Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE 17.13.x

First Published: 2023-12-16

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 Cisco Catalyst 8500 Series Edge Platforms



Note Cisco IOS XE 17.13.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.13.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 17.13.1a



Note Cisco SD-Routing enables a traditional router operating in Autonomous mode to be fully managed by Cisco Catalyst SD-WAN Manager. This functionality is not currently supported on C8500L-8S4X.

Table 1: Software Features

Feature	Description
Support for Persistence of BGP Dynamic Neighbors	From IOS XE 17.13.1a, the device maintains the neighbor information even after the session is terminated. To configure this, use the **bgp listen persistent** command for all dynamic neighbors and **bgp listen range peer-group persistent** command for specific neighbors.
Enhancements to BGP Maximum Prefix	• **Discard Extra Prefixes:** This enhancement introduces the **neighbor maximum prefix discard extra** command to drop all excess prefixes received from the neighbor when the configured value of the prefixes exceed the maximum limit. • **Logging Enhancement:** The logging system is enhanced to support a per neighbor logging every 60 seconds.
View Packet Drops History	From Cisco IOS XE 17.13.1a, you can use the **show drops history qfp** command to view the history of the QFP drops on the Catalyst 8500 Series Edge Platforms.
IPv6 Load Balancing Support for IKEv2 Cluster	This feature introduces load balancing support for IKEv2 cluster in an IPv6 topology
Using VASI in NTPv6 Environment	You can use the VRF-Aware Software Infrastructure Scale feature in the NTPv6 environment to support inter-VRF communication. This inter-VRF communication can include access control lists (ACLs), Network Address Translation (NAT), policing, and zone-based firewalls for MPLS traffic or IPv4 and IPv6 traffic flowing across two different VRF instances. The VASI interfaces support redundancy of the Route Processor (RP) and Forwarding Processor (FP).
Initiating GARP for NAT Mapping	This feature introduces support for configuring retry time intervals for GARP messages on the BD-VIF interface. You can configure this feature using the **ip arp nat-garp- retry** and **ip nat inside source static** commands.

Feature	Description

Support for Suite B ciphers with GET VPN	This enhancement introduces support for Suite B ciphers with GET VPN on the following router models:
	• Cisco ASR 1000 Series Aggregation Services Routers
	  • ASR1009-X + ESP200-X
	• Cisco Catalyst 8000V Edge Software
	• Cisco Catalyst 8200 Series Edge Platforms
	  • C8200-1N-4T
	• Cisco Catalyst 8300 Series Edge Platforms
	  • C8300-2N2S-4T2X
	  • C8300-1N1S-6T
	• Cisco Catalyst 8500 Series Edge Platforms
	  • C8500-12X
	  • C8500-20X6C

Strength Enforcement for IKE Security Association (SA)	This feature ensures that the strength of the IKE (IKEv1 and IKEv2) SA encryption cipher is greater than or equal to the strength of its child IPsec SA encryption cipher. To enable this feature, use the **crypto ipsec ike sa-strength-enforcement command.**
Cisco SD-Routing Cloud OnRamp for Multicloud	Cisco SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-Routing devices. With these capabilities, the devices can access the applications hosted in the cloud.
Schedule Software Upgrade on SD-Routing Devices	With this feature, you can schedule software image upgrade on Cisco SD-Routing devices. This allows you to avoid any downtime due to the software upgrade process.
SD-Routing Configuration Group	The SD-Routing Configuration Group feature provides a simple, reusable, and structured method to configure the SD-Routing device using Cisco Catalyst SD-WAN Manager.

