Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Release 17.15.x

First Published: 2024-08-27

Last Modified: 2026-08-05

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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, and Cisco 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 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 opt 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 licenses that are available via Cisco DNA:

- 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 17.15.1a release:

- c8000v-universalk9.17.15.01a.ova

- c8000v-universalk9.17.15.01a.iso
- c8000v-universalk9.17.15.01a.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. Images with the universalk9 designation in the image name refers to a universal image that offers all the Cisco IOS features including strong payload cryptography features such as IPSec VPN, SSL VPN, and Secure Unified Communications. This image also supports security features like Zone-Based Firewall and intrusion prevention.
17.15.01a	Indicates that the software image is mapped to the Cisco IOS XE 17.15.1a 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 17.15.x

New and Changed Software Features in Cisco IOS XE 17.15.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.5

Table 2: Software Features

Feature	Description
Support for Nutanix AHV Hypervisor	Cisco IOS XE 17.15.5 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. This deployment 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 or .qcow2 image for these deployments using Nutanix Prism Central dashboard, Nutanix Prism Element dashboard, Nutanix AOS REST APIs or Nutanix AOS CLIs. For more information, see Nutanix support.
Support for Microsoft HyperV on Azure Local certified servers	Cisco IOS XE 17.15.5 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. For more information, see Azure Local.
Support for RHEL 9.6 hypervisor for KVM hosts	Cisco IOS XE 17.15.5 supports the deployment of Cisco Catalyst 8000V on Red Hat RHEL 9.6 operating system with KVM hypervisor.
Support for Nvidia Mellanox ConnectX-7 network interface cards	Cisco IOS XE 17.15.5 supports SR-IOV connectivity for Nvidia Mellanox ConnectX-7 Network Interface Cards (NICs) that deliver higher throughput and performance for the supported hypervisors.

New and Changed Software Features in Cisco IOS XE 17.15.4c

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.4

There are no new software features in this release.

New and Enhanced Software Features in Cisco IOS XE 17.15.3a

Table 3: Software Features

Feature	Description
Support for DSv5 instances for Microsoft Azure deployments	Cisco IOS XE 17.15.3a supports DSv5 instances for Cisco Catalyst 8000V deployments in Microsoft Azure.
Support for N2 instances for Google Cloud Platform deployments	Cisco IOS XE 17.15.3a supports n2-standard-8, n2-standard-4 instance types for Cisco Catalyst 8000V deployments in Google Cloud Platform.

New and Changed Software Features in Cisco IOS XE 17.15.2a

There are no new features in this release.

New and Enhanced Software Features in Cisco IOS XE 17.15.1

Note Cisco IOS XE 17.15.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE 17.15.x release series.

Table 4: Software Features

Feature	Description
Support for AWS Local Zones	AWS Local Zones (LZs) enable you to deploy latency sensitive applications closer to end-users. Starting with Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on c5d.2xlarge instances available in AWS Local Zones.
Support for Interface speed setting of 40000	From Cisco IOS XE 17.15.1a, you can set an interface speed of upto 40000 in Cisco Catalyst 8000V. This enables some traffic profiles to see higher throughputs.
Support for RHEL 9.2 hypervisor for KVM hosts	From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on RedHat RHEL 9.2 operating system with KVM hypervisor. Note that support for RHEL 7.x is deprecated from this release.
Support for SUSE Linux® Enterprise Server 15 SP5	From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on SUSE Linux® Enterprise Server 15 SP5 operating system with KVM hypervisor.

