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: 2023-10-16

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 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 http://www.cisco.com/go/cfn.

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

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms IOS XE Dublin 17.12.1a

Feature	Description
IPv6 Unicast Support with DLEP	The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	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.
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: • Cisco Catalyst 8300 Series Edge Platforms

Feature	Description
Segment Routing over IPv6 Dataplane	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: • Interior Gateway Protocol (IS-IS only) • Border Gateway Protocol (BGP) In addition, the following functionalities are available for Segment Routing over IPv6 dataplane: • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)
Support for Automatic Log Deletion	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 logging purge-log buffer days command.
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: • Security Group Tag (SGT) or Destination Group Tag (DGT) Policies • Unidirectional IPv4 SGT Exchange Protocol (SXP) connections • Bidirectional IPv4 SXP connections • IPv4 SGT Bindings • IPv6 SGT Binding • Security Group Access Control Entries (SG ACEs)

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
Catalyst 8300 Series Edge Platforms			
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)
Catalyst 8200 Series Edge Platforms			
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 17.12.1a

Identifier	Headline
CSCwe82666	Not all HSL entries get pushed to device if more than 1 HSL entries are configured.
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to device.
CSCwe98345	FHRP stay in active/active state after physical interface flap.
CSCwe43341	TLS control-connections down, traffic from controller dropped with SDWAN Implicit ACL Drop.
CSCwe18124	MACsec remains marked as secured, but randomly the traffic stops working.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwb74821	Unexpected behavior due to unstable power source.
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload).
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe90501	Router upgrade fails due to **advertise aggregate** with VRF.
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe88689	ROMMON for auto-upgrade.

Identifier	Headline
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec.
CSCwe66318	NAT entries expire on Standby Router.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Platform punt-policer is not configurable.
CSCwe73408	For some error condition platform_properties may double free.
CSCwd42523	Same label is assigned to different VRFs.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates.
CSCwe57239	All usb internal communcation is closed when using **platform usb disable** command.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwe85421	Device BFD Session Down with interface flap.
CSCwe95606	Double GR_Additional log enablement defect.
CSCwe31471	Segmentation fault in PB rx when per-tunnel qos config withdraw.
CSCwe89404	No way audio when using secure Hardware conference with secure endpoints.
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwe70642	AAR overlay actions are applied to DIA traffic.
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.
CSCwe79007	Device unexpected reload when doing ips test with UTD IPS engine.
CSCwe31281	Autotunnel Ipsec tracker: Tracker does not come up at all on vedge.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
CSCwf65696	Non-fabric- Load the minimal bootstrap configs again if device rebooted without saving the configs.
CSCwd76648	Port-channel DPI Load-Balancing not utilizing all the member-links.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCwb39206	Enable VFR CLI.

Identifier	Headline
CSCwe85022	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
CSCwf70854	Changes to speed on the interface via CLI/GUI dont go through unless first done via shell access.
CSCwh67812	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed.
CSCwf72079	Router unexpectedly reloads due to 'LocalSoft'.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwh06870	APN password in plain text when Cellular controller profile is configured.
CSCwf87292	Punt keep alive failure crash on controller managed device apparently due to data packets.
CSCwf83850	With Pure IPV6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in wan int G1.
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwa57254	Router Silent Reload due to CpuCatastrophicError.
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCwf94052	BFD going down for newly onboarded device.
CSCwh01095	Rapid memory leak on ngiolite process.
CSCwf61720	No licenses in use after upgrading from Traditional to Smart licensing IOS-XE versions.
CSCwf80927	Speed tests to internet from device triggered will fail sometimes.
CSCwf84522	Unexpected reboot due QFP UCode due to IPSec functions.
CSCwh00320	**Show run** and other show commands not in sync after removing GigabitEthernet3.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwf77252	SIP calls not working on device with ZBFW enabled.
CSCwf96416	Could not access any device show commands at all.
CSCwf67564	RP3 observes Memory Leak at process SSS Manager.

Identifier	Headline
CSCwf34171	**Configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh01425	ITU channel configuration seems not working on router.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device.
CSCwf69062	SDRA-SSLVPN : The SSLVPN session closes with re-authentication error after some interval of time.
CSCwf79264	Traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf45486	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop.
CSCwh01313	Unexpected reboot due qfp Ucode due to IPsec functions.
CSCwf95527	BFD Entries Removed.
CSCwe26895	Router has Local Soft ADR crash, writes flat core, and reloads.
CSCwh01318	Multiple Crashes observed on device platform due to Memory Exhaustion.
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface,ack/seq number abnormal.
CSCwf49390	Device crashes with crypto map unlock map head.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT with GRE over IPsec cannot be applied.
CSCwf84960	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.