Feature	Description
Support for Flexible NetFlow Application Visibility on SD-Routing Devices	The Flexible NetFlow (FNF) feature provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Also, it provides visibility for all the traffic that passes through the VPN0 on Cisco SD-Routing devices by using the SD-Routing Application Intelligence Engine (SAIE).
Speed Test for SD-Routing Devices	Cisco SD-WAN Manager allows you to measure the network speed and available bandwidth between a device and an iPerf3 server. The speed tests measure upload speed from the source device to the selected or specified iPerf3 server, and measure download speed from the iPerf3 server to the source device.
Application Performance Monitor	The Application Performance Monitor feature introduces a simplified framework that enables you to configure intent-based performance monitors. With this framework, you can view real-time, end-to-end application performance filtered by client segments, network segments, and server segments.
Support for Packet Capture for SD-Routing	This feature allows you to configure options to capture the bidirectional IPv6 traffic data to troubleshoot connectivity on the SD-Routing devices.
Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.13.1a, Segment Routing is supported over the IPv6 dataplane for Border Gateway Protocol (BGP) on L3VPN networks using On-Demand Next Hop (ODN).
Support for Security-Enhanced Linux	SELinux (Security-Enhanced Linux) is a solution designed to incorporate a strong, flexible mandatory access control (MAC) architecture into Cisco IOS XE platforms. From Cisco IOS XE 17.13.1a, SELinux is enabled by default in Enforcing mode for Cisco IOS XE platforms..

Resolved and Open Bugs for Cisco IOS XE 17.13.1a

Resolved Bugs for Cisco IOS XE 17.13.1a

Identifier	Headline
CSCwh10813	Add verbose log to indicate grant ra-auto unconfigures grant auto in PKI server
CSCwf25735	QoS more than four remark with set-cos not work
CSCwf44703	NAT64 prefix is not originated into OMP

Identifier	Headline
CSCwf80400	Device may experience unexpected reset while executing **show utd engine standard statistics**
CSCwf14607	Crash observed exporting PKCS12 to terminal via SSH CLI
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path Installation on chosen next-hop

Open Bugs for Cisco IOS XE 17.13.1a

Identifier	Headline
CSCwh94906	Segmentation fault crash with Network Mobility Services Protocol (nmsp)
CSCwi03502	Create CLI to push required when configuring multi-PDN
CSCwh84068	Device crash after changing NAT HSL configuration.
CSCwi16716	Device crashed upon increasing the gatekeeper cache size
CSCwh77221	SNMP unable to poll tunnel data after a minute
CSCwi15930	Device failing to upgrade due to CDB issue
CSCwi08171	Device may crash due to crypto IKMP process
CSCwh76453	Tracker for TLOC extension is down even though TLOC is up and there is ICMP reachability
CSCwi14178	Failed to connect to device : Connection failed
CSCwh01678	FTM crash with SIG enabled
CSCwi07137	Crash when traffic is sent to UTD
CSCwi06843	Endpoint tracker triggers a CPU Hog
CSCwi16452	Error thrown when switching from SSE to SIG
CSCwi11807	snmpbulkget breaks the OID after minute not returning the correct order
CSCwi00369	Device lost security parameter after upgrade
CSCwi06404	PKI related crash after failing a CRL Fetch
CSCwi13563	IP SLA probe for end-point-tracker doesnt work once endpoint tracker is changed until reload
CSCwh65016	Unexpected reboots on device due to QFP Exception
CSCwi05395	snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs

Identifier	Headline
CSCwi15688	Unexpected NAT translation occurs in a specific network
CSCwh91136	Traffic not encrypted and droped over IPSEC SVTI tunnel
CSCwi23562	When RADIUS is down, and there is an IKE-AUTH request received, the device stops replying to DPD packets.
CSCwh72869	cpp_mcplo_ucode crash with port-channel and NAT
CSCwi16015	SSE tunnels don't come up with Dialer interface. Relax check in IKE
CSCwi19875	Device is unable to process hidden characters in a file while trying to use bootstrap method
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many ipsec interfaces
CSCwi31833	UTD deployment failing if deployed from remote server hostname rather than ip
CSCwh52440	IP SLA doesnt have checks for ICMP probes to be sent on source interface.
CSCwj30529	AAA:Template push fail when aaa authorization is set to local .
CSCwh73573	**show ppp al** display PPP-Server IP though no IP configured on BRAS/PPP-Server .

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)* **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
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

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.