Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE 17.16.x

First Published: 2024-12-22

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 The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note Sections in this documentation apply to all models of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

Note Cisco IOS XE 17.16.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE 17.16.x release series.

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.

New and Changed Hardware and Software Features

There are no new hardware features in this release.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.

Note To access CFN, you do not require an account on cisco.com.

New and Changed Hardware Features

There are no new hardware features in this release.

New and Changed Software Features in Cisco IOS XE 17.16.1a

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms

Feature	Description
Asymmetric carrier delay	Asymmetric Carrier Delay allows you to configure separate delay times for link-up and link-down event notification on physical interfaces. From Cisco IOS XE 17.16.1a, asymmetric carrier delay is supported on <***Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms***.
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.
DHCP support for MAP-T Customer Edge (CE)	From Cisco IOS XE 17.16.1a onwards, the MAP-T CE functionality is extended to support DHCP.
Disablement of WeakSSH Algorithms	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
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
Enhancements to Segment Routing over IPv6 Data plane	From Cisco IOS XE 17.16.1a, Segment Routing over IPv6 data plane supports these functionalities:- eBGP Inter-AS- PCE-Delegated Path Computation- Enhancements to OAM Traffic Engineering.
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 the following parameters: • Access Point Name (APN), and • Cellular Link Uptime
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.
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.
Monitoring Crypto VPN solutions on SD-Routing devices	If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNson SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize theVPN 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.
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.
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.

Feature	Description
Support for Enrollment over Secure Transport (EST)	From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the **enrollment http username [http_username] password [http_password]** command.
Support for Network Slicing on 5G standalone networks	From Cisco IOS XE 17.16.1a, slice-type and slice-differentiator options are introduced for cellular profiles in 5G standalone networks.
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.
Cisco Unified Border Element (CUBE)	
Secure Communications Interoperability Protocol (SCIP) support in CUBE	From Cisco IOS XE 17.16.1a onwards, support for Secure Communication Interoperability Protocol (SCIP) voice and video codec is available, that ensures secure traffic sessions between the endpoints. **Preview Feature Disclaimer** The Secure Communications Interoperability Protocol (SCIP) feature in Cisco IOS XE 17.16.1a release is available in 'preview' mode as it includes limited functionality or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Cisco Technical Support provides reasonable effort support for features in preview mode. There is no Service Level Objective (SLO) in response times for features in preview mode; response times may be slow.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.15.x releases.

Table 2: Minimum and Recommended ROMMON Releases Supported on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
Catalyst 8300 Series Edge Platforms			

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
C8300-1N1S-4T2X|6T	17.15.1a	17.3(4.2r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.15.1a	17.3(4.1r)	17.7(1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)
C8200L-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)

Note For Cisco Catalyst 8200 and 8200L Series Edge platforms, if your ROMMON is at a version lower than 17.6(8.1r), you can upgrade the device to IOS XE 17.15.1a using any of the following methods:

- in bundle mode, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a, OR
- in bundle mode, manually upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a.
- in install mode, you can upgrade the device to IOS XE 17.15.1a; the ROMMOM is auto-upgraded to the recommended version when the device boots.

For Cisco Catalyst 8300 Series Edge platforms, if your ROMMON is at a version lower than the minimum supported version, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to the recommended version. You can then upgrade the device to 17.15.1a.

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 ROMMON Compatibility Matrix 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.

Resolved and Open Bugs for Cisco IOS XE 17.16.x

Resolved Bugs in Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwn15231	VG410 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.
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.
CSCwm89225	CPP crashes After Routing Table Changes.
CSCwk62954	Multiple "match address local interface <int>" not pushed from vmanage under crypto profile.
CSCwk79606	The PKI **Trustpoint password** command only allows encryption type 0 and 7 on all IOS XE platforms.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwm48459	Software crash with Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
CSCwn29062	Traceback log output on C8200 with "DATACORRUPTION" 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	SIT-SDWAN: Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
CSCwm88350	The **no autostate** command isn't available on CLI C1121X-8PLTEP but possible to configure via CLI Add-On.
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call.

Open Bugs in 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.
CSCwn09185	Traffic loss observed on minimal values with time based policy-map.

Identifier	Headline
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.
CSCwk27078	ROMMON auto-upgrade is failing.
CSCwm71639	The cpp_cp_svr crash noticed when configured service-policy to a Dialer interface.
CSCwn24226	GETVPN Mismatch in GMs reported across COOP.
CSCwn40906	Device 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 reloading the device.
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwm87270	MKA session down with "ICV Verification of a MKPDU failed for" error on one of the interface.
CSCwn39447	SpeedTest might work abnormally after changing system-ip.
CSCwn12594	SIG zscaler Ipsec - Vpn credentials for primary tunnel not created.
CSCwn35476	The cflowd source interface for sub-interface does not get pushed to cedge.

Related Documentation

- Hardware Installation Guide for Catalyst 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide

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.