



# Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE Dublin 17.12.x

---

**First Published:** 2023-08-22

**Last Modified:** 2023-12-18

## 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](http://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 Dublin 17.12.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Dublin 17.12.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

### 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://cfng.cisco.com/>.



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

### New and Changed Hardware Features

Hardware	Description
<a href="#">Cisco C-NIM-8M</a>	The C-NIM-8M are the next generation LAN/WAN NIM modules that provide enhanced security, reliability, and performance. The Cisco C-NIM-8M module provides 2.5 Gbps mGig connectivity and supports UPoE+. Also, Cisco C-NIM-8M supports Layer 2 and Layer 3 configurable Ethernet network.

### New and Changed Software Features in Cisco IOS XE 17.12.2

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 17.12.1a

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

Feature	Description
<a href="#">IPv6 Unicast Support with DLEP</a>	The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.
<a href="#">Managing the SD-Routing Devices Using Cisco SD-WAN Manager</a>	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network manage system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.
<a href="#">Quantum-Safe Encryption Using Post-Quantum Preshared Keys</a>	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: <ul style="list-style-type: none"> <li>• Cisco Catalyst 8300 Series Edge Platforms</li> </ul>

Feature	Description
<a href="#">Segment Routing over IPv6 Dataplane</a>	<p>Segment Routing (SR) can currently be applied on Multiprotocol Label Switching (MPLS) dataplane. From Cisco IOS XE 17.12.1a, SR is supported over the IPv6 dataplane for the following protocols:</p> <ul style="list-style-type: none"> <li>• Interior Gateway Protocol (IS-IS only)</li> <li>• Border Gateway Protocol (BGP)</li> </ul> <p>In addition, the following functionalities are available for Segment Routing over IPv6 dataplane:</p> <ul style="list-style-type: none"> <li>• Segment Routing Traffic Engineering Policies</li> <li>• Static Routes</li> <li>• Performance Management</li> <li>• Operations, Administration and Maintenance (OAM)</li> </ul>
<a href="#">Support for Automatic Log Deletion</a>	<p>This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the <a href="#">logging purge-log buffer days</a> command.</p>
TrustSec and Software-Defined Access Scale Measurement	<p>With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following:</p> <ul style="list-style-type: none"> <li>• Security Group Tag (SGT) or Destination Group Tag (DGT) Policies</li> <li>• Unidirectional IPv4 SGT Exchange Protocol (SXP) connections</li> <li>• Bidirectional IPv4 SXP connections</li> <li>• IPv4 SGT Bindings</li> <li>• IPv6 SGT Binding</li> <li>• Security Group Access Control Entries (SG ACEs)</li> </ul>

## ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.12.x releases.

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

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
<b>Catalyst 8300 Series Edge Platforms</b>			
C8300-1N1S-4T2X 6T	17.12.1a	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X 6T	17.12.1a	17.3(1.2r)	17.6(6.1r)
<b>Catalyst 8200 Series Edge Platforms</b>			
C8200-1N-4T	17.12.1a	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.12.1a	17.5(1.1r)	17.6(6r)

## Resolved and Open Bugs for Cisco IOS XE 17.12.x

### Resolved Bugs in Cisco IOS XE 17.12.2

Identifier	Headline
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a> .
<a href="#">CSCwf78735</a>	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPsec cannot be applied.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating TP generates an invalid TP.
<a href="#">CSCwh20734</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
<a href="#">CSCwh41497</a>	DDNS update retransmission timer fails to work with a traceback error.
<a href="#">CSCwf63706</a>	Device HSRP received unexpected active hello packet when the interface is recovered.
<a href="#">CSCwf49390</a>	Device crashes@crypto_map_unlock_map_head.
<a href="#">CSCwh30377</a>	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
<a href="#">CSCwh20577</a>	Crashed by track client thread at access invalid memory location.
<a href="#">CSCwf82676</a>	CPU usage mismatch in <b>show sdwan system status</b> vs <b>show process cpu platform</b>
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCwf80191</a>	Flowspec on device does not revoke.
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running <b>show crypto</b> command.
<a href="#">CSCwf67564</a>	Device observes memory leak at process "SSS Manager".

