Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, 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)

About The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note Sections in this documentation apply to all models of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

Note Cisco IOS XE 17.15.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE 17.15.x release series.

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 Changed Hardware and Software Features

There are no new hardware features in this release.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.

Note To access CFN, you do not require an account on cisco.com.

New and Changed Hardware Features

There are no new hardware features in this release.

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

There are no new features in this release.

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 Changed Software Features in Cisco IOS XE 17.15.3a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.2a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.1a

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms

Feature	Description
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.

Feature	Description
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.
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
Flexible Gigabit Ethernet and Fibre Channel Services	Cisco Coarse Wavelength-Division Multiplexing (CWDM) Small Form-Factor Pluggable (SFP) solution allows you to deploy scalable Gigabit Ethernet and Fibre Channel services efficiently. These hot-swappable transceivers convert electrical signals into single-mode fiber-optic interfaces and can be connected to CWDM passive optical systems using standard SC connectors
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.

Feature	Description
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.
Monitoring 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 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.
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.
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.
Seamless Software Upgrade for SD-Routing Devices	This feature explains how to seamlessly upgrade and onboard an existing Cisco Routing device into the Cisco SD-WAN infrastructure.
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.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.15.x releases.

Table 2: Minimum and Recommended ROMMON Releases Supported on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X|6T	17.15.1a	17.3(4.2r)	17.9(7r)
C8300-2N2S-4T2X|6T	17.15.1a	17.3(4.1r)	17.7(1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)
C8200L-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)

Note For Cisco Catalyst 8200 and 8200L Series Edge platforms, if your ROMMON is at a version lower than 17.6(8.1r), you can upgrade the device to IOS XE 17.15.1a using any of the following methods:

- in bundle mode, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a, OR
- in bundle mode, manually upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a.
- in install mode, you can upgrade the device to IOS XE 17.15.1a; the ROMMOM is auto-upgraded to the recommended version when the device boots.

For Cisco Catalyst 8300 Series Edge platforms, if your ROMMON is at a version lower than the minimum supported version, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to the recommended version. You can then upgrade the device to 17.15.1a.

Upgrade ROMmon

To upgrade the ROMmon version of your device, use these steps:

1. Check the existing version of ROMmon by using **show rom-monitor r0** command. If you are installing Cisco IOS XE software on a new device, skip this step.
2. Review Minimum and Recommended ROMmon Releases to identify the recommended version of ROMmon software for the device you plan to upgrade.
3. Go to https://software.cisco.com/# and download the ROMmon package file.
4. Copy the ROMmon file to flash drive:

   copy ftp://*username*:*password*@*IP address*ROMmon package file **flash:**

5. Upgrade the ROMmon package using the following command:

   upgrade rom-monitor filename bootflash:*ROMmon package name* **all**

6. Execute **reload** command to complete the ROMmon upgrade process
7. Execute **show rom-monitor r0** command to ensure the ROMmon software is upgraded.

Resolved and Open Bugs for 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.

Identifier	Headline
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 in Cisco IOS XE 17.15.5

Identifier	Headline
CSCwp06956	NGFW Policy deployment fails due to long rule name.
CSCwr03611	LWM "memory free low-watermark processor" value its changing itself after upgrade.
CSCwr83968	Unexpected reload on cEdge with static NAT when polling NAT translation data.
CSCwq79503	Device may reload unexpectedly during startup due to segmentation fault.
CSCwr19450	Stuck locally originates BGP EVPN type-2 route.
CSCws30834	Device ignore the keepalive command under the SIG tunnel interface pushed by the vmanage.
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.
CSCwq92624	Device unexpected reload with configuration changes.
CSCwr51490	DMVPN hub routers could experience an unexpected reload after tunnel down in specific timing scenario.
CSCwq07879	Unexpected reload when issuing show commands related to STCAPP.
CSCwq90015	The unicast communication of the directly - connected link is not working, but the multicast communication is normal.
CSCws09528	TPLUS Process is taking high CPU in IOSd.
CSCwn18874	DMVPN spoke crashed at Process = NHRP.
CSCwo14975	Memory Leak 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 not expiring.
CSCwr05809	PKI : Discard CRL of greater than 5MB on device.