Feature	Description
Support for VMware ESXi 8.0	From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on VMware ESXi 8.0 Update 2 hypervisor operating system. Note that ESXi hypervisor version 6.0 will no longer be supported from this release.
Absolute Path for HTTP or HTTPS File Transfer	The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the **copy** command. From Cisco IOS XE 17.15.1a, you must provide the absolute file path when you execute the **copy** command, to transfer the file.
Cisco Umbrella Scope Credentials	From Cisco IOS XE 17.15.1a, this feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.
Configure DMVPN for SD-Routing Devices	Cisco DMVPN (Dynamic Multipoint VPN) is a routing technique to build a VPN network with multiple sites without having to statically configure all devices. This technique uses tunnelling protocols and encrypted security measures to create virtual connections, or tunnels, between sites. These tunnels are dynamically created as needed, making them both efficient and cost-effective.
Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF	You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic.
Configure Site-Cloud Support to AWS Using Configuration Groups	This release introduces support to configure site to cloud connectivity from an SD-Routing branch to Amazon Web Services using Configuration Groups. This is an enhancement over the existing implementation of configuring site to cloud connectivity from an SD-Routing branch to Amazon Web Services using CLI-Add on Profile.
Enabling Flow Level Flexible NetFlow Support for SD-Routing Devices	The Flow-level Flexible NetFlow (FNF) feature allows you to monitor the NetFlow traffic and view all the flow-level FNF data that is captured including application-level statistics.

Feature	Description
Enhanced NAT Management	From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the ip nat translation max-entries cpu command. This feature also enables streamlining NAT synchronization in redundant systems using the **ip nat settings redundancy optimized-data-sync** command.
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.15.1a, Segment Routing over IPv6 dataplane supports these functionalities: • IS-IS Microloop Avoidance • IS-IS Loop-Free Alternate Fast Reroute • IS-IS Topology-Independent Loop-Free Alternate Fast Reroute • OAM Traffic Engineering
Monitoring Software Defined (SD) - Routing Alarms	From Cisco IOS XE 17.15.1a, network administrators can monitor SD-Routing device alarms on Cisco Catalyst SD-WAN Manager. This feature enables SD-Routing devices to record and store various alarms generated by control components and routers. For more information, see Cisco SD-Routing Command Reference Guide.
Network-Wide Path Insights on Software Defined (SD) - Routing Devices	Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network.
SD-Routing License Management	This release introduces license management support for SD-Routing devices. The supported licensing workflows include license assignment or configuration, license use, and license usage reporting. Depending on the device, these workflows are performed in the Cisco Catalyst SD-WAN Manager or on the device.
Classic CLI	This feature provides support for including Cisco IOS XE CLI configuration commands that do not have an associated yang model. When used with the current configuration group, Classic CLI provides a robust provisioning mechanism for SD-Routing devices from Cisco SD-WAN Manager.

Resolved and Open Bugs - Cisco IOS XE 17.15.x

Resolved Bugs in Cisco IOS XE 17.15.6

Identifier	Headline
CSCws96978	Policy download fails after modifying SGACL on ISE and pushing using COA.
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.
CSCwt09078	Enhanced logging for file system read failure.
CSCwq54131	Device crash when configuration replace is performed using VTY session.
CSCwo90776	Messages in MQIPC buffer queue may not get drained during connrent and eagain conditions in race condition.
CSCws68876	Unexpected reload due to ISSU client ISSU Virtual-Template Client.
CSCwu04279	System instability and potential service disruption after invalid GPM load.
CSCwr77437	Seg Fault in HTTP CORE potentially due to SDAVC-related Corruption.
CSCwt35490	Config-Sync: Log the errno value for all file open operation failure.
CSCwq82256	Already committed SMU packages are removed from R0 on SMU activation failure later.
CSCwt00254	Anonymous memory leak due to missing SSL async FD deselect in WebAuth.
CSCwt86654	IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing.
CSCwt29087	After performing forced switchover and pushing COA for SGACL change, old SGACL is seen on switch.
CSCws66419	Unexpected Reload due to block overflow in RSA verification.
CSCwt69624	TCP application (LISP/BGP) can stuck in write blocked state forever.
CSCwt00262	OPSSL changes for SSL async job memory leak.
CSCwt87294	mDNS Cache-Flush behavior not consistent.
CSCwo26985	Wireless client authentication fails due to RADIUS client unable to parse Microsoft MPPE-Send-Key VSA; In another scenario, certificate reassembly may fail for retransmissions.

