Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE 17.14.x

First Published: 2024-04-29

Full Cisco Trademarks with Software License

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.

About Cisco Catalyst 8500 Series Edge Platforms

Note Cisco IOS XE 17.14.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.14.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 17.14.1a

Table 1: Software Features

Feature	Description
QFP Drops Threshold and Warning	From Cisco IOS XE 17.14.1a, this feature enables you to configure the warning threshold for each drop cause, and the total QFP drop in packets per second. If the configured threshold exceeds, then a rate-limited syslog warning is generated. You can configure the threshold using the platform qfp drops threshold command.
DC-PE Router in Cisco ACI to SR-MPLS Hand-off	From Cisco IOS XE 17.14.1a, Cisco ASR 1000 Series Aggregation Services Routers and Cisco Catalyst 8500 Series Edge Platforms can be used as intermediate DC-PE devices in Cisco ACI to SR-MPLS hand-off interconnection. SR-MPLS hand-off is an interconnection option that enables Cisco ACI to WAN interconnect using Segment Routing (SR) MPLS underlay.
IP Endpoint Delay Measurement and Liveness Monitoring	This feature enables you to measure the end-to-end delay and monitor liveness towards either a specified IPv4 or IPv6 endpoint. From Cisco IOS XE 17.14.1a, you can configure this feature using the **performance-measurement endpoint** and **performance-measurement delay-profile endpoint** commands.
Enhanced IS-IS Fast Flooding	The IS-IS Fast Flooding feature optimizes LSP transmission to accelerate network convergence by dynamically adjusting the LSP rate based on receiver capability. From Cisco IOS XE 17.14.1a, IS-IS Fast Flooding can be configured using the router isis lsp-fast-flooding command. The LSP transmission can be further customized with arguments such as **max-lsp-tx**, **psnp-interval**, and **per-interface** within the samerouter isis command, and enhanced by using the isis remote-psnp-delay command. This feature is disabled by default, and requires manual configuration to enable.

Feature	Description
Support for Suite B Ciphers with GET VPN	From Cisco IOS XE 17.14.1a, this enhancement introduces support for Suite B ciphers with GET VPN on the following platforms and its corresponding models: • Cisco ASR 1000 Series Aggregation Services Routers:- ASR 1000 with ESP100-X • Cisco Catalyst 8300 Series Edge Platforms:- C8300-1N1S-4T2X, C8300-2N2S-6T • Cisco Catalyst 8200 Series Edge Platforms:- C8200L-1N-4T • Cisco Catalyst 8500 Series Edge Platforms:- C8500-12X4QC, C8500L-8S4X • Cisco 1000 Series Integrated Services Routers: • C1131 • C112X • C116X • C111X
Increase in L2TPv3 Scalability	From Cisco IOS XE 17.14.1a, the capacity for unidimensional scalability of L2TPv3 tunnel is increased to 12,000 for the following platforms: • Cisco ASR 1000 Series Aggregation Services Routers using RP3 with ESP200-X and ESP100-X • Cisco Catalyst 8500 Series Edge Platforms The scalability is increased to 8000 for Cisco Catalyst 8500L-8S4X Platform.
Support to Configure VPN Solutions for SD-Routing devices	This release introduces support for the following VPN solutions: • FlexVPN • GETVPN • DMVPN • L3VPN These VPN solutions can be configured by using **Configuration** > **Configuration Groups** > **CLI Add-on Profile** option in Cisco SD-WAN Manager.

Feature	Description
YANG Configurational Model Support for SD-Routing Devices	This release introduces support for the following YANG Configurational Models: • BGP • MPLS • RSVP • SNMP • AAA • QOS • ACL • DHCP
Enhancement to the show reload-history Command	From Cisco IOS XE 17.14.1a, the **show reload-history** command is modified toshow reload history.The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.
View Unmodelled Commands on SD-Routing Devices	After an SD-Routing device is deployed, you can view the unmodelled commands on Cisco SD-WAN Manager. The list of unmodelled commands are regenerated if the device reboots.
Configure Secure Service Edge	Secure Service Edge is a cloud solution that provides seamless, transparent, and secure Direct Internet Access (DIA) to protect against internet-based threats. This solution can be configured through Policy Groups by using Cisco SD-WAN Manager.
Configuration Group Enhancements	This release introduces support for the following in Cisco SD-WAN Manager: • Transport Profiles • Management Profile • Service Profile • CLI Profile • Policy Object Profile

Feature	Description
Voltage and Current Metrics	Power Entry Module (PEM) sensors are critical components in the device that are responsible for monitoring various aspects of the power supply, such as voltage, current, and sometimes temperature, to ensure the device operates within safe and efficient parameters. From Cisco IOS XE 17.14.1a, you can use the show environment command to display the PEM sensor readings in mV (milli-volt) and mA (milli-ampere) for your devices..

