

Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Dublin 17.12.x

First Published: 2023-08-22

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 Cisco Catalyst 8500 Series Edge Platforms



Note Cisco IOS XE Dublin 17.12.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Dublin 17.12.x release series.

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

The Cisco Catalyst 8500 Series Edge Platforms includes the following models:

- C8500-12X4QC
- C8500-12X
- C8500L-8S4X
- C8500-20X6C

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, see the [Cisco 8500 Series Catalyst Edge Platform datasheet](#).

Sections in this documentation apply to all models of unless a reference to a specific model is explicitly made.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the features, platform, and software image support on Cisco Catalyst 8500 Series Edge Platforms. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on cisco.com is not required.

New and Changed Software Features

Table 1: Software Features

Feature	Description
Segment Routing over IPv6 Dataplane	<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"> • Interior Gateway Protocol (IS-IS only)- • Border Gateway Protocol (BGP) <p>In addition, the following functionalities are available for Segment Routing over IPv6 dataplane:</p> <ul style="list-style-type: none"> • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)
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"> • 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 Bindings • Security Group Access Control Entries (SG ACEs)
IPv6 Unicast Support with DLEP	<p>The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.</p>
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	<p>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.</p>

Feature	Description
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: <ul style="list-style-type: none"> • Cisco 1000 Series Integrated Services Routers • Cisco Catalyst 8500 Series Edge Platforms
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.

Resolved and Open Bugs for Cisco IOS XE 17.12.x

Resolved Bugs for Cisco IOS XE 17.12.1a

Bug ID	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
CSCwe43341	TLS control-connections down, traffic from device dropped
CSCwe18124	MACsec remains marked as secured, but the traffic randomly stops working
CSCwe18276	Route-map not getting effected when its applied in OMP for BGP routes
CSCwf83850	With Pure IPv6, minimal bootstrap unable to onboard non-fabric - IPv6 config missing in WAN int G1
CSCwb74821	Unexpected behavior due to unstable power source
CSCwe79007	Unexpected reload when doing ips test with UTD ips engine
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload)
CSCwe38296	Procyon packets drop due to MACsec post-encryption padding behavior
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail
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
CSCwd53710	Crash seen when name_lookup takes > 30 sec
CSCwe66318	NAT entries expire on standby router
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console , tel interface. until router reload
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP

Bug ID	Headline
CSCwe70374	Platform punt-policer is not configurable
CSCwf05405	Traceback seen after BDI interface is configured
CSCwe73408	For some error condition platform_properties may double free
CSCwd42523	Same label is assigned to different VRFs
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups
CSCwe12194	Auto-Update cycle incorrectly deletes certificates
CSCwd90056	C8500-12X4QC : P2MP WAN MACsec does not allow traffic to pass on the link
CSCwe09298	C8500L sees the increase of input errors without any other specific errors increasing under show interface
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
CSCwe85421	BFD session down with interface flap
CSCwe95606	Double GR_Additional log enablement defect
CSCwe31471	Segmentation fault in device 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
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated
CSCwe70642	AAR overlay actions are applied to DIA traffic
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data
CSCwe06518	C8500-12X : ~23% degradation in IPSEC IPv6 profile for 1400B
CSCwe31281	Autotunnel Isec tracker:Tracker does not come up at all on device
CSCwe39157	During soak run, On C8500L-8S4X, Memif channel's were missing and causing SC-SN state down
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 device is not received by remote peer device
CSCwb39206	Enable VFR CLI
CSCwe85022	Device is showing 4 additional NR bands support - 1, 3, 7, and 28

Open Bugs for Cisco IOS XE 17.12.1a

Bug ID	Headline
CSCwf70854	Changes to speed on the interface via CLI/GUI dont go through unless first done via shell access.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP
CSCwf87292	Punt keep alive failure crash on controller managed device apparently due to data packets
CSCwf94294	Misprograming during vpn-list change under data policy.
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
CSCwf80927	Speed tests to internet from C8500 device triggered will fail sometimes
CSCwf84522	C8500L Unexpected rebooted while classifying packet with CTF (Common Flow Table)
CSCwh00320	Show commands 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
CSCwf62757	C8500L Interface data report interval issue for physical interface
CSCwf96416	Couldn't access any show commands at all.
CSCwf67564	Device observes memory leak at process SSS Manager
CSCwf34171	Configure replace command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices
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	In device 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 LocalSoftADR 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

Bug ID	Headline
CSCwh00332	B2B NAT: when configuration ip nat inside/outside on VASI interface,ack/seq number abnormal

ROMmon Release Requirements

Use the following tables to determine the ROMmon version required for your Catalyst 8500 model:

Table 2: Minimum and Recommended ROMmon Releases

	DRAM	Minimum Rommon	Recommended Rommon
C8500-12X4QC & C8500-12X	16GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	All variants	17.10(1r)	17.10(1r)
C8500L-8S4X	-	17.8(2r) - available from Cisco IOS XE 17.9.1a release	-
	-	17.10(1r)- available from Cisco IOS XE 17.10.1a release	-



Note In case of C8500L-8S4X platform, the ROMmon image is bundled with the Cisco IOS XE software image which ensures that when the device is booted up, the ROMmon image is also automatically upgraded to the recommended version.

Table 3: ROMmon Release per Platform

C8500-12X4QC & C8500-12X	17.2(1r)
	17.3(1r)
	17.11(1r)
C8500-20X6C	17.10(1r)
C8500L-8S4X	17.8(2r)
	17.10(1r)

Table 4: What's New in the ROMmon Release

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.3(1r)	Supports 64GB DRAM for C8500-12X4QC & C8500-12X
17.10 (1r)	Added support for new platform C8500-20X6C
17.11(1r)	Fixed a issue in data wipe feature
ROMmon Release for C8500L-8S4X	Fixes
17.10(1r)	CSCwa41877 - Fixes for Intel 2021.2 IPU CSCwb67177 - Fixes for Intel 2022.1 IPU CSCwb60723 - Fixes for CPU temperature CSCwb60863 - Fixes for TAM_LIB_ERR_WRITE_FAILURE error

Related Documentation

- [Hardware Installation Guide for Catalyst 8500 Series Edge Platforms](#)
- [Hardware Installation Guide for Catalyst 8500L Series Edge Platforms](#)
- [Smart Licensing Guide for Access and Edge Platforms](#)
- [Software Configuration Guide for Catalyst 8500 Series Edge Platforms](#)

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at <https://www.cisco.com/en/US/support/index.html>.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

