



# 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

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](http://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 17.14.1a 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://cfng.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
<a href="#">Configuration Group Enhancements</a>	This release introduces support for the following in Cisco SD-WAN Manager: <ul style="list-style-type: none"> <li>• Transport Profiles</li> <li>• Management Profile</li> <li>• Service Profile</li> <li>• CLI Profile</li> <li>• Policy Object Profile</li> </ul>
<a href="#">Configure Secure Service Edge</a>	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.
<a href="#">Configure SSL/TLS Proxy for Decryption of TLS Traffic on SD-Routing Devices</a>	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	<p>This release introduces support for the following VPN solutions:</p> <ul style="list-style-type: none"> <li>• FlexVPN</li> <li>• GETVPN</li> <li>• DMVPN</li> <li>• L3VPN</li> </ul> <p>These VPN solutions can be configured by using <b>Configuration &gt; Configuration Groups &gt; CLI Add-on Profile</b> option in Cisco SD-WAN Manager.</p>
YANG Configurational Model Support for SD-Routing Devices	<p>This release introduces support for the following YANG Configurational Models:</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• MPLS</li> <li>• RSVP</li> <li>• SNMP</li> <li>• AAA</li> <li>• QoS</li> <li>• ACL</li> <li>• DHCP</li> </ul>
<a href="#">View Unmodeled Commands on SD-Routing Devices</a>	<p>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.</p>
<a href="#">Enhanced IS-IS Fast Flooding</a>	<p>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 <b>router isis lsp-fast-flooding</b> command. The LSP transmission can be further customized with arguments such as <b>max-lsp-tx</b>, <b>psnp-interval</b>, and <b>per-interface</b> within the same router isis command, and enhanced by using the <b>isis remote-psnp-delay</b> command. This feature is disabled by default, and requires manual configuration to enable.</p>

Feature	Description
Enhancement to the show reload-history Command	From Cisco IOS XE 17.14.1a, the <b>show reload-history</b> command is modified to <b>show reload history</b> . 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 <b>performance-measurement endpoint</b> command and <b>performance-measurement delay-profile endpoint</b> 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 <b>show power usage</b> 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: <ul style="list-style-type: none"> <li>• C8300-1N1S-6T</li> <li>• C8300-1N1S-4T2X</li> <li>• C8300-2N2S-6T</li> <li>• C8300-2N2S-4T2X</li> </ul> Cisco Catalyst 8200 Series Edge Platforms: <ul style="list-style-type: none"> <li>• C8200-1N-4T</li> <li>• C8200L-1N-4T</li> </ul>

Feature	Description
<a href="#">Voltage and Current Metrics</a>	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 <b>show environment</b> command to display the PEM sensor readings in mV (millivolt) and mA (milliampere) for your devices.
<a href="#">Support for Load Balancing for EtherChannels on the Transport Side</a>	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 <b>port-channel load-balance-hash-algo</b> SD-WAN command.
<b>CUBE Features</b>	
<a href="#">Secure SIP with TLS 1.3 support</a>	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of <a href="#">Transport Layer Security (TLS) version 1.3 and associated cipher suites</a> .
<b>Licensing Features</b>	
<a href="#">500 Mbps Aggregate for Tier 1 and 250 Mbps Throughput Configuration in Autonomous Mode</a>	Starting with this release, when you configure a throughput of 250 Mbps or T1, <i>if</i> 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 <i>each</i> 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
<b>Catalyst 8300 Series Edge Platforms</b>			
C8300-1N1S-4T2X 6T	17.14.1a	17.3(1r)	17.6(6r)

