTMD crash observed in ENCS platform while running PWK suite
CSCvo01546	NHRP reply processing may dequeue an unrelated request
CSCwh49644	CSDL Compliance failure: Use of 3DES by IPSec is denied
CSCwi01046	PoE module does not provide enough power to bring the ports after an unexpected reload
CSCwh01425	ITU channel configuration does not work
CSCwh20577	Crashed by TRACK client thread at access; invalid memory location
CSCwh70449	PMTUD incorrectly converges without attempting to learn a higher MTU
CSCwf34171	The **configure replace** command fails due to the `license udi PID XXX SN:XXXX` line on IOS-XE devices
CSCwh36801	Crash in IP input process during tunnel encapsulation

Open Bugs - Cisco IOS XE 17.6.7

There are no open bugs in this release.

Resolved Bugs in Cisco IOS XE 17.6.6a

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 17.6.6a

Identifier	Headline
CSCwe92277	Performance degradation on C8000V hosted in Azure cloud when the traffic flow is asymmetrical
CSCvz96485	Azure: C8000V NETVSC PMD DPDK Support
CSCwe37016	The output rate on the port channel does not match the total physical interface output rate
CSCwh14083	High CPU due to MPLS MIB poll
CSCwd16559	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table

Identifier	Headline
CSCwf99647	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call
CSCwh21376	Unable to disable the call-home feature on devices
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more
CSCwf80400	IOS XE Router may experience unexpected reset while executing the **show utd engine standard statistics** command
CSCwd46688	Unable to apply the Service Policy on tunnel interfaces
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwe29301	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping
CSCwe90119	Device-tracking database entry stuck on UNKNOWN state with temporal mac address.
CSCwh15021	QFP crash when configuring S2S VPN (IKEv2/IPSEC) with Azure vWAN/HUB
CSCwf55145	SFP transceiver DOM does not work after some time; however interface forwards the traffic as expected
CSCvu85539	Unable to delete wrong interface name in C8000V
CSCwd97212	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt Service Process
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwc67429	CTS PI changes for adding new binding source priority for LISP sourced local host bindings
CSCwh45169	Unexpected reboot while dispalying information from a cleared SSS session
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied
CSCwb89958	Unified Policy HSL does not send NBAR application information
CSCvz68895	Device crashes after adding trustpoint
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces
CSCwf95535	Intf/System xml files are not generated
CSCwf99947	Crash when modifying tunnel after running the **show crypto** commands
CSCvy94747	GRACEFUL-RELOAD: Wrong state: 1 to recieve chasfs event:

Identifier	Headline
CSCwf34171	The **configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices
CSCwf74668	HSEC licenses incrementing
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
CSCwf80191	Flowspec on device won't revoke
CSCwf41084	Extranet Multicast code improvements for better handling of data structure
CSCwc87565	Unexpected reload due to a watchdog on the kernel
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwd94495	SSM On-Prem responds with message completed to poll_id requests without ACK data
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwh01738	Unexpected reload when using rsh/rcmd
CSCwf59929	CTS CORE process crash after configuring role based ACL
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location
CSCwe21703	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured
CSCvz20285	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode

Resolved Bugs - Cisco IOS XE 17.6.6

Identifier	Headline
CSCwf70596	Fix VLAN replay for SRIOV i40e interface after link flap
CSCwe09745	Memory leak in Pubd when continuously trying to connect to remote peer
CSCwd63063	Standby BGP session receives incorrect routes from Active
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured

Identifier	Headline
CSCwd90168	Unexpected reload after running the **show voice dsp** command while an ISDN call disconnects
CSCwe60059	Crash when using dial-peer groups with STCAPP
CSCwe36122	ISIS crash when performing TI-LFA calculation
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification
CSCwf00769	L2RIB thread crash after removing EVPN member from bridge domain
CSCwf83301	Device displays incorrect values for Call Quality statistics(RTT/MOS)
CSCwe72462	Username/Password under voice register pool gets deleted post CME reload
CSCwe25006	An unexpected removal of the underlay S,G entry resulting ~20s disruption in the multicast flow SDA
CSCwe21042	NBAR DP traceback - "Failed to process non-graph batch message: wrong batch id" is logged
CSCwf47796	NHRP cache entries flood matching a /32 default route
CSCwe32862	Router IOS-XE crashes while executing AES crypto functions
CSCwf09758	Watchdog crashes while importing a large CRL file into the device
CSCwf67564	Memory Leak at process SSS Manager
CSCvy87339	Telemetry subscription fails to connect to grpc receiver when multiple XPATH changes are made to it
CSCwe41946	DTMF is failing through IOS MTP during call on-hold
CSCvq81894	Check nexthop reachability before installing route for a prefix
CSCwe52796	Intermittent one way audio issue after hold and resume SRTP to RTP
CSCvz12193	SNMPwalk: Authentication failure with MD5 SNMPv3 user
CSCwd09685	Memory leak found via the MLD tool
CSCwe64213	LSPVif removal on OIF for RP discovery group 224.0.1.40 with timing related trigger
CSCwf47563	Device crashes after importing the trustpoint with rsakeypair
CSCwe12194	Auto-Update cycle incorrectly deletes certificates
CSCwe33793	Memory allocation failure with extended antireplay enabled
CSCwd59423	Unexpected reload on device caused by WNCd process after removing a VLAN from a VLAN-GROUP
CSCwc03176	Device crashes when applying a service-policy to a newly created tunnel

Identifier	Headline
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data
CSCwh04884	VC Down due to control-word negotiation
CSCwc24044	IOS XE device may experience an unexpected reset with high volume of multicast
CSCwb47153	Keyman process crash
CSCwc99453	Enable the **license feature hseck9** command
CSCwe18124	Macsec remains marked as SECURED, but randomly the traffic stops working
CSCwb59052	Observe traceback message when BVM client do Inter-xTR roaming
CSCwd73783	Observed qfp-ucode-wlc crash
CSCwf14135	SIPREC recording fails in transfer scenario when certian options are enabled during configuration
CSCwf56463	IOS process crashes during VRRP hash table lookup
CSCwf44649	LISP failed to recreate the more specific away table entries after less specific entries toggled
CSCwe23150	CUBE memory leak sdp_copy_all_attrs sdp_parse_attribute sdp_add_new_attr
CSCwf48808	FlexVPN: Stale Client Routes stuck in RIB on FlexServer
CSCwf39490	MCID (Malicious Call Identification) breaks due to custom prefix setting under STCAPP FAC
CSCwd99921	The IOS XE software crashes while validating certification trust
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M)
CSCwc56033	No alarms are triggered when RPM of a fan is 0
CSCwe36743	Segmentation Fault - Crash - SSH - When Changing AAA Group Configs
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop
CSCwf41082	MallocLite Memory Leak observed in HTTP CORE Allocator
CSCwh11858	Switch running IOS-XE crashes when removing FQDN ACL
CSCwc89823	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info
CSCwf29859	Logging in get-config processing affecting the template push fail
CSCwd28734	Device memory leak in pubd causes switch reload

Identifier	Headline
CSCwf27815	DSP resource can not be released after call ends
CSCuq20562	ISDN memory leak when PRI link flaps, crashes router
CSCwf01986	Radius attribute 31 not being sent on device for CTS Pac provisioning
CSCwf03292	I/O middle pool leaking when VOIP trace is enabled
CSCwe66318	NAT entries expire on Standby Router
CSCwh05407	Gateway disconnecting incoming calls when FPI Correlator is not released after disconnect on PRI Leg
CSCwe39011	GARP on port up/up status from router is not received by remote peer device
CSCwf14589	IOS-XE device may experience a segmentation fault with L2VPN EVPN when clearing duplicate MAC
CSCwe70237	CUBE reloads due to a segmentation fault in CCSIP_SPI_CONTROL process
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router
CSCwf24164	Netflow stops working when flow monitor reaches cache limit
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched
CSCwf08698	Device Crashes Unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'

Open Bugs - Cisco IOS XE 17.6.6

Identifier	Headline
CSCwe92277	Performance degradation on C8000V hosted in Azure cloud when the traffic flow is asymmetrical
CSCvz96485	Azure: C8000V NETVSC PMD DPDK Support
CSCwe37016	The output rate on the port channel does not match the total physical interface output rate
CSCwh14083	High CPU due to MPLS MIB poll
CSCwd16559	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table
CSCwf99647	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call
CSCwh21376	Unable to disable the call-home feature on devices
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more