Open Bugs - Cisco IOS XE 17.15.6

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

Resolved Bugs - Cisco IOS XE 17.15.5

Identifier	Headline
CSCwr55240	C8000v experiences critical failure with OMPd process
CSCwr31999	Using Azure Portal GUI stop button initiates reload before forcefully shutting down in 10 minutes
CSCwp06956	NGFW Policy deployment fails due to long rule name
CSCwr03611	The LWM "memory free low-watermark processor" value ts changing itself after upgrade
CSCwr83968	Device reloads unexpectedly with static NAT when polling NAT translation data
CSCwq79503	Device reloads unexpectedly during startup due to segmentation fault
CSCwr19450	EVPN type-2 locally originated route is not withdrawn even if there is no information about the MAC/IP in SISF/EVPN Manager/L2RIB.
CSCwr19564	After migration event and receiving the route via the EVPN Fabric, locally originated BGP route and L2RIB route stuck even if the SISF entry and EVPN Manager entry does not exist.
CSCwq29468	BGP routes are advertised with 0 in AS PATH attribute when replacing ASN
CSCwm85778	After VRRS flaps AAA overflows the packet buffers causing an Out of Memory crash
CSCwr51490	DMVPN hub routers experiences an unexpected reload after tunnel down in specific timing scenario
CSCws09528	Device experiences an issue where all line interfaces become blocked and unable to forward traffic
CSCwn18874	DMVPN spoke crashes at NHRP Process
CSCwp17828	uCode core is not getting generated when specific interrupt instructions are executed
CSCwo14975	Memory leak is seen in DNS Proxy; SKA triggers unexpected reloads
CSCwp67808	ZBFW invalid zone drops after upgrade
CSCwn85623	Missing Calling-Station-ID in radius messages
CSCws15533	IPv6 stale entries are not expiring
CSCwr05809	PKI: Discard CRL of greater than 5MB. Large CRL processing can take significant time causing CPUHOG and subsequent crash if it continues
CSCwq22471	Device unexpectedly reboots when importing CA chains
CSCwr10159	Even after the 5-minute ‘block-for’ timer expires, ACL remains active on the VTY lines, preventing SSH access

Identifier	Headline
CSCwq26347	Device accepts under object-group service tcp port range where the end port is less than the starting port
CSCws30834	Device ignores the keepalive command under the SIG tunnel interface
CSCwq32935	After running the **show policy-map type inspect zone-pair sessions** command, memory increase for a couple of hours until it crashes
CSCwk55051	IR1101: polaris_vconfd_cfgpull_t denials observed during config push trigger
CSCwr02964	Initial Authc/Authz does not go to first TACACS server even when the server is alive
CSCwp06965	SNMPv3 user with encrypted password is not seen in **show run** command without re-configuring all SNMPv3 configurations
CSCwr69613	cpp_cp_svr crash if CEF OCE points to MPLS-SR-Tunnel interface
CSCwm01063	Device unexpectedly reload due to segmentation fault on IP SLA DynHostName process
CSCwr09289	Device crashes when collecting backtrace for callsite
CSCwp59954	Unexpected reboot occurs whne PIM Sparse-Dense interface flap triggers a system crash
CSCwo92849	IPcommunity-list standard CLI template attach failure
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when security policy is enabled
CSCwp35552	Calling-Station-ID attribute (31) for 4G is not being shared in the Radius Accounting to Radius Server
CSCwr43693	Memory leak is seen in repm
CSCwr37828	BGP neighborship flap occurs during configure replace
CSCwp10785	Unexpected reload occurs that is caused by HTTP CORE process
CSCwp38609	CTS Trustpoint loop triggers PKI segfault
CSCwr83214	Device send fib-update alarms, causing the maximum alarm limit to be reached
CSCwp36696	IP aliases stuck in VRF even NAT statements removed
CSCwk74877	NETCONF/RESTCONF sync fails and dmiauthd may crash when AAA authentication banner contains a leading newline
CSCwj24696	IPv6 ND HA memory leak seen from IPv6 NS on management port
CSCwm74448	Unexpected reload on device when using the **show logging last X** command
CSCws21640	TFTP server declines TFTP client request when "BLKSIZE" optional header is not contained

