Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-17

Full Cisco Trademarks with Software License

About Cisco Catalyst 8300 Series Edge Platforms

The Cisco 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 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 8300 Series Edge Platforms is 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 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 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 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 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 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 Cupertino17.7.1a is the first release for Cisco Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Cupertino 17.7.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

Table 1: New Hardware Features

Feature	Description
5G LTE PIM	The 5G sub-6 GHz Pluggable Interface Module (PIM) P-5GS6-GL is supported on the Cisco Catalyst 8300 Series Edge Platforms.

New and Changed Software Features

This section enlists the new and enhanced or modified features that are supported on the Cisco Catalyst 8300 Series Edge Platforms:

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 2: New Software Features in Release Cisco IOS XE Cupertino 17.7.1a

Feature	Description
Cisco ThousandEyes Eterprise Application Hosting	The Cisco ThousandEyes Enterprise Agent Application introduces the functionality to inherit the Domain Name Server (DNS) information from the device. With this enhancement, the DNS field in vManage ThousandEyes feature template is an optional parameter.

Feature	Description
Multicast Group Calculation	The **show ip multicast overlay-mapping** command displays an underlay group address from the overlay group address which is used to troubleshoot or configure the network. The output includes the underlay group address that is within the configured SSM (Source Specific Multicast) address range.
Install Mode for Cisco Catalyst 8000 Series Edge Platforms	All the Cisco Catalyst 8000 Series Edge Platforms are now configured to boot by default in install mode instead of bundle mode. This allows you to boot the device, and upgrade or downgrade the device using a set of install commands. Install mode uses *.pkg* files instead of *.bin* file to install the package, and provides a faster installation, with increased flexibility and control.
SHA2 Support for TLS1.2 & SRTP	This feature supports the Next Generation Encryption (NGE) cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both STCAPP analog phone and SCCP DSPFarm conferencing service. These cipher suites provide confidentiality, integrity, and authenticity to validate messages.
Programmability Features	
Converting IOS Commands to XML	This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages.
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.7.1a uses the YANG version 1.0; however, you can download the Cisco IOS XE YANG models in yang version 1.1 from GitHub athttps://github.com/YangModels/yang/tree/master/vendor/cisco/xe folder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG version 1.1 migration process, send an email to xe-yang-migration@cisco.com.
Smart Licensing Using Policy Features	
Ability to Save Authorization Code Request and Return in a File and Simpler Upload in the CSSM Web UI	If your product instance is in an air-gapped network, you can now save an SLAC request in a file on the product instance. The SLAC request file must be uploaded to the CSSM Web UI. You can then download the file containing the SLAC code and install it on the product instance. You can also upload a return request file in a similar manner. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate an SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, you must upload the SLAC request or return file in the same way as you upload a RUM report. In the required Smart Account, navigate to **Reports** > **Usage Data Files**. See: No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU, Saving a SLAC Request on the Product Instance, Removing and Returning an Authorization Code, Uploading Data or Requests to CSSM and Downloading a File.
Account Information Included in the ACK and showcommand outputs	A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See: show license summary, show license status, show license tech.

Feature	Description
CSLU Support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux. See: CSLU, Workflow for Topology: Connected to CSSM Through CSLU, Workflow for Topology: CSLU Disconnected from CSSM
Factory-installed Trust Code	For new hardware and software orders, a trust code is now installed at the time of manufacturing. **Note** You cannot use a factory-installed trust code to communicate with CSSM. See: Overview, Trust Code.
RUM Report Optimization and Availability of Statistics	RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See: RUM Report and Report Acknowledgement, Upgrades, Downgrades, show license rum, show license all, show license tech.
Support to Collect Software Version in a RUM Report	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version information is included in the RUM report. See: license smart (global config).
Support for Trust Code in Additional Topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to Cisco Smart License Utility (CSLU)and in topologies where the product instance is in an air-gapped network. See: Trust Code, Connected to CSSM Through CSLU, Tasks for Product Instance-Initiated Communication, CSLU Disconnected from CSSM, Tasks for Product Instance-Initiated Communication,No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU.