Resolved and Open Bugs for Cisco IOS XE 17.14.1a

Resolved Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwh94906	segmentation fault crash with Network Mobility Services Protocol (nmsp)
CSCwi03502	Create CLI to push device required when configuring Multi-PDN
CSCwi49846	FTMD crashed when SIG GRE tunnels configs are removed
CSCwi55725	SDR CLI config group issue
CSCwi61369	Device may unexpectedly reload due to SIGABRT
CSCwi35716	AAR backup preferred color not working as expected
CSCwi76516	Device configuration template deployment fails
CSCwi53306	Unknown appID in ZBFW HSL log
CSCwf84567	Unexpected reload after re-connecting to the device
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : error : Connection failed
CSCwi82405	mGRE Tunnels with shared ipsec profile cause ucode crash
CSCwi40603	Memory leak in the Crypto IKMP process
CSCwf08658	Devices will flap the BFD sessions if we are in a non equilibrium state and have symmetric NAT
CSCwi35177	Device crash caused by continuous interface flap, interface associated to many ipsec interfaces
CSCwi60266	Device with enterprise certificates not forming control connections with controllers after upgrade
CSCwi67983	Log is missing when DNS Query fails.

Identifier	Headline
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a device reboot
CSCwb25507	Add vendor specific parameter for NBAR protocol pack version
CSCwi53549	Device crash with reason Critical process fman_fp_image fault on fp_0_0 (rc=134)
CSCwi82548	Crash in IKEv2 cluster load balancer
CSCwi51381	TrapOID is different from MIB file
CSCwh09033	Device unable to boot with C-NIM-8T module
CSCwj25493	Device crashed twice with Critical process linux_iosd_image fault on rp_0_0
CSCwi78365	Trim installed certificate on upgrade
CSCwi85293	IKEv2 IPv6 cluster load balance: Secondary in cluster unable to connect to cluster in case of FVRF
CSCwi86698	No error msg while using multicast address as system-ip on device.
CSCwi93784	FW upgrade does not work properly on P-LTE-MNA
CSCwj06622	Segmentation fault and core files are seen on IOS-XE due to speedtest
CSCwi16111	**ipv6 tcp adjust-mss** not working after delete and reconfigure
CSCwi62230	SIG tunnel is showing blank value
CSCwj27545	Device crashing due to ftmd
CSCwi62239	Error after configuring loopback managment vrf then removing it
CSCwj70773	Unable to create a portchannel interface with maximum number limit

Open Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwj04575	Device crashed during SNMPwalk when removing SFP
CSCwj25508	Device reports incorrect DOM values over SNMP
CSCwj48393	Service with no priority are not working as expected
CSCwj48421	IPSEC packet has invalid spi
CSCwi86227	Device reports incorrect DOM values over SNMP
CSCwj01917	Device forced to Admin Down
CSCwj30909	Device upgrade fails

Identifier	Headline
CSCwj09284	Unexpected reboot due to SSL
CSCwj40589	Endpoint tracker using DNS does not log DOWN message when DNS server reachability is lost
CSCwj26085	Control connections goes to trying state with UTD
CSCwj29381	Service-policy will not be applied to a new tunnel interface when sourced using sub-interface.
CSCwj45177	dmidecode: command not found error seen executing **show sdwan certificate validity**
CSCwh29856	Removing IP DNS profile:0 active_prof:0 immediately after attachment
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE
CSCwi56641	Device reports link-flap error when peer reloads
CSCwi81026	BFD Sessions Flapping During IPSec Rekey in Scaled Environment
CSCwi59854	**show sdwan policy service-path** command gives inconsistent results with app name specified
CSCwj42448	APN password in plain text when device is configured
CSCwj02661	UTD signature update failure and device not recording the update
CSCwi89510	Device flow causing overruns
CSCwj43905	Unexpected Reboot Due to QFP-Ucode-Radium Failure
CSCwj38804	ZBFW FQDN patterns missing from QFP patten-list
CSCwj02628	Speed-test not working for device
CSCwi91887	IPsec PWK SPI mismatch causes tunnels to remain in down state
CSCwj49941	dns-snoop-agent has TCAM entry with all zeros for some regex patterns
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented
CSCwj40223	appRouteStatisticsTable sequence misordered or OS returns wrong order
CSCwi98171	Interface will not come up with autonego enabled
CSCwj32347	DIA Endpoint tracker not working with ECMP routes when Loopback is used as Source
CSCwj27108	Device not balancing traffic to default route
CSCwj44843	Deploy of Policy Group fails after detach of Embedded Security Policy
CSCwj31354	Template push failure due to service timestamps

Identifier	Headline
CSCwj30334	CVLA ucode crash when attempting merge on used block
CSCwj48785	Cellular Monitoring: Active SIM value should not come up as 0 when NO SIM in device

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) - 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: 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 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 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.