Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE 17.15.x

First Published: 2024-08-27

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 17.15.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.15.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 unless a reference to a specific model is explicitly made.

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.

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 https://cfnng.cisco.com/ An account on cisco.com is not required.

New and Changed Software Features in Cisco IOS XE 17.15.1a

Table 1: Software Features

Feature	Description
Enhanced NAT Management	From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the ip nat translation max-entries cpu command. This feature also enables streamlining NAT synchronization in redundant systems using the ip nat settings redundancy optimized-data-sync command.
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.15.1a, Segment Routing over IPv6 dataplane supports these functionalities: • IS-IS Microloop Avoidance • IS-IS Loop-Free Alternate Fast Reroute • IS-IS Topology-Independent Loop-Free Alternate Fast Reroute • OAM Traffic Engineering
Enhancement to SGACL Logging	This feature enhances the Security Group-based Access Control List (SGACL) logging capability by using High Speed Logging (HSL) for Cisco IOS XE devices. SGACL logging through HSL provides an efficient and reliable logging method for security events in network environments with high-traffic volumes.
Absolute Path for HTTP or HTTPS File Transfer	The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the copy command. From Cisco IOS XE 17.15.1a, you must provide the absolute file path when you execute the copy command, to transfer the file.
Network-Wide Path Insights on Software Defined (SD) - Routing Devices	Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network.
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.

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.
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.
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.
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.

Resolved and Open Bugs for Cisco IOS XE 17.15.1a

Resolved Bugs for Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwj51700	CPP crashes after reconfiguring **ip nat settings pap limit** feature in high QFP state
CSCwk42634	A critical process vip_confd_startup_sh has failed

Identifier	Headline
CSCwj53456	Crash triggered by **crypto ikev2 cluster detail** Command
CSCwk26247	C8500L QFP stuck threads crash while handling netflow features under autonomous mode
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	No data to display for device
CSCwk39131	Device crashed when issuing **show sdwan ftm next-hop chain all**
CSCwk22225	FTMd crashes after receiving credentials
CSCwj48909	Coredump observed in tracker module while running cxp_sig_auto_tunnel suite
CSCwk23723	Mean queue calculation is incorrect on hierarchical QoS
CSCwk45165	Memory leak on device
CSCwj76501	Data plane crash in ERSPAN processing
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN Hub & Spoke setup
CSCwi56641	Device reports link-flap error when peer reloads
CSCwk20583	40G interfaces with breakout configurations flap after reload
CSCwj90614	High CPU utilisation for confd_cli
CSCwi81026	BFD sessions flapping during IPSec rekey in scaled environment
CSCwk39268	Failing to renew
CSCwj76662	High memory utilization due to ftmd process
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk44078	GETVPN Migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwk22942	Unable to build two IPSec SAs with same source destination where one peer is PAT through the other
CSCwj96092	ICMP tracker type (from echo to timestamp) change causes tracker to fail
CSCwj99827	Device unexpectedly reloads due to a crash

Identifier	Headline
CSCwi99454	FNF test tunnel name change failed due to session of pm5 was not alive
CSCwj02401	Device reloaded when generating admin tech while processing very high number of flows
CSCwj40223	appRouteStatisticsTable sequence misordered or OS returns wrong order
CSCwk19725	Add FNF cache limit
CSCwk22312	Input errors and overrun on port channel interface and physical interface
CSCwj86794	Device crashes while processing an NWPI trace
CSCwk42253	Unexpected reboot when a HTTP connection fails with 404
CSCwj67591	Activate effective only after second re-try with new uuid
CSCwj32347	DIA Endpoint tracker not working with ECMP routes

Open Bugs for Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwk75733	Custom applications may not be programmed properly
CSCwk89256	Speed mismatch in IOS-XE configuration after device template push for ISR
CSCwk85704	add-on CLI push failed
CSCwm07396	Few BFD sessions down after clear mka session on client
CSCwk95308	CRC errors increment on down interface of device
CSCwk98006	Unable to Establish NAT Translations with ZBFW enabled
CSCwk86355	File transfer fails - lost connection
CSCwk49806	Device rebooted unexpectedly due to process NHRP crash
CSCwk81360	Device reboots unexpectedly while configuring NAT Static translation
CSCwk62954	Multiple configs 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
CSCwk25731	Device flaps more than once when interface is bounced with SRBD optics
CSCwk54544	TCAM misprogramming after rules are reordered on device

Identifier	Headline
CSCwk89523	IOSd crash during function to add/delete a MAC address from the MAC accounting table
CSCwk74298	Device denied for template push and some show commands with error application communication failure
CSCwk98578	GETVPN ipv6 crypto map not shown in interface configuration
CSCwk70630	Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to tunnels
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 reboots due to QFP CPP
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured
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
CSCwm08545	Centralized policy policer worked per PC on the same site not per site/vpn-list
CSCwk34187	Application Dicom under family Middleware not displayed in DPI flows
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

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	-	17.10(1r) -	17.14(1r)

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: 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
17.14(1r)	CSCwf98337 - Evaluation of C8500L-8S4X for Intel 2023.3 IPU and SMRAM vulnerabilities CSCwe21026 - Evaluation of C8500L-8S4X for Intel 2023.1 IPU and SMM vulnerabilities

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.

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms

- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing 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 DevNet.
- 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.

© 2023 Cisco Systems, Inc. All rights reserved.