Identifier	Headline
CSCwq22471	Device may unexpectedly reboot when importing CA chains.
CSCwr10159	sl_def_acl is not getting removed from vty after block period expiry.
CSCwq26347	object-group service TCP port range .
CSCwq32935	Device after running show policy-map type inspect zone-pair sessions memory increase for a couple of hours until it crash.
CSCwk55051	polaris_vconfd_cfgpull_t denials during config push trigger.
CSCwr02964	Initial Authc/Authz not going to first TACACS server even when the server is alive.
CSCwp06965	SNMPv3 user with encrypted pswd is not seen in 'show run' without re-configuring all snmpv3 configs.
CSCwr69613	cpp_cp_svr crash if CEF OCE points to MPLS-SR-Tunnel interface.
CSCwm01063	Unexpected reload due to segmentation fault on IP SLA DynHostName process.
CSCwr09289	Crash when collecting backtrace for callsite.
CSCwr19564	Stuck EVPN BGP type-2 local route and L2RIB route.
CSCwp59954	Unexpected Reboot: PIM Sparse-Dense Interface Flap Triggers System Crash.
CSCwo92849	ip community-list standard CLI template attach failure.
CSCwo75966	Pubd memory leak when SSID monitoring is disabled.
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy.
CSCwp35552	Missing Calling-Station-ID (31) in Radius Accounting.
CSCwr43693	Memory leak in repm.
CSCwr37828	BGP neighborship flap during configure replace.
CSCwp10785	Unexpected Reloads Caused by HTTP CORE Process.
CSCwp38609	CTS Trustpoint loop triggers PKI segfault.
CSCwr83214	cEdge is sending lots of fib-updates alarms to vManage filling max alarms in vManage.
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.
CSCwm27749	Speed test download / Throughput issue on C8200 platform seen with IPSEC ESP-NULL transform using Zscaler.
CSCwj24696	IPv6 ND HA Memory Leak from IPv6 NS on Mgmt port.

Identifier	Headline
CSCwm74448	Defect Created by AutoAn for eem_cli_template_cedge.
CSCws21640	TFTP server declines TFTP client request when "BLKSIZE" optional header is not contained.
CSCwq92340	IOS XE MTP using BDI interface does not forward rtp-nte when configured for passthrough and report.
CSCwn80721	Unexpected Reboot in Process Sessmgrd.
CSCwp40010	RP Crash While Debugging IKEv2.
CSCwo75362	Device ethernet modules fail to boot after software reload.

Open Bugs in Cisco IOS XE 17.15.5

Identifier	Headline
CSCws75443	IPv6 neighbour table entries are not timing out causing High TCAM utilisation (no default timers configured).
CSCws71815	Behaviour change for "ip dhcp use class" command on router.
CSCws51814	Increased CPU utilization caused by BGP scanner process.
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP.
CSCws35452	Device attempts DHCP relay instead of local assignment – clients losing connectivity.

Resolved Bugs in Cisco IOS XE 17.15.4c

Identifier	Headline
CSCwq31287	Device software SNMP denial of service and remote code execution vulnerability.

Open Bugs in Cisco IOS XE 17.15.4c

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

Resolved Bugs in Cisco IOS XE 17.15.4

Identifier	Headline
CSCwp03641	Multiple inside local addreses are translated to same inside global IP address and port.
CSCwo84352	Segmentation fault on the sessmgrd process.
CSCwo19997	QFP crash with stuck threads while attempting to lock cft policy under autonomous mode.

Identifier	Headline
CSCwn99822	Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps.
CSCwn60316	"cpp-mcplo-ucode" crashes on device running IOS-XE 17.9.5a.
CSCwm62981	Device crashes with PKI "revocation-check ocsp none" enabled.
CSCwn52179	Traffic with TTL 2 is punted to CPU when CEF holds **MPLS** labels set to **None**.
CSCwo66822	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).
CSCwo59694	Unable to Deploy 'aaa accounting network' Command.
CSCwp12923	IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from Radius server .
CSCwi44116	IOS-XE reboot after change telemetry subscription update-policy from periodic to on-change
CSCwo42107	Device crashes when applying a service-policy to a PO interface used as Tunnel source.
CSCwo90396	Serial interface configuration lost after reload.
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwn39832	Adding "authorization bypass" to vDSP EEM scripts.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwp02391	Administratively shutdown ports Are re-enabled after core isolation recovery (WAN link recovered).
CSCwo15543	Functional SJC Alpha 9840 eWLC HA- Standby eWLC reloads after upgrade to 17.17.1.
CSCwp01534	Elevated memory usage on devices.
CSCwn62695	KMI messages introducing a crash while enabling debug.
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	cEdges running 17.12.4 crashed 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.
CSCwo14777	Router tracebacks observed in voip trace flow.

