Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Cupertino 17.8.x

First Published: 2022-04-22

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 Cupertino17.9.1a is the first release for Cisco Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Cupertino 17.9.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

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 1: New Software Features in Release Cisco IOS XE Cupertino 17.8.1a

Feature	Description
Configuring Supplementary Voice Features	The device supports the SIP Line Side features such as Directed Call Park, Call Pick Up, Call Transfer, and so on. To provision these features, configure the outbound VOIP Dial-Peer, Pots Dial-Peer, Voice Card, and SIP in the device.
Download AnyConnect Profiles with IPSec IKEv2 VPN	This feature allows you to configure Internet Protocol Security (IPSec)-Internet Key Exchange (IKEv2) VPN to download AnyConnect profiles over SSL, for IOS-XE headends.

Feature	Description
Support for bidirectional debugging	You can now enable bidirectional debugging of traffic using d**ebug platform condition match** command.
Aggregate Throughput Throttling	For throughput levels greater than 250 Mbps and Tier 2 and higher tiers, when you configure the bidirectional throughput value on the device, aggregate throughput throttling is effective. This means that traffic is throttled in an aggregate manner irrespective of the distribution of the traffic in the upstream and downstream direction. The bidirectional throughput is represented in the license PID (For example, DNA-C-**500M**-E-3Y and DNA-C-**T2**-E-3Y). The aggregate throughput is double the bidirectional throughput. For more information, see Licenses and Licensing Models.
Programmability Features	
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.8.1a uses the YANG version 1.0; however, you can download the YANG version 1.1 from GitHub at https://github.com/YangModels/yang/tree/master/vendor/cisco/xefolder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG migration process, send an email to xe-yang-migration@cisco.com.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.8.x releases.

Table 2: 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 3: 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 17.8.1a

Identifier	Headline
CSCwb23043	MACsec not working on subinterfaces using dot1q >255.
CSCvz34380	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability.
CSCwa78020	ZBFW dropping packets as Input VPN ID set to 0 instead of 99.
CSCwa47219	Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table.
CSCwa13553	QFP core due to NAT scaling issue.
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum.
CSCwb11389	NAT translation stops suddenly(ip nat inside does not work).
CSCvz98373	ZBFW: FirewallPolicy drops seen with RTSP traffic in steady state.
CSCwa26412	ZBFW: OG lookups are missing from device for optimized policy.
CSCwa98047	SASE - after the device upgrade, umbrella dns config set to NONE in show umbrella config.
CSCvz91913	Bay 2 startup config of 40Gbps not applied on reload.
CSCvy78501	AAR not working properly as configured SLA classes are not shown under app-route stats.
CSCwa36699	Prefetch CRL download fails.
CSCvz74773	Discrepancies in CLI and GUI interface details (Truncating interface numbers)
CSCvx21819	Keychain macsec key input value 0 should be restricted.
CSCwa15085	Router Crash due to Stuck Thread with appnav-xe dual controller mode.
CSCwa07494	IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface.
CSCwa67398	NAT translations do not work for FTP traffic in the device.
CSCwa93930	The **alarms alarm bfd-state-change syslog** command is getting rejected while reconfiguring the device.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (ThousandEyes).
CSCwa92411	Slowness issues caused by intermittent traffic drop on device ingress from GRE tunnel.
CSCwa93668	FBD: flowdb entry double free during pperx pipeline collision.
CSCvz80101	Policy XML pruning without ConfD dependency.
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCvt15177	Certificate Signing Request made by IOS-XE never show the Subject Alternate Name

Identifier	Headline
CSCwa46760	Memory Utilisation value sent 0.6 always to vManage; shows wrong value 60%.

Open Bugs in Cisco IOS XE 17.8.1a

Identifier	Headline
CSCvz65764	Peer MSS value showing incorrect.
CSCwb18108	Device is unable to boot due to "TAM Status TAM_LIB_ERR_WRITE_FAILURE".
CSCwb23632	The command **show sdwan utd file reputation** incorrectly shows "Not connected to AMP cloud".
CSCwb40139	Device fails to load bootstrap configuration with '@' in the admin password.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading peer device.
CSCwa57254	Silent Reload due to CpuCatastrophicError.
CSCwb32635	Daemon file is incomplete when running admin-tech.
CSCwb11389	NAT translation stops suddenly(ip nat inside doesn't work).
CSCwb42807	After Enforce Software Version (ZTP) completed successfully, it automatically rolled-back.
CSCwb04815	NHRP process taking more CPU with ip nhrp redirect configured.
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post upgrade.
CSCwb43423	IOS XE image installation fails.
CSCwa64955	Device loses control connections after installing new enterprise hardware wan edge certerficate.
CSCwa49721	HUB with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map.
CSCwb18223	SNMP v2 community name encryption problem.
CSCwb16723	Traceroute not working with NAT.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwb27710	Critical process qfp_ucode_radium fault on fp_0_0 (rc=139).
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCwb27486	New Key for NBAR app and NBAR category without OGREF optimized.
CSCwa84919	"Revocation-check crl none" does not failover.

Identifier	Headline
CSCwb01477	Logging message "%IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'fman stats bipc'".
CSCvy23366	Kernel crash on device with UCSE module.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.
CSCvw50622	NHRP network resolution not working with link-local ipv6 address.
CSCwb29362	Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160.
CSCwa00293	QFP Crash due to SDWAN Flow-Exporter pending query.
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.

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.