Identifier	Headline
<a href="#">CSCwf60151</a>	Memory leak with pubd.
<a href="#">CSCwh60190</a>	<b>ip name-server</b> command not pushed.
<a href="#">CSCwf56463</a>	IOS process crash during VRRP hash table lookup.
<a href="#">CSCwh11858</a>	Device running IOS-XE crashes when removing FQDN ACL.
<a href="#">CSCwf99906</a>	NTP authentication removed after reload using more than 16 bytes.
<a href="#">CSCwf59173</a>	Segmentation fault at IPv6 BGP backup route notification.
<a href="#">CSCwf67351</a>	Cisco IOx application hosting environment privilege escalation vulnerability.
<a href="#">CSCwf68612</a>	WLC unexpected ueload due to segmentation fault in WNCD process.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot.
<a href="#">CSCwf41084</a>	Extranet multicast code improvements for better handling of data structure.
<a href="#">CSCwh04884</a>	VC down due to control-word negotiation.
<a href="#">CSCwf26494</a>	BDI + NTP configuration puts DMI process in degraded mode.
<a href="#">CSCwh96700</a>	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

### Open Bugs in Cisco IOS XE 17.12.2

Identifier	Headline
<a href="#">CSCwh73350</a>	Router keeps crashing when processing a firewall feature.
<a href="#">CSCwh94906</a>	Segmentation fault crash with Network Mobility Services Protocol (NMSP).
<a href="#">CSCwf67983</a>	The platform USB disable will not work once USB is removed and inserted.
<a href="#">CSCwh22414</a>	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
<a href="#">CSCwh59071</a>	Displays faulty Output for <b>show int te0/0/0 transceiver</b> command.
<a href="#">CSCwh16901</a>	HSEC license installation from the workflow does not complete.
<a href="#">CSCwh77221</a>	SNMP unable to poll Cisco SD-WAN tunnel data after a minute.
<a href="#">CSCwh10813</a>	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
<a href="#">CSCwh68508</a>	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
<a href="#">CSCwh79161</a>	Device requires Shut/No Shut to populate IP address from modem to host.
<a href="#">CSCwh75800</a>	Router unexpectedly reloads while fetching certificate trustpool for SIP TLS.

Identifier	Headline
<a href="#">CSCwh57544</a>	Silent reload due to LocalSoftADR causes crash without core file.
<a href="#">CSCwi01046</a>	PoE module is not providing enough power to bring the ports after an unexpected reload.
<a href="#">CSCwh50510</a>	Router crash with segmentation fault (11), Process = NHRP when processing NHRP traffic
<a href="#">CSCwd69953</a>	Device driver is not sending NGIO packets to UCSE after the router reload.
<a href="#">CSCwh73320</a>	NAT Pool does not working under prefix 16. Available address = zero.
<a href="#">CSCwh96700</a>	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper.
<a href="#">CSCwh45169</a>	Unexpected reboot while displaying information from cleared SSS session.
<a href="#">CSCwh70449</a>	PMTUD incorrectly converging without attempting to learn a higher MTU.
<a href="#">CSCwf91481</a>	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwh83228</a>	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running.
<a href="#">CSCwe54687</a>	After removing the USB from the device, the files copied to it will be deleted.
<a href="#">CSCwh91136</a>	IOS XE:Traffic not encrypted and dropped over PSec SVTI tunnel.
<a href="#">CSCwh96415</a>	Unable to disable DMVPN logging.
<a href="#">CSCwh12093</a>	Enable SoS/ROC feature for DSL.
<a href="#">CSCwf86207</a>	Frame relay DTE router crashes due to EXMEM exhaustion.
<a href="#">CSCwh58252</a>	IPv6 SPD min/max defaulting to values 1 and 2.
<a href="#">CSCwh14083</a>	High CPU due to MPLS MIB poll.
<a href="#">CSCwh22981</a>	WNCD process crashes.
<a href="#">CSCwh99513</a>	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
<a href="#">CSCwh90851</a>	pubd process showing high CPU utilization.
<a href="#">CSCwh83532</a>	1Gig int on device using GLC-SX-MMD are down/down after changing connection.
<a href="#">CSCwh96891</a>	Memory leak with pubd.
<a href="#">CSCwh91085</a>	Convergence improvement after device reboot with mVPN profile 14.

Identifier	Headline
<a href="#">CSCwh58919</a>	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
<a href="#">CSCuu85298</a>	FIB/LFIB inconsistency after BGP flap.
<a href="#">CSCwf83684</a>	IOS XE router may experience "%FMANRP_QOS-4-MPOLCHECKDETAIL:" errors.
<a href="#">CSCwh59926</a>	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.
<a href="#">CSCwh24280</a>	Mismatch between the resource allocation and "app-resource profile custom" configuration.
<a href="#">CSCwh82668</a>	Incorrect local MPLS label in CEF after BGP flap.
<a href="#">CSCwh95036</a>	Cisco IOS-XE IPv6 based subscription telemetry does not work.
<a href="#">CSCwh99464</a>	Guestshell connectivity not working with NAT overload.
<a href="#">CSCwh30928</a>	SDA - using "spt-threshold infinity" and having LHR+FHR can cause the S,G to be pruned on the RP.
<a href="#">CSCwh01738</a>	Unexpected reload when using rsh/remd.
<a href="#">CSCwh04124</a>	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
<a href="#">CSCwh67285</a>	WLC unable to get telemetry data due to pubd unexpected reload and fail.
<a href="#">CSCwh96332</a>	Device crash due to dhcpd_binding_check.
<a href="#">CSCwh56940</a>	Site tag change wncd working/failing EAP-TLS.
<a href="#">CSCwh44418</a>	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.
<a href="#">CSCwh46559</a>	LLDP location information not sent when configured.
<a href="#">CSCuv36790</a>	<b>clear bgp</b> command does not consider AFIs when used with update-group option.
<a href="#">CSCwh02698</a>	Device sending incomplete SGT to ISE.
<a href="#">CSCwh05869</a>	Only portion of HSRP config being pushed via CLI ADDON template.
<a href="#">CSCwf53750</a>	"match pktlen-range" does not work with GRE/IPSEC GRE.
<a href="#">CSCwh60107</a>	In the show tech file, "enable secret" does not get hidden.
<a href="#">CSCwh45579</a>	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
<a href="#">CSCwh95024</a>	ISIS crash in local uloop.
<a href="#">CSCwh41155</a>	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.



