Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE 17.16.x

First Published: 2024-12-24

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 17.16.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.16.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 17.16.1a

Table 1: Software Features

Feature	Description
Configure Source Interface for High Speed Logging	From Cisco IOS XE 17.16.1a, you can configure source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager. You can also enable HSL for your firewall messages, to allow a firewall to log records with minimum impact to packet processing.
Disablement of Weak SSH Algorithms	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
UTD Container Management for SD-Routing Devices	When Cisco IOS-XE autonomous devices transition to Cisco SD-Routing mode, the Unified Threat Defense (UTD) Container Migration feature ensures that existing container functionalities are preserved. From Cisco IOS XE 17.16.1a you can detect, upgrade, and manage UTD Security Virtual Images through Cisco Catalyst SD-WAN Manager. For devices without pre-existing containers, you can also install and manage UTD images using policy groups.
Speed Test Enhancement for SD-Routing Devices	From Cisco IOS XE 17.16.1a, Cisco Catalyst SD-WAN Manager enables site-to-site speed tests to measure bandwidth between devices over DMVPN tunnels. These tests check upload speed from the source device to the destination, and measure download speed from destination to the source device.
Monitoring Crypto VPN Solutions on SD-Routing Devices	If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts and events.Having high visibility into the network can help identify errors in real time therefore reducing the network down time.
Monitoring Application Performance on SD-Routing Devices	In Cisco IOS XE 17.16.1a, you can now monitor TCP and RTP traffic on DMVPN tunnels for IKEv2 traffic using Application Response Time (ART) monitor and Media monitor respectively. This functionality is only supported on DMVPN tunnels with IKEv2 encryption.
Enhanced support for binary tracing	From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the **show logging process IOS module nhrp** command, without enabling DMVPN event tracing.

Feature	Description
Support for Enrolment over Secure Transport	From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the **enrollment http username** command.
Enhancement to the show cellular 0/x/0 connection command	From Cisco IOS XE 17.16.1a, the output for the **show cellular 0/x/0 connection** command includes Access Point Name (APN), and Cellular Link Uptime parameters.
Asymmetric carrier delay	From Cisco IOS XE 17.16.1a, asymmetric carrier delay is supported on Cisco Catalyst 8500 Series Edge Platforms.
Enhancements to the show power command	From Cisco IOS XE 17.16.1a, two new keywords **detail** and **history**) are introduced for the **show power** command. The **detail** keyword provides power usage information for each component, and the **history** keyword provides the power consumption history for the device.
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.16.1a, Segment Routing over IPv6 dataplane supports these functionalities:- • eBGP Inter-AS • PCE-Delegated Path Computation • Enhancements to OAM Traffic Engineering
Onboard Cisco ThousandEyes Enterprise Agent on SD-Routing Devices	From Cisco IOS XE 17.16.1a, you can configure Cisco ThousandEyes Enterprise agent on SD-Routing devices to gather granular details of network and application performance. This facilitates end-to-end traffic visibility, supporting optimization and troubleshooting.

Resolved and Open Bugs for Cisco IOS XE 17.16.1a

Resolved Bugs for Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwm74060	IOSD chasfs task crashes when retrieving platform info
CSCwn15231	Null-way audio within the same layer2
CSCwm56800	FIA trace packet decode displays incorrect value for fragmentation offset
CSCwk78018	Yang model does not handle properly default ikev2 authorisation policy

Identifier	Headline
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down
CSCwm48459	Software crash with critical process vip_confd_startup_sh fault on rp_0_0 (rc=6)
CSCwm89225	CPP crashes After routing table changes
CSCwk05354	Interface flap with auto-neg CLI
CSCwk62954	Multiple match address local interface not pushed from vmanage under crypto profile
CSCwm70520	Device tracebacks generation
CSCwj33723	Config not synced between active and third member of stack
CSCwk79606	PKI trustpoint password command only allows encryption type 0 and 7 on all IOS XE platforms
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration
CSCwn29062	Traceback log output on device with data corruption error logs
CSCwm62981	Device crashes with PKI revocation-check ocsp none enabled
CSCwm74317	'%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI
CSCwm54978	Selinux: polaris_iosd_t denials
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call

Open Bugs for Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwn32668	L2 traffic go to blackhole due to mac-route originated from blocked node after power-cycle
CSCwk56961	Device critical alarm LED always on
CSCwn09185	Traffic loss observed on minimal values with time based policy-map
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IPFragErr on IP VFR and MPLS enabled tunnel interface
CSCwn12594	SIG zscaler ipsec - vpn credentials for primary tunnel not created
CSCwm71639	Crash noticed when configured service-policy to a dialer interface

Identifier	Headline
CSCwn24226	GETVPN mismatch in GMs reported across COOP
CSCwn40906	Router crash observed when optimizing encrypted traffic with DRE
CSCwm81246	MACsec interfaces lock up on TX direction after reload
CSCwn34457	Post power cycle, unable to login to router due to error authentication failed
CSCwn19586	Certificate-based MACsec flapping when dot1x reauth timers are set and after reload
CSCwm87270	MKA session down with ICV Verification of a MKPDU failed for error on one of the interface
CSCwn39447	Speed test might work abnormally after changing system-ip
CSCwn35476	Source interface for sub-interface does not get pushed to device
CSCwn24036	Optical power values diffrent for **show int** and **show hw-module**
CSCwo39530	Applied changes in the filter of pcap fileds are not reflecting after refreshing.

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)	17.15(1r) **Important** Downgrading to a ROMmon version lower than 17.15(1r) is not supported.
C8500L-8S4X	-	17.10(1r) -	17.14(1r)* **Important** This version of ROMmon is only available with Cisco IOS XE 17.15.1a onwards

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

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

ROMmon Release for C8500-20X6C	Fixes
17.15(1r)	CSCwf98335 Evaluation of all_routing_iosxe for Intel 2023.3 IPU and SMRAM vulnerabilities. CSCwd96405 ASR 1000 BL and ML hashes not seen in the "Show system intergrity" CLI for Aikido based platformsAdditional minor fixes.

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 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 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.