Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-12-01

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 Cisco IOS XE Bengaluru 17.5.1a is the first release for Cisco Catalyst 8300 Series Edge Platforms.

Hardware and Software Features-New and Enhanced

New and Changed Hardware Features

New Hardware Features

- Cisco Catalyst 8300 Series Edge Platforms are available in these models:

- C8300-1N1S-4T2X
- C8300-1N1S-6T
- C8300-2N2S-4T2X
- C8300-2N2S-6T

Note N=Network Interface Modue, S=Services Module, and T=Gigabit Ethernet, X=Ten Gigabit

For information on the hardware features supported on the Cisco Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge Platforms datasheet.

- NIM-PVDM is the next-generation digital signal processor (DSP) module to utilize a PVDM4 chip for IP media services. This module enables the Catalyst 8300 Series Edge platforms to provide rich-media capabilities, such as high-density voice connectivity, conferencing, transcoding, media optimization, transrating, and secure voice for Cisco Unified Communications solutions

For information on the hardware features supported on the NIM-PVDM, refer to the Cisco Packet Voice Digital Signal Processor Modules for Cisco Unified Communications Solutions datasheet.

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 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.

Software Features

Smart Licensing Using Policy: An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.

With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.

Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available.

Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.

For conceptual, configuration, migration, and troubleshooting information for Smart Licensing Using Policy, see Cisco 8300 Series Software Configuration guide.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Table 1: New Software Features in Release Cisco IOS XE Bengaluru 17.4.1a

Feature	Description
Change of Authorization and Trustsec	This feature utilizes Posture Assessment capabilites to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication,authorization, and accounting (AAA) session after it is authenticated. Identity-Based Networking Services supports change of authorization (CoA) commands for session query,reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation
IP-SLA-HTTPS	This feature has enhanced capabilities of IP SLA device tracking with HTTPS probes and helps to verify reachability in the network.
Software Configuration Guide for Catalyst Cellular Gateway	Cisco Catalyst Cellular Gateways combine the latest in cellular technology with deployment flexibility, investment protection, and ease of management, with both traditional and SD-WAN deployments.
NBAR Support on the EVC Service Instance	To classify the data packets, enable NBAR FIA-trace data on the Ethernet flow point (EFP) interface. Quality of service (QoS) takes action on the EPF interface based on the results from the NBAR traffic classification.
BGP Large Community	The BGP large communities provide the capability for tagging routes and modifying BGP routing policy on routers. BGP large communities can be appended or removed selectively on the large community attribute as the route travels from router to router.
Consent Token Authorization Process for Dev Key Access	With the introduction of the dev-key install functionality, a subset of Cisco IOS XE platforms that support dev-key functionality are shipped only with a release public key. **Note** An image that is signed with a dev-key does not boot due to the absence of dev public key for image verification.
Configure Performance Measurement	This feature enables hardware timestamping. The Performance Measurement (PM) for link delay uses the light version of Two-Way Active Measurement Protocol (TWAMP) over IP and UDP
Configuring the Same Global Address for Static NAT and PAT	You can now configure the same global address within the static NAT and static PAT. This configuration is supported only on outside static NAT.

Feature	Description
Configuring Stateless Static NAT	Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. A new keyword stateless is introduced for Cisco IOS XE static NAT configuration and it applies only to static NAT command. When the static mapping is set to stateless, no sessions will be created for that traffic flow.
Dynamic Core Allocation	Platforms allow limited flexibility on how services run on the service plane cores. Dynamic core allocation allows in-service upgrade of Services, which eliminates the inactivity of compute resources. But, this requires reboot of the system to let the changes take effect.

Table 2: New SRST and CUBE Software Features in Release Cisco IOS XE Bengaluru 17.4.1a

Feature	Description
Unified SRST: Smart License Using Policy	Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.
CUBE: Hunt Stop for Server Groups	With server groups, you can create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured policy. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.
CUBE: Smart License Using Policy	Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.
CUBE: VoIP Trace Serviceability Framework	VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for persistently monitoring and troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition, data for calls with IEC errors is written to the logging buffer.

Feature	Description
CUBE: Clear Hung RTP Ports	When establishing a call, CUBE allocates several RTP ports that are based on the media that are negotiated for the session. Some ports remain assigned even after the call ends. In the current behavior, **show voip rtp stats**command displays only the ports allocated from the global table, even if the ports are allocated from all the three tables (Global port, media IP address-based, and media VRF-based). Now this command is enhanced to display the ports allocated from all the three tables. The command also displays the hung ports and allows you to release those ports. Releasing the hung ports increases the efficiency of the routers as more ports are available to receive calls.

