Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE 17.14.x

First Published: 2024-04-29

Full Cisco Trademarks with Software License

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 17.14.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE 17.14.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 17.14.1a

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

Feature	Description
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
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 the Cisco SD-WAN Manager.
Configure SSL/TLS Proxy for Decryption of TLS Traffic on SD-Routing Devices	The SSL/TLS Proxy feature allows you to configure an autonomous device as a transparent SSL/TLS proxy. Such proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection by Unified Threat Defense (UTD) and identify risks that are hidden by end- to-end encryption.

Feature	Description
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.
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
View Unmodeled Commands on SD-Routing Devices	After an SD-Routing device is deployed, you can view the unmodeled commands on the Cisco SD-WAN Manager. The list of unmodeled commands are regenerated if the device reboots.
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 same router 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
Enhancement to the show reload-history Command	From Cisco IOS XE 17.14.1a, the **show reload-history** command is modified to **show reload history**. The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.
IP Endpoint Delay Measurement and Liveness Monitoring	This feature enables you to measure the end-to-end delay and monitor liveness toward either a specified IPv4 or IPv6 endpoint. From Cisco IOS XE 17.14.1a, you can configure this feature using the **performance-measurement endpoint** command and **performance-measurement delay-profile endpoint** command.
MAP-T Customer Edge (CE) Support	The MAP-T Customer Edge (CE) functionality is used to translate IPv4 packets to IPv6 packets, and vice versa. From Cisco IOS XE 17.14.1a, MAP-T utilizes the existing NAT44 pool-based translation on the CE device to translate private IPv4 addresses to public IPv4 addresses, and then utilizes the existing NAT64 translation to replace the IPv4 header with the IPv6 header.
Power Usage Statistics	This feature allows you to display the name of the component and its power consumption, including the total power usage of the device. From Cisco IOS XE 17.14.1a, you can use the **show power usage** command to display the power consumption of each component of the device, and the total power consumption of the device.
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 Catalyst 8300 Series Edge Platforms: • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T • C8200L-1N-4T

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 (millivolt) and mA (milliampere) for your devices.
Support for Load Balancing for EtherChannels on the Transport Side	This feature adds the ability to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices using the **port-channel load-balance-hash-algo** SD-WAN command.
Cisco Unified Border Element (CUBE) and SRST Features	
CUBE: Secure SIP with TLS 1.3 support	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of Transport Layer Security (TLS) version 1.3 and associated cipher suites.
SRST: Secure SIP with TLS 1.3 support	Starting from Cisco Unified SRST 14.4 release, the SRST security feature is enhanced to support TLS version 1.3 and associated ciphers.
Licensing Features	
500 Mbps Aggregate for Tier 1 and 250 Mbps Throughput Configuration in Autonomous Mode	Starting with this release, when you configure a throughput of 250 Mbps or T1, *if* an HSECK9 license is available on the device, then aggregate throughput throttling is effective. Any distribution of traffic within the 500 Mbps limit is allowed in the upstream and downstream direction. In earlier releases, bidirectional throughput throttling was applicable to T1 and 250 Mbps and throughput was capped at 250 Mbps in *each* direction.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.14.x releases.

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

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X|6T	17.14.1a	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.14.1a	17.3(1.2r)	17.6(6.1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.14.1a	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.14.1a	17.5(1.1r)	17.6(6r)

Resolved and Open Bugs for Cisco IOS XE 17.14.1a

Resolved Bugs in Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwh94906	The device Wireless LAN Controller (WLC) experienced a crash due to a segmentation fault associated with the Network Mobility Services Protocol (NMSP).
CSCwi03502	Create a CLI command that sends 'at#enadis=0' followed by 'at#reboot' to the device, which is necessary during the configuration of Multi-PDN.
CSCwi49846	ftmd crashed when SIG GRE tunnels configs are removed.
CSCwi55725	SDR CLI config group issue.
CSCwi61369	cEdge device may unexpectedly reload due to SIGABRT.
CSCwi35716	AAR backup preferred color not working as expected from 17.12.1.
CSCwi76516	esim cellular configuration tamplate deployemt fails.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwf08658	If we are in a non-equilibrium state and have symmetric NAT, edge devices will cause the BFD sessions to flap.
CSCwf84567	Unexpected reload after re-connecting to the Cisco SD-WAN Controller.
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
CSCwj25493	cEdge crashed twice with critical process linux_iosd_image fault on rp_0_0.
CSCwi40603	Memory leak in the Crypto IKMP process.