Identifier	Headline
CSCwq92340	IOS XE MTP using BDI interface does not forward RTP-NTE when configured for passthrough and report
CSCwn80721	Unexpected reboot is seen in process Sessmgrd
CSCwp40010	RP crash occurs while debugging IKEv2

Open Bugs - Cisco IOS XE 17.15.5

Identifier	Headline
CSCws51814	Increased CPU utilization caused by BGP scanner process
CSCwo60972	Device shows high memory usage as `cpp_ha_top_leve` keeps increasing
CSCws75443	IPv6 neighbour table entries are not timing out causing High TCAM utilisation when no default timers are configured
CSCwr00088	Add CLI to change the per MPLS label CEF statistics query interval on FMAN FP
CSCws71815	Behaviour change for the **ip dhcp use class** command on device
CSCws35452	Device attempts DHCP relay instead of local assignment leading to clients losing connectivity

Resolved Bugs - Cisco IOS XE 17.15.4c

Identifier	Headline
CSCwo75362	Catalyst 8000 series ethernet modules fail to boot after a software reload.

Open Bugs - Cisco IOS XE 17.15.4c

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

Resolved Bugs - Cisco IOS XE 17.15.4

Identifier	Headline
CSCwp03641	Multiple inside local addreses are translated to same inside global IP address and port
CSCwo84352	Unexpected reload occurs when applying the aaa authentication login configuration:
CSCwo19997	QFP crashes with stuck threads while attempting to lock EFT policy under Autonomous mode
CSCwn99822	BFD sessions might not be recovered to up, after **no ip nat outside** is configured on the interface.

Identifier	Headline
CSCwn60316	Ucode crash is observed on the SRTP-SRTP call flow
CSCwm62981	Device crashes with PKI *revocation-check ocsp none* enabled
CSCwn52179	If a device does not receive MPLS binding from LDP peers for a given prefix, MPLS labels will be set to None
CSCwo66822	Device reloads with reason: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwo59694	Unable to deploy the **aaa accounting network** command
CSCwp12923	Cisco Secure client does not receive all the split tunnel network prefixes passed in from the Radius server
CSCwo14777	Device tracebacks observed in VOIP trace flow.
CSCwi44116	Device reboots after change in telemetry subscription update-policy from periodic to on-change
CSCwo42107	Device crashes when applying a service-policy to a PO interface used as a tunnel source
CSCwo90396	Serial interface configuration is lost after reload
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned
CSCwn39832	vDSP fails to go into running state or install hangs with no state in **show app-hosting list**
CSCwn02485	Large fragmented SIP port 5060 and DNS port 53 packets are dropped during virtual reassembly and re-fragmentation operation on the hub router
CSCwp02391	Administratively shutdown interfaces that are part of an EVPN multi-homing Ethernet Segment are unexpectedly brought back up after a BGP EVPN session flap or core isolation recovery event.
CSCwo15543	Standby eWLC crashes after upgrade
CSCwp01534	Elevated memory usage is seen on devices
CSCwn62695	While using debugs of - debug crypto isakmp kmi - there might a crash in IOSd
CSCwn03824	Memory leak in CCSIP_SPI_CONTROL and *Dead* processes
CSCwo05166	Memory leak on Chunk Manager via DBAL EVENTS process
CSCwo99641	Out of CGM (Class-Group Manager) memory intermittently with scaled ZBFW policy
CSCwo09168	Devices crash due to Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6)
CSCwn48140	Failing to ping to service-side IPv4 interface from remote cEdge with IPv6 tunnel and LTE Cellular