Cisco Catalyst 8300 Series Edge Platforms ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 17.3.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
17.3.1	17.3(1r)	17.3(1r)

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

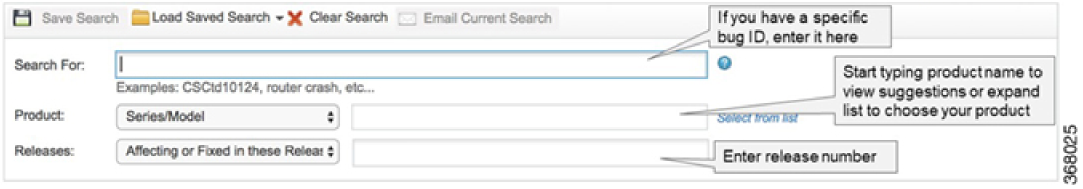
Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
17.3.1	17.3(1.2r)	17.3(1.2r)

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.



Search For:

Examples: CSCtd10124, router crash, etc...

Product: Series/Model

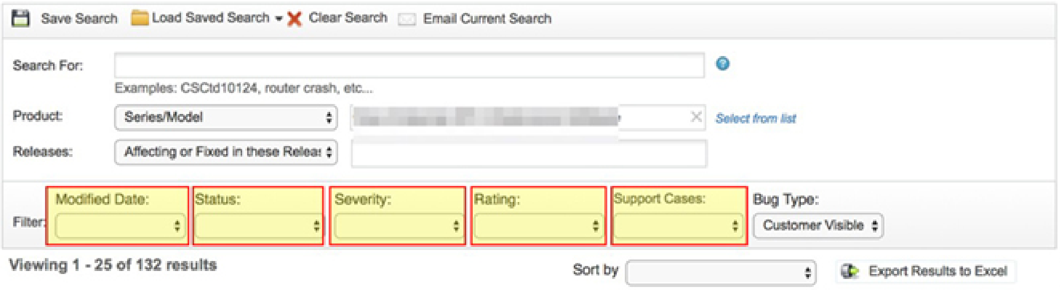
Releases: Affecting or Fixed in these Releas

If you have a specific bug ID, enter it here

Start typing product name to view suggestions or expand list to choose your product

Enter release number

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.



Search For:

Examples: CSCtd10124, router crash, etc...

Product: Series/Model

Releases: Affecting or Fixed in these Releas

Filter: Modified Date: | Status: | Severity: | Rating: | Support Cases: | Bug Type: Customer Visible

Viewing 1 - 25 of 132 results

Sort by

Resolved Caveats in Cisco IOS XE Bengaluru 17.4.2

There are no resolved caveats in this release.

Open Caveats in Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw84883	DDNS feature triggers crash on IOS XE 16.X and 17.X releases due to memory corruption.

Resolved Bugs in Cisco IOS XE Bengaluru 17.4.1a

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvu07639	UTD policy on global VPN does not work properly for DIA traffic
CSCvu10006	Performance monitor caused QoS miss classification
CSCvu11066	Umbrella custom dns config not in sync between confd and ios
CSCvu11115	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process
CSCvu34009	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall config
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP ISR4k router
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled
CSCvu76378	Curie : DP_Stuck is observed after reloading the NIM-VA-B module overnight
CSCvu77745	PMAN-3-PROCFAIL: Chassis 1 R0/0: pman: R0/0: The process keyman has failed (rc 139)

Caveat ID Number	Description
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart
CSCvu92879	Huge amount of Crypto PKI RECV memory leaks keep increasing during clients' SCEP enrollments.
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv04236	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails
CSCvv08341	Netconf deleting wrong IKEv2 parameters
CSCvv12401	ZBFW HA redundancy stuck in STANDBY-COLK-BULK. Bulksync Traceback seen in logs
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv36247	Memory Leak in MallocLite / Crypto IKMP
CSCvv47691	Reload: IOS-XE router crashing due to DN mismatch
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv83345	Summary/default-map routes getting ignored for p2p interface
CSCvw06719	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw64452	During Soak run, lot of policy drops due to less CPS rate set on Thorium
CSCvw12940	Curie 2RU Uranium: Make default filesystem format as ext4 on M2.NVMe
CSCvw33950	C8300-1N1S-4T2X: QFP uCode crash @ ipv4_nat_create_out2in_session_entry with traffic soak
CSCvw31389	PKTlog functionality is broken

Open Caveats in Cisco IOS XE Bengaluru 17.4.1a

Caveat ID Number	Description
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvv33576	IGMP snooping table not populated on ISR4k
CSCvv44331	AppQoe Clear Alarm is not generated from device
CSCvv68635	Observed HTX core at tcpproxy_libuinet_pkt_process during longevity test
CSCvv78028	No responder-bytes from cEdge when UTD is enabled

Caveat ID Number	Description
CSCvv79072	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	crash observed at NHRP while using summary-map
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
CSCvw70461	17.4 ZBFW:Classification of traffic not happening correctly sometimes when a rule in RS is edited.
CSCvw71941	QFP crash in cpp_ess_tc_tgt_if_fm_edit_helper
CSCvw74361	IPSec SA receives HMAC error" observed during the tunnel interface flap

Related Documentation

- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Policy for Smart Licensing guide
- Software Configuration Guide for Catalyst 8300 Series Edge Platforms