Identifier	Headline
CSCwp40115	Crash 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 @ cts_authz_acl_info_create when using CTS.
CSCwp01610	CUBE is not responding with 200 OK for REINVITE from ISP causing the transfer call getting affected.
CSCwn92976	PPP is not establishing when l2tp over ipsec.
CSCwo66011	Config parser issue for NAT with reversible and redundancy.
CSCwo47118	Crash when clearing L2TP tunnels with the command "clear vpdn tunnel l2tp <ID>".
CSCwo22585	cEdge device crashes when running a NWPI trace initiated from vManage on version 20.12.4
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	Facing space issue on the flash during upgrade using Cisco Catalyst Center.
CSCwo00577	Random crashes observed after tcp confg 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 after reload.
CSCwn50935	Crash occurs during haripin call.
CSCwo89702	Configuring logging discriminator name longer than 8 characters reloads standby switch.
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.

Identifier	Headline
CSCwn93483	confd_cli high cpu utilization after executing "show zbfw-dp sessions | tab".
CSCwn39832	Adding "authorization bypass" to vDSP EEM scripts.

Open Bugs in Cisco IOS XE 17.15.4

Identifier	Headline
CSCwq08151	Device experienced unexpected reload due to dbgd process.
CSCwo57783	"NHRP Encap Error for Purge Request" populates on spoke despite correct routing at HUB.
CSCwp28915	SNMP walk fails to consistently return tunnel names due to incomplete tunnel setup.

Resolved Bugs in Cisco IOS XE 17.15.3a

Identifier	Headline
CSCwn99822	Large number of BFD sessions stuck with out of window drops with Kotak bank profile.
CSCwm78086	BFD session is down after change tloc preference with pairwise-keying enabled.
CSCwn56474	Pairwise-keying every single bfd session up/down which trigger tunnel delete/create events.
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call.
CSCwn57838	Startup config lost for interfaces NIM-(1|2)GE-CU-SFP.
CSCwo03915	Unexpected reload on device due to performance monitor with packet service insertion from spoke.
CSCwo09168	Device crashed due to critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwn53302	Administrative distance of IPv6 static route to cellular interface overwrite with 254.
CSCwn51758	Incoming packet are drop with bad checksum when l2tp through ipsec encrypted tunnel on device.
CSCwm71639	cpp_cp_svr crash noticed when configured service-policy to a dialer interface.
CSCwn20614	After change integrity-type twice, all bfd sessions will be down.
CSCwn15231	Device null-way audio within the same layer2.
CSCwn40794	Failed to load cert chain for trustpoint.
CSCwk27078	Device ROMMON auto-upgrade is failing.

Identifier	Headline
CSCwn24226	GETVPN Mismatch in GMs reported across COOP Due to KEK Sync Issue Between Prim & Sec KSs.
CSCwm60651	UTD snort crash at memif_shm_peek_first_packet (handle=0x0).
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel.
CSCwn35476	Cflowd source interface for sub-interface does not get pushed to cedge.
CSCwn48914	Router crash during SGW sync in VOICE REG BG Process.
CSCwn61584	Listen-port command is not working properly under tenants for UDP.
CSCwn13988	CDR file accounting credentials exposure.
CSCwn60303	Router cube sip-ua commands lost after reload.
CSCwm91195	Memory leak on CUBE in subscribe pass-thru scenario.
CSCwn19326	CDR file accounting creates dummy files.
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak on CUBE.
CSCwn49403	CUBE incorrectly offers rtp instead of srtp in 200OK for srtp fallback scenario.

Open Bugs in Cisco IOS XE 17.15.3a

Identifier	Headline
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwn92976	PPP is not establishing when l2tp over ipsec.
CSCwn60286	Memory Leak observed in IPSEC/IKE session bringup with cert-based authentication.
CSCwn44339	Router crash due to failed DLC license conversion when contacting CSSM.
CSCwn82715	DSL SFP: VDSL/ADSL lines are flapping in Customer site.
CSCwn24036	Tx/Rx optical power values diffrent for "show int" and "show hw-module".
CSCwo47118	Crash when clearing L2TP tunnels with the command "clear vpdn tunnel l2tp <ID>".
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 in Cisco IOS XE 17.15.2a