Identifier	Headline
CSCwn91302	Device does not retain DSCP markings when using MPLS on tunnel and QOS on underlay interaface
CSCwp40115	Crash occurs while making calls during codec negotiation
CSCwn06900	Segfault in CCSIP_SPI_CONTROL During CALL_LOOP and TLS_SOCKET_SEND_BLOCKED Events
CSCwn60320	SGW sends AOR id value in RPID/PAI header
CSCwm61335	ID manager runs out of IDs, memory leak is seen at cts_authz_acl_info_create when using CTS
CSCwp01610	CUBE is not responding with 200 OK for REINVITE from ISP causing the transfer call to get affected
CSCwn92976	When IPSec is applied on tunnel interface, PPP/LCP negotiation through L2TP fails
CSCwo66011	Config parser issue is seen for NAT with reversible and redundancy
CSCwo47118	Device crashes when clearing L2TP tunnels with the command **clear vpdn tunnel l2tp <ID>**
CSCwo22585	Device crashes when running a NWPI trace initiated from vManage
CSCwk79606	PKI Trustpoint password command only allows encryption type 0 and 7 on all IOS XE platforms
CSCwp02071	Tunnels dropping when CAC configured for VDPN when CPU over threshold due to SSH request for SH tech
CSCwi59338	Enable strict-kex support in IOS-SSH to address CVE-2023-48795 (aka Terrapin Attack)
CSCwo59318	Space issue is seen on the flash during upgrade using Cisco Catalyst Center
CSCwo00577	Random crashes observed after TCP configuration changes
CSCwn60286	Memory Leak observed in IPSEC/IKE session bringup with Cert-based Authentication
CSCwn24226	GETVPN mismatch in GMs reported across COOP due to KEK sync issue between prim & Sec KSs
CSCwo84747	Tunnel delete/create flaps unexpectedly for PWK case for private control NAT changes
CSCwn19586	Certificate-based MACSEC flapping when dot1x reauth timers are set and reload is through
CSCwn50935	Crash occurs during haripin call
CSCwo89702	Configuring logging discriminator name longer than 8 characters reloads standby switch
CSCwp20564	MACsec disable-sci stops the traffic

Identifier	Headline
CSCwn82786	AAA settings not working based on template associated with the domain-name
CSCwn12847	IPSec umbrella tunnels are going down everytime umbrella side executes the rekey
CSCwn93483	confd_cli experiences high cpu utilization after executing the **show zbfw-dp sessions | tab** command

Open Bugs - Cisco IOS XE 17.15.4

Identifier	Headline
CSCwq08151	Device experiences unexpected reload due to DBGD process
CSCwo57783	A *NHRP Encap Error for Purge Request* message populates on spoke despite correct routing at HUB
CSCwp28915	SNMP walk fails to consistently return tunnel names due to incomplete tunnel setup

Resolved Bugs - Cisco IOS XE 17.15.3a

Identifier	Headline
CSCwm73195	C8000V: show interfaces counters are incorrect and unreasonably large
CSCwn07540	C8000V: Crash observed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE
CSCwm72099	DPDK: ICE PF driver reports MDD and shuts down the driver
CSCwn99723	**request platform software package expand** commands are deprecated for upgrades
CSCwn57838	Startup configuration lost for NIM-(1|2)GE-CU-SFP interfaces
CSCwn99822	Large number of BFD sessions stuck with out of window drops with Kotak bank profile
CSCwn51758	Incoming packets are dropped with bad checksum when passing L2tp traffic through the IPSec encrypted tunnel
CSCwm71639	cpp_cp_svr crash is noticed when service-policy is configured to a dialer interface
CSCwn40794	IOS-XE crash PKI: Failed to load cert chain for trustpoint
CSCwn24226	GETVPN mismatch in GMs reported across COOP due to KEK sync issue between primary and secondary KS
CSCwo09168	Device crashes due to critical process vip_confd_startup_sh fault on rp_0_0 (rc=6)
CSCwm78086	BFD session is down after change in TLOC preference with pairwise-keying is enabled
CSCwn20614	After a change in the integrity-type twice, all BFD sessions are down.
CSCwm60651	HTX: UTD crash is only seen in response to a dataplane crash