Feature	Description
Tier Based Licenses	You can now configure tier-based throughput values if the license PID is tier-based. For example, for PID DNA-C-T0-E-3Y, you can configure Tier 0 (T0) as the throughput value on the platform. Starting with the lowest throughput level, the available tiers on the Cisco Catalyst 8200 Edge Series Platforms are Tier 0 (T0), Tier 1 (T1), Tier 2 (T2), and Tier 3 (T3). Each tier represents a throughput level. If you purchase a tier-based license PID, the license is displayed with the tier value in the CSSM Web UI. You can also convert the numeric throughput configuration of any existing tier-based license PIDs to a tier-based throughput value. **Note** T2 and higher tiers require an HSECK9 license and Smart Licensing Authorization Code (SLAC). Different platforms support different maximum throughput levels, therefore each tier means a different value for different platforms. The configuration guide provides details about how numeric throughput values map with tiers and how you can change to tier-based configuration. See: Available Licenses and Licensing Models.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.7.x releases.

Table 3: Minimum and Recommended ROMMON Releases Supported on C8300-1N1S-4T2X/6T

Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
17.6.1	17.3(5r)	17.3(5r)

Table 4: Minimum and Recommended ROMMON Releases Supported on C8300-2N2S-4T2X/6T

Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
17.6.1	17.3(4.1r)	17.3(4.1r)

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 17.7.2

Identifier	Headline
CSCwa17720	Router rebooted due to watchdogs after issuing the **show crypto mib ipsec** commands.

Identifier	Headline
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCwb03662	CDP/LLDP not working when 10GE interface enabled with MACSec .
CSCwa76260	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - DES, 3DES, DH1/2/5.
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade on the device.
CSCwb23043	MACsec not working on subinterfaces using dot1q >255 between Catalyst 8000 Series platforms.
CSCwa80474	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - MD5, SHA1.
CSCwa15085	Router crashes due to Stuck Thread with appnav-xe dual controller mode.
CSCvx28426	Router may crash due to Crypto IKMP process.
CSCwa38451	Packets loss happens on Cisco 8300 Series router when inserting SFP into or no shut other IF with a SFP.
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum.
CSCwa01293	ZBFW: Optimized policy traffic failure due to OG edit error.
CSCwa18177	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed.

Open Bugs in Cisco IOS XE 17.7.2

Identifier	Headline
CSCvz65764	Peer MSS value showing incorrect.
CSCwb25362	C-SM-16P4M2X module is not providing PoE on 17.6.1.
CSCwb78228	Device rebooted unexpectedly with reason "LocalSoft".
CSCwb25137	NAT: Source address translation for multicast traffic fails with route-map.
CSCwb78423	Excessive packet loss observed during DMVPN tunnel flapping.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading Catalyst 8300 peer device.
CSCwb66749	When configration IP NAt inside/outside on VASI intereface,ack/seq number abnormal.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwb74821	Yang-management process confd is not running, controller mode 17.6.2a.
CSCwb11389	NAT translation stops suddenly(IP NAT inside does not work).