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
C8300-2N2S-4T2X 6T	17.14.1a	17.3(1.2r)	17.6(6.1r)
<b>Catalyst 8200 Series Edge Platforms</b>			
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
<a href="#">CSCwh94906</a>	The device Wireless LAN Controller (WLC) experienced a crash due to a segmentation fault associated with the Network Mobility Services Protocol (NMSP).
<a href="#">CSCwi03502</a>	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.
<a href="#">CSCwi49846</a>	ftmd crashed when SIG GRE tunnels configs are removed.
<a href="#">CSCwi55725</a>	SDR CLI config group issue.
<a href="#">CSCwi61369</a>	cEdge device may unexpectedly reload due to SIGABRT.
<a href="#">CSCwi35716</a>	AAR backup preferred color not working as expected from 17.12.1.
<a href="#">CSCwi76516</a>	esim cellular configuration tamplate deployemt fails.
<a href="#">CSCwi53306</a>	Unknown appID in ZBFW HSL log.
<a href="#">CSCwf08658</a>	If we are in a non-equilibrium state and have symmetric NAT, edge devices will cause the BFD sessions to flap.
<a href="#">CSCwf84567</a>	Unexpected reload after re-connecting to the Cisco SD-WAN Controller.
<a href="#">CSCwi14178</a>	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
<a href="#">CSCwj25493</a>	cEdge crashed twice with critical process linux_iosd_image fault on rp_0_0.
<a href="#">CSCwi40603</a>	Memory leak in the Crypto IKMP process.
<a href="#">CSCwh36635</a>	17.13 Device: confd / SMP crash. Core file decode failed.
<a href="#">CSCwi35177</a>	Device crash caused by continuous interface flap, interface associated to many IPsec interfaces.

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

### Open Bugs in Cisco IOS XE 17.14.1a

Identifier	Headline
<a href="#">CSCwh86922</a>	Disabling EVC (Ethernet Virtual Circuit) does not restore the original MAC filter table entries for the interface on the device.
<a href="#">CSCwj48421</a>	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPsec packet has invalid spi.
<a href="#">CSCwj07584</a>	Using the same HSRP virtual MAC address across multiple interfaces can lead to issues with data processing on the device.



Identifier	Headline
<a href="#">CSCwj02246</a>	After executing the <b>no shutdown</b> command on the interface, the SFP EN (Enable) LED on the device does not illuminate.
<a href="#">CSCwi29637</a>	The SFP interface on the device is shut down, yet the corresponding interface on the connected device remains active.
<a href="#">CSCwj09284</a>	Unexpected reboot in WLC due to SSL.
<a href="#">CSCwi98707</a>	NIM module on the device reloads while collecting PCM captures on voice-port.
<a href="#">CSCwj40589</a>	The endpoint tracker, which utilizes DNS, fails to record a down message when it can no longer reach the DNS server.
<a href="#">CSCwj26085</a>	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 .
<a href="#">CSCwj45177</a>	When attempting to execute the <b>show sdwan certificate validity</b> command, an error stating 'dmidecode: command not found' is displayed.
<a href="#">CSCwj34578</a>	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.
<a href="#">CSCwi81026</a>	SDWAN BFD sessions are flapping during IPsec rekey in a scaled environment.
<a href="#">CSCwi67621</a>	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.
<a href="#">CSCwi59854</a>	When the <b>show sdwan policy service-path</b> command is executed with a specific application name included, it produces inconsistent results.
<a href="#">CSCwj42448</a>	APN password in plain text when cellular controller profile is configured.
<a href="#">CSCwj02661</a>	UTD signature update failure and device is not recording the update.
<a href="#">CSCwj43905</a>	Unexpected reboot due to QFP-Ucode-Radium failure.
<a href="#">CSCwj02628</a>	Speed-test is not working for the cEdge device running on code 17.12.2.
<a href="#">CSCwi59834</a>	entSensorThresholdValue OID for PDU1 missing on the device.
<a href="#">CSCwi77159</a>	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented.
<a href="#">CSCwj40223</a>	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.
<a href="#">CSCwj30334</a>	CVLA ucode crash when attempting merge on used block.

Identifier	Headline
<a href="#">CSCwj34010</a>	[SITLite]: TLOC extension FIA is missing on interface in edge device leading to incorrect control.
<a href="#">CSCwj27108</a>	The Cisco Catalyst SD-WAN Manager is not distributing traffic evenly across the default routes.
<a href="#">CSCwj49941</a>	dns-snoop-agent has TCAM entry with all zeros for some regex patterns.
<a href="#">CSCwj31354</a>	Template push failure due to service timestamps.
<a href="#">CSCwj32347</a>	DIA endpoint tracker is not working with ECMP routes.
<a href="#">CSCwj13681</a>	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.