Identifier	Headline
CSCwf80400	IOS XE Router may experience unexpected reset while executing the **show utd engine standard statistics** command
CSCwd46688	Unable to apply the Service Policy on tunnel interfaces
CSCwf55243	Device is crashing while adding a trustpoint to the router
CSCwe29301	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping
CSCwe90119	Device-tracking database entry stuck on UNKNOWN state with temporal mac address.
CSCwh15021	QFP crash when configuring S2S VPN (IKEv2/IPSEC) with Azure vWAN/HUB
CSCwf55145	SFP transceiver DOM does not work after some time; however interface forwards the traffic as expected
CSCvu85539	Unable to delete wrong interface name in C8000V
CSCwd97212	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt Service Process
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwc67429	CTS PI changes for adding new binding source priority for LISP sourced local host bindings
CSCwh45169	Unexpected reboot while dispalying information from a cleared SSS session
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied
CSCwb89958	Unified Policy HSL does not send NBAR application information
CSCvz68895	Device crashes after adding trustpoint
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces
CSCwf95535	Intf/System xml files are not generated
CSCwf99947	Crash when modifying tunnel after running the **show crypto** commands
CSCvy94747	GRACEFUL-RELOAD: Wrong state: 1 to recieve chasfs event:
CSCwf34171	The **configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices
CSCwf74668	HSEC licenses incrementing
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value

Identifier	Headline
CSCwf80191	Flowspec on device won't revoke
CSCwf41084	Extranet Multicast code improvements for better handling of data structure
CSCwc87565	Unexpected reload due to a watchdog on the kernel
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwd94495	SSM On-Prem responds with message completed to poll_id requests without ACK data
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwh01738	Unexpected reload when using rsh/rcmd
CSCwf59929	CTS CORE process crash after configuring role based ACL
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location
CSCwe21703	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured
CSCvz20285	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode

Resolved Bugs in Cisco IOS XE 17.6.5a

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 17.6.5a

Bug ID	Headline
CSCwd79089	Device controller crash when sending full line rate of traffic with >5 Intel AX210 stations
CSCwd90168	Unexpected reload after running 'show voice dsp' command while an ISDN call disconnects
CSCvq81894	Check nexthop reachability before installing route for a prefix

Bug ID	Headline
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwb89958	Unified Policy HSL does not send NBAR application information properly
CSCwd07580	Azure: C8000V QFP uCode crash due to MLX4 driver
CSCwd92344	C8000V crash observed in Azure due to Segmentation Fault with MLX5 drivers
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwd71458	Outgoing number of bytes decrease in router' interface
CSCwd97676	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched
CSCwe19617	Bash core observed on C8000V in the idle state.

Resolved Bugs - Cisco IOS XE 17.6.5

Bug ID	Headline
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply
CSCvz93612	%HW_FLOWDB-3-HW_FLOWDB_DBLDEL_FEATOBJ: FlowDB featobj cannot be deleted twice
CSCvy60839	CSDL Compliance: Added a new command to disable weak crypto checking in future releases.
CSCwc82140	QFP Crash When ZBFW configuration features "log dropped-packets" configuration
CSCwc99823	fman crash seen in SGACL@ fman_sgacl_calloc
CSCwc78021	Standby WLC crash @ fman_acl_remove_default_ace
CSCvz92994	Lack of MAC address in the Inform Event message.
CSCwc89328	Device might reboot when supporting explicit IV joins the SD-WAN network
CSCwb52324	C8000V unexpectedly reloads due to QFP ucode crash
CSCwd71584	DSPware 58.5.2 release targeting v176_throttle
CSCwd61255	Data Plane Crash on the device when Making QOS configuration changes
CSCwb04815	NHRP process takes more CPU because of FlexVPN event trace
CSCwc22314	RTSP Traffic not being rewritten by NAT
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor
CSCwd56131	LTE modem doesn't show GSM bands
CSCwb73395	Need CLI option to disable ALG
CSCwc54463	Device LAN module is down when high CPU noticed
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt

Bug ID	Headline
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event
CSCwb08057	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
CSCwc77981	C8000V crashed - track the fman-fp's memory leak caused by cond-debug
CSCwb32635	Device vdaemon file is incomplete when running admin-tech
CSCwd72312	GETVPN : Traffic drops seen on GM after rekey installing policies

Open Bugs - Cisco IOS XE 17.6.5

Bug ID	Headline
CSCwd79089	Device controller crash when sending full line rate of traffic with >5 Intel AX210 stations
CSCwd90168	Unexpected reload after running 'show voice dsp' command while an ISDN call disconnects
CSCvq81894	Check nexthop reachability before installing route for a prefix
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwb89958	Unified Policy HSL does not send NBAR application information properly
CSCwd07580	Azure: C8000V QFP uCode crash due to MLX4 driver
CSCwd92344	C8000V crash observed in Azure due to Segmentation Fault with MLX5 drivers
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwd71458	Outgoing number of bytes decrease in router' interface
CSCwd97676	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched
CSCwe19617	Bash core observed on C8000V in the idle state.

