Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE Dublin 17.10.x

First Published: 2022-12-17

Last Modified: 2023-10-16

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 Starting with Cisco IOS XE Amsterdam 17.3.2, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
- Cisco Smart License Utility (CSLU), and
- Smart Software Manager On-Prem (SSM On-Prem)

Note Cisco IOS XE Dublin 17.10.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Dublin 17.10.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

New and Changed Hardware Features

There are no new hardware features in this release.

New and Changed 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 http://www.cisco.com/go/cfn.

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

New Software Features

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms IOS XE Dublin 17.10.1a

Feature	Discription
Packet Tracer with UDF Offset	Using this feature you can configure to match the packets based on user defined field position and length. This can be used by an ACL to match packets that cannot be classified easily with the traditional Layer 3 and Layer 4 field information.
Segment Routing Absolute One-Way Link Loss Measurement for GRE-IPSec Tunnel	This feature provides a mechanism for link loss measurement for point-to-point GRE-IPSec tunnel and identifies paths that meet specified loss criteria. **Note** This feature is supported only on Cisco Catalyst 8300 Series Edge platforms.

Feature	Discription
Support for Secure Real-time Transport Protocol (SRTP) Dual-Tone Multi-Frequency (DTMF) Interworking	This feature provides support for Dual-Tone Multi-Frequency (DTMF) interworking between Cisco Unified Communications Manager (CUCM) and Secure Software MTP in pass-through mode. It is supported on both CUCM and Cisco IOS XE software.
Support for YANG Operational Model in the GETVPN architecture	This feature enables the YANG operational model in the GETVPN architecture to support the crypto gdoi command which was previously enabled only for the CLI and SNMP models.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.10.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	17.10.1a	17.3(1r)	17.3(5r)
C8300-2N2S-4T2X|6T	17.10.1a	17.3(1.2r)	17.3(4.1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.10.1a	17.4(1r)	17.4(3r)
C8200L-1N-4T	17.10.1a	17.5(1.1r)	17.5(2r)

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.

Resolved Bugs in Cisco IOS XE 17.10.1a

Identifier	Headline
CSCwc70511	Device reloads unexpectedly during NHRP processing.
CSCwb35303	X25 FRMR seen when switching from XOT to low speed serial.
CSCwc77981	Device running 17.3(4a) crashed - track the fman-fp's memory leak caused by cond-debug.

Identifier	Headline
CSCwc29735	Improve debug for reload at crypto_dev_proxy_ipc_ipsec_sa_crt_hndlr when scale exceed limit.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linestate down.
CSCwc78021	Standby device crash @ fman_acl_remove_default_ace.
CSCwd16664	GetVPN Long Security Association - GM re-registration after encrypting 2^32-1 of packets in one IPsec security association.

Open Bugs in Cisco IOS XE 17.10.1a

Identifier	Headline
CSCwd25107	Interface Vlan1 is placed in shutdown state when configured with **`ip address pool`** command.
CSCwd23810	IOS-XE: A high CPU utilization caused by NHRP.
CSCwd45402	MSR Unicast-To-Multicast is not working if the destination and source address are the same in Service Reflect configuration.
CSCwd45363	IPSEC throughput level displays ambiguous outputs.
CSCwd61255	Data Plane crash is seen on the device when making the QOS configuration changes.
CSCwd49309	Ucode crash is seen on the device with traffic pointing to segfault in coff handler.
CSCwc65697	Device crashing and restarting during call flow with new image.
CSCwd53205	IKEv2: The RRI routes are intermittently disappearing from a FlexVPN hub.
CSCwd34860	Displays the increase of Input errors without any other specifc errors when the **`show interface`** is executed.
CSCwc99823	Fman crash is seen in SGACL@ fman_sgacl_calloc.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwd67335	Device reload unexpectedly when enabling IDS.
CSCwd12828	Segmentation fault crash in CCSIP_SPI_CONTROL process.
CSCwd74089	CUBE call leak at FPI layer.
CSCwc66646	Unexpected reload due to segmentation fault in the CCSIP_SPI_CONTROL process.
CSCwc23645	When using SRTP with higher ciphers, CUBE is inserting distortion in voice.

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.