Identifier	Headline
<a href="#">CSCwh31485</a>	Member interface config not applied with mis-match in packages.conf files.
<a href="#">CSCwh72437</a>	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
<a href="#">CSCwi00680</a>	Router unexpectedly reloads while using DHCP for ISG.
<a href="#">CSCwh96823</a>	IOS-XE router not installing classless-static-routes from DHCP option 121.
<a href="#">CSCwh77706</a>	SVL, 10G link on the active chassis will go down after reload.
<a href="#">CSCwh02592</a>	Device sync fails when device prompt comes along with device banner and TACACS is used.
<a href="#">CSCwh84850</a>	Unexpected reboot in device due to SISF and STP initialization.
<a href="#">CSCwh64903</a>	Crash on device polling SPA sensor data.
<a href="#">CSCwh53432</a>	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
<a href="#">CSCwh21796</a>	Password getting visible for the mask-secret in show logging.
<a href="#">CSCwh50104</a>	Upgrade failing with config check track-id-name.
<a href="#">CSCwf59929</a>	CTS CORE process crash after configuring role based ACL.
<a href="#">CSCwh81471</a>	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
<a href="#">CSCwh93772</a>	Option 121 never requested by IOS-XE client.
<a href="#">CSCwh06087</a>	[IPv6 BGP] multiple sourced paths present for the same prefix.
<a href="#">CSCwh29120</a>	IP SPD queue thresholds are out of range.
<a href="#">CSCwh14953</a>	CBQoS polling for the object cbQosCMPPostPolicyBitRate returns incorrect value.
<a href="#">CSCwh89096</a>	Device unexpected reload.
<a href="#">CSCwh99597</a>	After migration MAC/IP only MAC is advertised.
<a href="#">CSCwh75992</a>	"BGP Router" process crash.
<a href="#">CSCwh48058</a>	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.
<a href="#">CSCwh76920</a>	Memory leak in linux_iosd-imag due to SNMP.
<a href="#">CSCwh75112</a>	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.

### Resolved Bugs in Cisco IOS XE 17.12.1a

Identifier	Headline
<a href="#">CSCwe82666</a>	Not all HSL entries get pushed to device if more than 1 HSL entries are configured.

Identifier	Headline
<a href="#">CSCwe31226</a>	Issues/discrepancies around CPU alarms generated and sent to device.
<a href="#">CSCwe98345</a>	FHRP stay in active/active state after physical interface flap.
<a href="#">CSCwe43341</a>	TLS control-connections down, traffic from controller dropped with SDWAN Implicit ACL Drop.
<a href="#">CSCwe18124</a>	MACsec remains marked as secured, but randomly the traffic stops working.
<a href="#">CSCwe18276</a>	Route-map not getting effect when its applied in OMP for BGP routes.
<a href="#">CSCwb74821</a>	Unexpected behavior due to unstable power source.
<a href="#">CSCwe81182</a>	(EPC, packet-trace) for IPsec running COFF (Crypto Offload).
<a href="#">CSCwe63222</a>	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated.
<a href="#">CSCwe93905</a>	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
<a href="#">CSCwe90501</a>	Router upgrade fails due to <b>advertise aggregate</b> with VRF.
<a href="#">CSCwe85195</a>	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwe88689</a>	ROMMON for auto-upgrade.
<a href="#">CSCwd53710</a>	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec.
<a href="#">CSCwe66318</a>	NAT entries expire on Standby Router.
<a href="#">CSCwd84599</a>	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
<a href="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwe70374</a>	Platform punt-policer is not configurable.
<a href="#">CSCwe73408</a>	For some error condition platform_properties may double free.
<a href="#">CSCwd42523</a>	Same label is assigned to different VRFs.
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwe12194</a>	Auto-Update Cycle incorrectly deletes certificates.
<a href="#">CSCwe57239</a>	All usb internal communication is closed when using <b>platform usb disable</b> command.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
<a href="#">CSCwe85421</a>	Device BFD Session Down with interface flap.