Resolved Bugs - Cisco IOS XE 17.6.4

Bug ID	Headline
CSCwb95559	Packet Sanity failed for Resolution Reply on Spoke due to missing SMEF capability
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA
CSCvz63684	EWC HA pair experiencing IOS tracebacks followed by KEYMAN Crash
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions

Bug ID	Headline
CSCwc33311	cEdge crash @ imgr_n2_ipsec_sa_ctx_register
CSCwa33174	Azure C8000V: 'show interfaces' counters are incorrect and display extremely large values
CSCwc06967	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3
CSCwc37320	RP Switchover Causes Linecard NFS mount Failure Resulting in Memory Leak
CSCwb05743	Crash seen with umbrella config during soak run
CSCvz83016	BFD tunnel uptime does not show correct values post upgrade
CSCwb43605	OMPd crash during RIB-out attribute aspath/community processing
CSCwc13013	IPSec Key Engine process holding memory continuously and not freeing up
CSCwb34625	C8000V auto mode: static ip from bootstrap config overwritten by dhcp on fresh install
CSCwb73511	Device is not able to bring up SIG tunnels after reboot
CSCwb91729	Fix mishandling of policy sequence programming failures and notify with syslog/notification
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async
CSCwc39881	C8000V generated from hardware cEdge contains "/" in Common Name
CSCvz23982	IOS sending UP Event for the sub interface which is in down state
CSCvx93283	Service Chain is not created when Tracking is disabled
CSCvz99832	Per class BFD - echo response pkts
CSCwb08636	IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error seen for TLOCExt setup after upgrade
CSCvx74917	DNS packets are not redirected to configured custom DNS after Umbrella template edit
CSCwa72273	ZBFW dropping return packets from tunnel post upgrade
CSCwb32934	Device does not use QAT when malloc failure
CSCwa08378	C8000V Day0 ZTP ignores crypto configuration before licensing
CSCwa64955	Device loses control connections after installing new enterprise hardware wan edge cert
CSCwa92137	Device is changing ICMP ID in ICMP echo, replies intermittently
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwb49857	Memory leaks on keyman process when key is not found
CSCwb76866	CSDL failure: Use of MD5 by IPSEC key engine is denied
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored
CSCwa80826	IOS-XE: Devices running crypto ipsec policy experience installation failure
CSCwb83376	Device endpoint-tracker cannot be configured on a 100G interface
CSCwc13304	Per-tunnel QoS counters and shapers not working for some bfd tunnel with stale 'nh_overlay' objects

Bug ID	Headline
CSCwa67398	NAT translations do not work for FTP traffic in device
CSCwb78173	CSDL failure: IPSec QM Use of DES by encrypt proc is denied
CSCwb76170	IPsec SIG auto tunnels are not coming up
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp
CSCvy54048	CPP Unexpected reboot occurs while freeing CVLA chunk
CSCwa30857	Internet SpeedTest with loopback binding mode doesn't work with implicit ACL drop for return traffic
CSCwb14020	Serial interface stuck in "line protocol is down" state after it went down and is recovered
CSCwa98545	Checks of route leaks creates memory corruption
CSCwb46649	NAT translation does not show (or use) correct timeout value for an established TCP session
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwb58468	Sig Autotunnels:tunnel 409 response received
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed
CSCwb12647	Device crash for stuck threads in cpp on packet processing
CSCwc04688	Device crash observed after enabling NWPI trace with IPv6 traffic
CSCwb76988	IKEv2 fragmentation causes wrong message ID to be used for EAP authentication
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
CSCvz37340	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
CSCwb99793	CRL verification failure results in 400 Bad Request with DigiCert
CSCwb90470	Device crashed with last reload reason 'Critical process cxpd fault'
CSCwb32059	Cellular interface tracker down but NAT route persists in the Service VPN Routing Table
CSCwb51595	Missing IOS config (voice translation rule) on upgrade
CSCwb40575	After upgrade, umbrella dns config set to NONE in show umbrella config
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
CSCwc04289	Inconsistency between Path MTU Discovery result and Tunnel MTU