Identifier	Headline
CSCwm37417	Interface does not always come back up after a **clear interface** command.
CSCwk68546	HSEC request is included in rum report when using network-advantage_T0 license.
CSCwm14665	Enable BFD L2 messages in the Punt path for the device.
CSCwm41535	DSP occasionally crashes when pcm capture is enabled.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwk87452	Procyon synchronize DTL does not wait until complete due to compiler optimization.
CSCwm31516	DSMP layer is unable to close EDSP channels if a call is disconnected before connect.
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwk81360	Cisco IOS-XE router can reboot unexpectedly while configuring NAT static translation.
CSCwk53438	Process crash seen on SD-Routing TSN platform + Permission Denied errors.
CSCwk85704	**match traffic-category** through vManage add-on CLI push failed.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering statistics.
CSCwk64137	High IRAM utilization at 99% in scaled flows.
CSCwk70630	Cannot import device certificate.
CSCwm07651	An IOS XE router running as a cEdge may experience an unexpected reset due to dbgd process.
CSCwk61133	Process IOMd memory leak due to POE TDL message.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device.
CSCwm30984	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device - CCE changes.
CSCwm05524	Unexpected Reload Due to "cpp-mcplo-ucode" Process when handling fragments with SRv6 routing
CSCwk50488	Memory leak in fman_rp under acl_db.
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE.
CSCwm13223	Device crashes in IOSd due to Malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog.

Open Bugs in Cisco IOS XE 17.15.2a

Identifier	Headline
CSCwm11203	Static default route disappears on RIB table.
CSCwm67178	Cannot configure MD5 for the hash under the IKEv2 proposal when compliance shield is disabled.
CSCwn07671	Tracker group with IP and DNS name tracker elements goes down when DNS query is failing.
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwn31739	Device crashes when EPC is configured on 100Gb link.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwn40794	Device crash PKI: Failed to load cert chain for trustpoint.
CSCwm62981	Device crashes with PKI **revocation-check ocsp none** enabled.
CSCwn80352	Device removes NAT egress-interface option from cEdge config - NAT yang changes.
CSCwm74060	IOSD chasfs task crashes when retrieving platform information.
CSCwn65589	DMVPN Tunnel bounces for the second time after RP3 failover and recovery.
CSCwn82715	DSL SFP: VDSL/ADSL lines are flapping in customer site.
CSCwn59851	Unexpected reload Critical process linux_iosd_image fault on rp_0_0 (rc=139).
CSCwn92976	PPP is not establishing when l2tp over IPsec.
CSCwn83135	Unable to reach inband management IP on standby firewall HA device.
CSCwn46221	**peer reactive** CLI for FlexVPN tunnel on IR1800 does not work.
CSCwn36533	Device interface using DOD ip range.
CSCwn35772	CCP craashed during UTD policy config application.
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwn38464	Unable to configure stream on cellular interface.
CSCwn80360	Device removes NAT egress-interface option from cEdge config - CRYPTO yang changes.

Resolved Bugs in Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwj51700	CPP crashes after re-/configuring **ip nat settings pap limit ... bpa** feature in high QFP state.

Identifier	Headline
CSCwk03686	Crash due a segmentation fault due a negative value.
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**.
CSCwk37351	IOS XE router: unexpected reboot during PVDM OIR.
CSCwk22225	FTMd crashes after receiving credentials feature template update.
CSCwj48909	Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk23723	Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwk45165	fman_fp memory leak on device.
CSCwj16153	10G front-panel port does not go down on single mode fiber when Rx side goes down.
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.
CSCwj92560	STCAPP command removed from device after reload.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk44078	GETVPN / migrating to new KEK RSA key does not trigger GM re-registration.

Identifier	Headline
CSCwi99454	FNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwj96092	ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	Device unexpectedly reloads due to a crash in 'vdaemon' process.
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492.
CSCwj02401	Router reloaded when generating admin tech while processing very high number of flows.
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwk19725	add FNF cache limit for show sdwan app-fwd flows.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwj67591	Chassis activate effective only after second re-try - with new uuid.
CSCwj32347	DIA endpoint tracker not working with ECMP routes.
CSCwj41728	Unable to install the TE agent using http link in CLI

Open Bugs in Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwi76516	esim cellular configuration tamplate deployemt fails.
CSCwk75733	Custom applications may not be programmed properly.
CSCwk89256	Speed mismatch in IOS-XE configuration after device template push.
CSCwm07994	Router crash with stuck threads.
CSCwk85704	**match traffic-category** add-on CLI push failed.
CSCwj01917	After upgrade, cellular interface IP ADDRESS NEGOTIATED mismatching.
CSCwm01269	Speed test is giving better result from TLOC extension from the secondary router.
CSCwj76689	Device configuration lost after .bin upgrade.
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.

Identifier	Headline
CSCwk62954	Multiple "match address local interface <int>" not pushed under crypto profile.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk97092	MKA session not coming up after shut/no shut with EVC.
CSCwm07564	data-policy local-tloc-list breaks RTP media stream.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered.
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.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwk70630	Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded.
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.
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	SPA.smu.bin drops when packet duplication link fails-over.
CSCwj87028	Device showing custom APP as "unknown" for egress traffic when using DRE Opt.
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
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

- Hardware Installation Guide for Catalyst 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms

- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide

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.