Identifier	Headline
CSCwn56474	Every single BFD session state change with up/down may trigger IPSec tunnel delete/create events unexpectedly with pairwise-keying enabled
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel
CSCwn53302	Administrative distance of IPv6 static route to cellular interface is overwriten with route with AD 254
CSCwn35476	cflowd source interface for sub-interface does not get pushed to device
CSCwo03915	Unexpected reload on device due to performance monitoring with packet service insertion from spoke
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call
CSCwk08261	Unexpected reload occurs with ipv4_sbc_input () at /dplane/feature/sbc/sbc_packet decode
CSCwn48914	Router crashes during SGW sync in VOICE REG BG process
CSCwn61584	The **listen-port** command does not work as expected under tenants for UDP
CSCwn13988	CDR file accounting credentials exposure
CSCwn60303	**cube sip-ua** commands lost after reload
CSCwm91195	Memory leak is seen in subscribe pass-thru scenarios
CSCwn19326	CDR file accounting creates dummy files
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak
CSCwn49403	CUBE incorrectly offers RTP instead of SRTP in 200OK for SRTP fallback scenarios

Open Bugs - Cisco IOS XE 17.15.3a

Identifier	Headline
CSCwh91039	C8000V: High system CPU load is reported due to unsupported number of vCPUs allocated
CSCwm71868	Stopping C8000V in Azure results in the device reloading and stopping after 10 minutes
CSCwo45527	C8000V: Hot add and delete do not work in AWS
CSCwn85623	Missing Calling-Station-ID in radius messages
CSCwn92976	PPP is not establishing when L2tp over ipsec
CSCwn60286	IOS-XE: Memory leak is observed in IPSEC/IKE session bringup with cert-based authentication
CSCwn44339	Router crashes due to failed DLC license conversion when contacting CSSM

Identifier	Headline
CSCwo47118	Crash observed when clearing L2TP tunnels with the **clear vpdn tunnel l2tp <ID>** command
CSCwn48140	Failing to ping to service-side IPv4 interface from remote cEdge with IPv6 tunnel and LTE cellular
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned
CSCwj65057	BFD sessions stuck in down state due to SA_NOT_FOUND

Resolved Bugs - Cisco IOS XE 17.15.2a

Identifier	Headline
CSCwk69597	C8000V: Running config write memory does not persist after reload
CSCwi87546	CPP unexpectedly reboots due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released
CSCwk53438	Process crash seen on SD-Routing TSN platform. Permission Denied errors seen.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered
CSCwk63722	Startup configuration failure occurs post PKI server enablement
CSCwk64137	High IRAM utilization at 99% in scaled flows
CSCwk70630	Cannot import device certificate
CSCwk85704	"match traffic-category " through vManage add-on CLI push failed
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels
CSCwm07651	An IOS XE router running as a cEdge may experience an unexpected reset due to dbgd process
CSCwm13223	Crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog
CSCwm30984	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device - CCE changes
CSCwm31516	DSMP layer is unable to close EDSP channels if a call is disconnected before connect
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats
CSCwm05524	Unexpected reload occurs due to "cpp-mcplo-ucode" process when handling fragments with SRv6 routing
CSCwm14462	IPv6 flowspec nexthop redirect policy does not redirect the traffic on IOS XE
CSCwm41535	DSP occasionally crashes when pcm capture is enable
CSCwk50488	Unexpected reboot occurs due to a memory leak produced under the process fman_rp database
CSCwk81360	Cisco IOS-XE router reboots unexpectedly while configuring NAT Static Translation

Identifier	Headline
CSCwk61133	Process IOMd memory leak due to POE TDL message
CSCwk61238	RRI static does not populate route after reload if stateful IPSec is configured
CSCwh96578	SKA_PUBKEY_DB leak found in TDL

Open Bugs - Cisco IOS XE 17.15.2a

Identifier	Headline
CSCwk37946	C8000V: Error message seen whenever Intel I350-sriov driver is used in the setup with vrrp/hsrp configuration, and state change occurs
CSCwm28388	C8000V: CPU HOG traceback appears randomly and intermittently on specific AWS instance types
CSCwn83135	Unable to reach Inband Management IP on standby firewall HA Device
CSCwn80352	Device removes NAT egress-interface option from cEdge config - NAT yang changes
CSCwn80360	Device removes NAT egress-interface option from cEdge config - CRYPTO yang changes
CSCwn36533	vmanage_system and loopback65529 interfaces using DOD ip range and need to disable it
CSCwn46221	CLI for FlexVPN tunnel on device does not work
CSCwn38464	Unable to configure stream on cellular interface
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface
CSCwn07671	Tracker group with IP and DNS name tracker elements goes down when DNS query is failing
CSCwn35772	Umbrella SMU with interfaces using DOD ip range
CSCwn40794	IOS-XE crash PKI: Failed to load cert chain for trustpoint
CSCwn59851	Unexpected reload critical process linux_iosd_image fault on rp_0_0 (rc=139)
CSCwn85623	Missing Calling-Station-ID in radius messages
CSCwn92976	PPP is not establishing when L2tp over IPsec
CSCwm74060	IOSD crashes when retrieving platform info
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled
CSCwn65589	DMVPN Tunnel bounces a second time after RP3 failover and recovery