Identifier	Headline
<a href="#">CSCwe95606</a>	Double GR_Additional log enablement defect.
<a href="#">CSCwe31471</a>	Segmentation fault in PB rx when per-tunnel qos config withdraw.
<a href="#">CSCwe89404</a>	No way audio when using secure Hardware conference with secure endpoints.
<a href="#">CSCwd39257</a>	IOS-XE cpp crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwe70642</a>	AAR overlay actions are applied to DIA traffic.
<a href="#">CSCwa96399</a>	Configuring <b>entity-information</b> xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwe79007</a>	Device unexpected reload when doing ips test with UTD IPS engine.
<a href="#">CSCwe31281</a>	Autotunnel Isec tracker: Tracker does not come up at all on vedge.
<a href="#">CSCwd93401</a>	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
<a href="#">CSCwf65696</a>	Non-fabric- Load the minimal bootstrap configs again if device rebooted without saving the configs.
<a href="#">CSCwd76648</a>	Port-channel DPI Load-Balancing not utilizing all the member-links.
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device.
<a href="#">CSCwb39206</a>	Enable VFR CLI.
<a href="#">CSCwe85022</a>	Telstra Cert: FN980 modem (P-5GS6-GL) is showing 4 additional NR bands support - 1, 3, 7, and 28.

### Open Bugs in Cisco IOS XE 17.12.1a

Identifier	Headline
<a href="#">CSCwf70854</a>	Changes to speed on the interface via CLI/GUI dont go through unless first done via shell access.
<a href="#">CSCwh67812</a>	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed.
<a href="#">CSCwf72079</a>	Router unexpectedly reloads due to 'LocalSoft'.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating TP generates an invalid TP.
<a href="#">CSCwh06870</a>	APN password in plain text when Cellular controller profile is configured.
<a href="#">CSCwf87292</a>	Punt keep alive failure crash on controller managed device apparently due to data packets.
<a href="#">CSCwf83850</a>	With Pure IPV6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in wan int G1.

Identifier	Headline
<a href="#">CSCwf94294</a>	Misprograming during vpn-list change under data policy.
<a href="#">CSCwa57254</a>	Router Silent Reload due to CpuCatastrophicError.
<a href="#">CSCwf55145</a>	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
<a href="#">CSCwf94052</a>	BFD going down for newly onboarded device.
<a href="#">CSCwh01095</a>	Rapid memory leak on ngiolite process.
<a href="#">CSCwf61720</a>	No licenses in use after upgrading from Traditional to Smart licensing IOS-XE versions.
<a href="#">CSCwf80927</a>	Speed tests to internet from device triggered will fail sometimes.
<a href="#">CSCwf84522</a>	Unexpected reboot due QFP UCode due to IPSec functions.
<a href="#">CSCwh00320</a>	<b>Show run</b> and other show commands not in sync after removing GigabitEthernet3.
<a href="#">CSCwf44703</a>	NAT64 prefix is not originated into OMP.
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running <b>show crypto</b> commands.
<a href="#">CSCwf77252</a>	SIP calls not working on device with ZBFW enabled.
<a href="#">CSCwf96416</a>	Could not access any device show commands at all.
<a href="#">CSCwf67564</a>	RP3 observes Memory Leak at process SSS Manager.
<a href="#">CSCwf34171</a>	<b>Configure replace</b> command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
<a href="#">CSCwh01425</a>	ITU channel configuration seems not working on router.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot on device.
<a href="#">CSCwf69062</a>	SDRA-SSLVPN : The SSLVPN session closes with re-authentication error after some interval of time.
<a href="#">CSCwf79264</a>	Traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped.
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload.
<a href="#">CSCwf45486</a>	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop.
<a href="#">CSCwh01313</a>	Unexpected reboot due qfp Ucode due to IPsec functions.
<a href="#">CSCwf95527</a>	BFD Entries Removed.
<a href="#">CSCwe26895</a>	Router has Local Soft ADR crash, writes flat core, and reloads.
<a href="#">CSCwh01318</a>	Multiple Crashes observed on device platform due to Memory Exhaustion.

Identifier	Headline
<a href="#">CSCwf71116</a>	Static route keep advertising via OMP even though there is no route.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config.
<a href="#">CSCwh00332</a>	B2B NAT: when configuration ip nat inside/outside on VASI interface,ack/seq number abnormal.
<a href="#">CSCwf49390</a>	Device crashes with crypto map unlock map head.
<a href="#">CSCwf78735</a>	Device uses the NIM-1T/4T card for interconnection, and NAT with GRE over IPsec cannot be applied.
<a href="#">CSCwf84960</a>	C-NIM-2T: LED L remains green after port shutdown.

## 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 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.

### Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The 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.