Identifier	Headline
CSCwh36635	17.13 Device: confd / SMP crash. Core file decode failed.
CSCwi35177	Device crash caused by continuous interface flap, interface associated to many IPsec interfaces.
CSCwi60266	After an upgrade, cEdge devices with enterprise certificates are failing to establish control connections with controllers.
CSCwi67983	Cisco Catalyst SD-WAN cEdge / Tracker state log is missing when DNS query fails.
CSCwi53951	Packets with unicast MAC get dropped on a Port Channel L2 sub-intf after a device reboot.
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version.
CSCwi53549	cedge router crash with reason, critical process fman_fp_image fault on fp_0_0 (rc=134).
CSCwi82548	Crash in IKEv2 cluster load balancer.
CSCwi51381	TrapOID of ciscoSdwanBfdStateChange is different from the MIB file.
CSCwh09033	Device unable to boot with C-NIM-8T module.
CSCwi78365	Trim installed certificate on upgrade.
CSCwi85293	In an IKEv2 IPv6 cluster with load balancing, if Front VRF (FVRF) is used, the secondary node in the cluster cannot establish a connection to the cluster.
CSCwi86698	When using a multicast address as the system IP in an SD-routing device, no error message is displayed.
CSCwi93784	(SWI case 01257768)FW upgrade does not work properly on P-LTE-MNA with 17.12.1a and 17.12.2 IOS.
CSCwj06622	Segmentation fault and core files are seen on IOS-XE in controller-manged SD-WAN due to speedtest.
CSCwi16111	After deleting and reconfiguring the IPv6 TCP adjust-mss setting, it is not functioning correctly.
CSCwi62230	For the SIG tunnel, the IG STATE displays a blank value.
CSCwj27545	cEdge device crashes due to ftmd.
CSCwj70773	Unable to create a portchannel interface with maximum number limit

Open Bugs in Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwh86922	Disabling EVC (Ethernet Virtual Circuit) does not restore the original MAC filter table entries for the interface on the device.

Identifier	Headline
CSCwj48421	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPsec packet has invalid spi.
CSCwj07584	Using the same HSRP virtual MAC address across multiple interfaces can lead to issues with data processing on the device.
CSCwj02246	After executing the **no shutdown** command on the interface, the SFP EN (Enable) LED on the device does not illuminate.
CSCwi29637	The SFP interface on the device is shut down, yet the corresponding interface on the connected device remains active.
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwi98707	NIM module on the device reloads while collecting PCM captures on voice-port.
CSCwj40589	The endpoint tracker, which utilizes DNS, fails to record a down message when it can no longer reach the DNS server.
CSCwj26085	During system integration testing (SIT), it has been observed that when Unified Threat Defense (UTD) is enabled, the control connections in Transport Layer Security (TLS) for Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager switch to a trying state .
CSCwj45177	When attempting to execute the **show sdwan certificate validity** command, an error stating 'dmidecode: command not found' is displayed.
CSCwj34578	When the device is configured for NAT64 and is also functioning as a Customer Edge (CE) device for Carrier Supporting Carrier (CsC), the NAT46 translation packets are being dropped.
CSCwi81026	SDWAN BFD sessions are flapping during IPsec rekey in a scaled environment.
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).The device has encountered a critical issue: the process named cpp_ha_top_level_server has failed on the forwarding processor fp_0_0 with a return code of 69.
CSCwi59854	When the **show sdwan policy service-path** command is executed with a specific application name included, it produces inconsistent results.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwj02661	UTD signature update failure and device is not recording the update.
CSCwj43905	Unexpected reboot due to QFP-Ucode-Radium failure.
CSCwj02628	Speed-test is not working for the cEdge device running on code 17.12.2.
CSCwi59834	entSensorThresholdValue OID for PDU1 missing on the device.
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented.

Identifier	Headline
CSCwj40223	In the CISCO-SDWAN-APP-ROUTE-MIB, the sequence of entries within the appRouteStatisticsTable is out of order, or alternatively, the operating system is returning the sequence in the incorrect order.
CSCwj30334	CVLA ucode crash when attempting merge on used block.
CSCwj34010	[SITLite]: TLOC extension FIA is missing on interface in edge device leading to incorrect control.
CSCwj27108	The Cisco Catalyst SD-WAN Manager is not distributing traffic evenly across the default routes.
CSCwj49941	dns-snoop-agent has TCAM entry with all zeros for some regex patterns.
CSCwj31354	Template push failure due to service timestamps.
CSCwj32347	DIA endpoint tracker is not working with ECMP routes.
CSCwj13681	Device can only store 64 FQDN patterns, but config accepts more than 64.

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 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.