Resolved Bugs - Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwi90648	C8000v crashes in ESXi On-prem environment
CSCwi34858	NETVSC VLAN sub interfaces not passing traffic after upgrade
CSCwj85529	C8000V license boot level config done via 'customdata' is getting lost after reload
CSCwk54698	C8000V hosted in Azure reloaded unexpectedly generating a system report
CSCwj51700	CPP crashes after re-/configuring **ip nat settings pap limit ... bpa** feature in high QFP state.
CSCwk42634	%PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6)
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk16333	Device repeatedly crashing in FTMd due to FNF flow add.
CSCwj96852	Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC.
CSCwj95633	SAIE application - no data to display for IOS XE router.
CSCwk39131	Device crashed when issuing **show sdwan ftm next-hop chain all**.
CSCwk22225	FTMd crashes after receiving credentials feature template update.
CSCwj48909	Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk45165	fman_fp memory leak on device.
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup.
CSCwj90614	High CPU utilisation for confd_cli.
CSCwi81026	BFD sessions flapping during IPSec rekey in scaled environment.
CSCwk39268	sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11.
CSCwj76662	High memory utilization due to "ftmd" process.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk44078	GETVPN / migrating to new KEK RSA key does not trigger GM re-registration.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.

Identifier	Headline
CSCwj96092	ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	Device unexpectedly reloads due to a crash in 'vdaemon' process.
CSCwi99454	FNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive.
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwj02401	Router reloaded when generating admin tech while processing very high number of flows.
CSCwk19725	add FNF cache limit for show sdwan app-fwd flows.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.
CSCwj67591	Chassis activate effective only after second re-try - with new uuid.
CSCwj32347	DIA endpoint tracker not working with ECMP routes.

Open Bugs - Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwh91039	C8000V: High system CPU load reported due to unsupported number of vCPUs allocated
CSCwk75733	Custom applications may not be programmed properly.
CSCwk89256	Speed mismatch in IOS-XE configuration after device template push.
CSCwk85704	"match traffic-category " add-on CLI push failed.
CSCwk87944	VRRP switchover with tloc preference change is generating rekey and crypto add/delete events.
CSCwk86355	File transfer fails "lost connection".
CSCwk49806	Router rebooted unexpectedly due to process NHRP crash.
CSCwk81360	Router can reboot unexpectedly while configuring NAT static translation.
CSCwk62954	Multiple "match address local interface <int>" not pushed under crypto profile.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwm07564	data-policy local-tloc-list breaks RTP media stream.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered.

Identifier	Headline
CSCwk74298	Device denied for template push and some show commands with error application communication failure.
CSCwk98578	GETVPN IPv6 crypto map not shown in interface configuration.
CSCwk70630	Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwm13223	Device crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog.
CSCwk79454	Endpoint tracker does not fail if default route is removed.
CSCwk69597	C8000V running config write memory did not persist after reload.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.
CSCwi87546	Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - lock id of 0 released.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwm12851	Device uses 3DES as default rekey algorithm for GETVPN.
CSCwk95044	1SPA.smu.bin drops when packet duplication link fails-over.
CSCwj87028	Device showing custom APP as "unknown" for egress traffic when using DRE Opt.
CSCwm08545	Centralized policy policer worked per PC on the same site not per site/vpn-list.
CSCwf62943	System image file is not set to packages.conf when image expansion fails due to disk space.
CSCwm00309	Packets not hitting the correct data policy after modifying the action of a sequence.

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 results 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.