Identifier	Headline
CSCwb51238	Router reloads unexpectedly twice when you enter the **netflowshow** command.
CSCwb61073	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps.
CSCvz94966	Device throughput drop of 10% from 17.3 to 17.6 Release.
CSCvz89354	Router Running 17.x.x Crashes Due to CPUHOG When Walking ciscoFlashMIB.
CSCwb79141	Device UCODE Crash with mpass function
CSCwb08186	E1 R2 - dnis-digits command is not working.
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
CSCwb12647	Device crashes for stuck threads in cpp on packet processing.
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled.
CSCwb41907	CPP uCode crashes due to ipc congestion from dp to cp.
CSCwb74917	Device incorrectly drops ip fragments due to reassembly timeout.
CSCwa67398	NAT translations do not work for FTP traffic.
CSCwb76509	Assert failure while showing FTM (Forwarding Traffic Manager) data in NH TYPE switch case.
CSCwa84919	Revocation-check crl none" does not failover to NONE DNAC-CA.
CSCwb78173	CSDL failure: IPSec QM Use of DES by encrypt proc is denied.
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwb46649	NAT translation do not show (or use) correct timeout value for an established TCP session.
CSCwb68897	Total output drops counter in show interface on Port-channel does not work properly.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwb29362	Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160.
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection.
CSCwb76866	CSDL failure: Use of MD5 by IPSEC key engine is denied.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.

Resolved Bugs in Cisco IOS XE 17.7.1a

Bug ID	Description
CSCvz71436	Call placing issue from SCCP phones.
CSCvy34805	Consecutive multicast crashes.
CSCvy92696	Cosmetic: 'Logging host' configuration inconsistent between sdwan and IOS configuration.
CSCvz30670	Qos issue on IPv6 Virtual access (tunnel ipsec) interface.
CSCvz14745	Memory leak seen when using DNS with IP SLA.
CSCvy27721	IOS-XE Router may experience unexpected reboot with X25 RBP.
CSCvy45095	IPV6 ebgp multihop session remains in "idle" state after removal and recreation of the config.
CSCvy72210	CIsco IOS XE crash after executing **show flowspec ipv4** command.
CSCvy42216	Switchport trunk native vlan xx" gets removed when upgrading from 16.12.x to 17.3.3
CSCvy53885	The **ip pim rp-candidate** command removed after reload when group list is configured.
CSCvz21812	QoS policy update with "random-detect dscp" configuration get rejected on device side.
CSCvy54964	Large tx/rx rate on Dialer interface in show interface output.
CSCvy23400	MC-LAG feature cannot preserve administratively shut down sub-interfaces.
CSCvy99942	Netconf: Logging to syslog stops working in certain scenarios.
CSCvy93946	Removal of SHA-1 HMAC Impacting ability to SSH.
CSCvy83154	MAG is not detecting the path UP after several reboots.
CSCvy29106	Device crashed on a Eigrp enabled device when Netconf get operation was used.
CSCvw13682	L3 connected lite session not coming up , stuck in data-plane(qfp).
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager.
CSCvy22343	Crash after reapplying BGP/ attempt to initialize an initialized wavl tree.
CSCvy91121	SSS manager Crash seen on latest polaris_dev image.
CSCvy08748	OSPF summary-address isn't generated though candidate exists.
CSCvz89043	Prevent SIP services from being blocked even if license usage ACK was not received.
CSCvy24754	Netconf-yang: no special characters allowed in ACL.

Open Bugs in Cisco IOS XE 17.7.1a

Bug ID	Description
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCwa07494	IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface.
CSCvz63763	QoS priority pkts dropped on serial interface when serial module is installed in C8300-2N2S SM slot.
CSCvz79855	CPU spike is observed on GD performance when Adaptive FEC is enabled.
CSCwa46001	VRRP traffic sent while the device boots will congest the interface queue causing taildrops.
CSCvz72871	Multicast traffic received over DMVPN tunnel are dropped on RP and not forwarded downstream.
CSCwa27659	virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCvz41067	IP Community-list config out of sync in sdwan and IOS -XE.
CSCwa22665	Memory leak in scaled EIGRP DMVPN implementation due to EIGRP: mgd_timer.
CSCvw06937	SNMv3 traps failing with initial configuration.
CSCvz86580	Unable to remove the BGP neighbor statement through vManage template.
CSCvz20285	Cisco SD-WAN image info not updated in packages.conf when upgrading in autonomous mode.
CSCvz55553	BGP routes refreshing in the routing table after adding "bgp advertise-best-external".

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.