Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE 17.13.x

First Published: 2023-12-16

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 17.13.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE 17.13.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

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 17.13.1a

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

Feature	Description
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 network segments.
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.
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.
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 global **i**p arp nat-garp-retry and ip nat inside source static commands.

Feature	Description
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.
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).
Speed Test for SD-Routing Devices	Cisco SD-WAN Manager allows you to measure the network speed and available bandwidth between adevice 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.
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.
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).
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.
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.

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
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.
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.
CUBE Features	
NAT Traversal using RTP Keepalive	From Cisco IOS XE 17.13.1a onwards, using RTP keepalive packets, CUBE supports media transmission in the NAT environment.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.13.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	17.13.1a	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.13.1a	17.3(1.2r)	17.6(6.1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.13.1a	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.13.1a	17.5(1.1r)	17.6(6r)

Resolved and Open Bugs for Cisco IOS XE 17.13.x

Resolved Bugs in Cisco IOS XE 17.13.1a

Identifier	Headline
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwf25735	QoS with more than four remark with set-cos does not work.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf80400	IOS XE router may experience unexpected reset while executing **show utd engine standard statistics** command
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 selected Next-hop.

Open Bugs in Cisco IOS XE 17.13.1a

Identifier	Headline
CSCwh94906	Device segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwi03502	Creation of CLI to push at#enadis=0, followed by at#reboot to FN980, is required when configuring Multi-PDN.
CSCwh84068	Device crash after changing NAT HSL configuration.
CSCwh77221	SNMP unable to poll Cisco SD-WAN tunnel data after a minute.
CSCwi15930	Device failing to upgrade due to CDB issue.

Identifier	Headline
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 : x.x.x.x Port: 830 user : Cisco SD-WAN-admin error : Connection failed.
CSCwh01678	Device FTM crash with SIG enabled.
CSCwi05395	SNMP bulkget cannot get loss, latency and jitter for ProbeClassTable and ClassIntervalTable OIDs.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwi05680	Device crashed generating multiple system reports.
CSCwi16452	Error thrown when switching from SSE to SIG
CSCwi11807	SNMP bulkget breaks the OID "appRouteStatisticsTable" 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.
CSCwi15688	Unexpected NAT translation occurs in a specific network.
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSec SVTI tunnel.
CSCwi14899	Device dropping IPSEC traffic when SVI is used as source for DMVPN tunnel.
CSCwi23562	When RADIUS down, and there is an IKE-AUTH request received, the box stops replying to DPD packets.
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.
CSCwh52440	IP SLA does not have checks for ICMP probes to be sent on source interface.
CSCwi31833	UTD deployment failing if deployed from remote server hostname rather than ip.
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many IPsec interfaces.
CSCwi30529	AAA:Template push fail when AAA authorization is set to local.

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.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The 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.