Open Bugs - Cisco IOS XE 17.6.4

Bug ID	Headline
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication

Bug ID	Headline
CSCwc23077	Firewall drop seen stating FirewallL4
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwc50477	Device crashed in ipv4_nat_create_out2in_session_entry
CSCwc55260	Memory leak due to FTMd process
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwb89958	Unified Policy HSL not sending proper NBAR application information.
CSCwc59598	Statistics collection causes service-side BFD to flap on every collection interval
CSCwc22314	RTSP Traffic not being rewritten by NAT
CSCwb83236	Traceback: QFP core after pushing data policy with IPv6 interface
CSCwc67465	Router cannot be upgraded
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms
CSCwc43973	DLC is not completing after upgrading to Smart licensing from CSL
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert
CSCwc27208	BFD sessions not coming up because of ANTI-REPLAY-FAILURES
CSCwc25291	NIM-LTE-EA No Data - Requires subslot reload to recover
CSCwd36511	Ping fail to VRRP virtual IP address.

Resolved Bugs - Cisco IOS XE 17.6.3a

Bug ID	Headline
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
CSCwa13553	C8000V QFP core due to NAT scaling issue
CSCvx40516	17.5 ZBFW + NAT: Traffic flow In2Out scenario failed
CSCwa26509	Shut/no shut of endpoint-tracker attached tunnel, doesn't create probe again on 17.6.2
CSCvz98373	ZBFW : FirewallPolicy drops seen with RTSP traffic in steady state
CSCvz71436	Call Placing issue from SCCP phones
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
CSCvz86591	VRF-aware static NAT with route-map and reversible not working
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel
CSCwa36699	Prefetch CRL Download Fails
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address
CSCwa76260	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - Cicso PSB Security Compliance

Bug ID	Headline
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
CSCvz41647	Partial multicast drops are seen after a failover event in a site with two cedges
CSCvz76277	Hostname not allowed beginning with numbers
CSCvz34668	Static mapping for the hub lost on one of the spokes
CSCvz84437	Unexpected reload due IPV6 UDP fragment header in VxLAN
CSCwa15085	Router Crash due to Stuck Thread with appnav-xe dual controller mode.
CSCvx28426	Router may crash due to Crypto IKMP process
CSCwa18177	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed
CSCvy97741	Multiple qfp-ucode crash when making a blind transfer from an outside SIP service

Open Bugs - Cisco IOS XE 17.6.3a

Bug ID	Headline
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCvz05814	Cwand issue observed ..potential crash
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to Ipv4 Unclassified
CSCwb32934	QAT is not used during malloc failure
CSCwa08378	C8000V Day0 ZTP ignores crypto configuration before licensing
CSCwb13820	C8Kv crashed at high scale with IPSEC and heavy features configured
CSCwb08186	E1 R2 - dnis-digits cli not working
CSCwb26741	ZBFW performance variance observed with 17.6 images on 8v CPU due to rx_miss errors
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwa68471	Traceback: CPP ucode core generated after HSRP priority change
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCwb18223	SNMP v2 community name encryption problem
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk
CSCwa98545	Checks of route leaks creates memory corruption.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop

Bug ID	Headline
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwa29964	SCEP fails if AAAA DNS repy is received and source interface has no IPv6 address
CSCvz55275	Show DMVPN command displays incorrect state
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection
CSCvz74322	"Shutdown" command visible in running config after reload of instance

Resolved Bugs - Cisco IOS XE 17.6.2

Caveat ID Number	Description
CSCvz08449	Cat8kv - Incorrect static route for primary interface during deployment resulting in unreachability

Open Bugs - Cisco IOS XE 17.6.2

There are no open bugs for this release.

Resolved Bugs - Cisco IOS XE 17.6.1a

Caveat ID Number	Description
CSCvw83359	AWS:C8000V crashed and reboots if shut/no shut an interface a number of times.
CSCvy52270	CSR1000V/C8000V: Console Port Access change CLI does not work in the CONTROLLER mode.
CSCvx86151	ovf-template should give option for DNA essentials, advantage, premier on C8kv deployment in vcenter
CSCvv35440	C8000v WebUI is not accessible by user.

Open Bugs - Cisco IOS XE 17.6.1a

Caveat ID Number	Description
CSCvx94285	C8000V crashes after oce_lookup_one_adj_id_handle while reading emu_mem.
CSCvz22268	With crl schedule download, stuck Failed to send the request. There is another request in progress.

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.