Release Notes for Cisco Catalyst 8500 SeriesEdge Platforms, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-10-28

Last Modified: 2023-10-28

About Cisco Catalyst 8500 Series Edge Platforms

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

The Cisco Catalyst 8500 Series Edge Platforms includes the following models:

- C8500-12X4QC
- C8500-12X

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, refer the Cisco 8500 Series Catalyst Edge Platform datasheet.

Sections in this documentation apply to all models of unless a reference to a specific model is made explicitly.

Note Starting with Cisco IOS XE Amsterdam 17.3.2 release, 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).

New and Changed Hardware Features

New Hardware Features

> **Note** Cisco IOS XE Amsterdam 17.3.2 is the first release for Cisco Catalyst 8500 Series Edge Platforms.

The Cisco Catalyst 8500 Series Edge Platforms are available in these models:

- C8500-12X4QC
- C8500-12X

New and Changed Software Features in Cisco IOS XE 17.3.8a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

New and Changed Software Features in Cisco IOS XE 17.3.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.7

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.5

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.2

This section enlists the new and enhanced or modified features that are supported on the Cisco Catalyst 8500 Series Edge Platforms:

Table 1: Software Features

Feature	Description
Cisco DNA Center Support for Smart Licensing Using Policy	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is Cisco IOS XE 17.3.2.
	Implement the "Connected to CSSM Through a Controller" topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgement (RUM ACK).
	In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options.
	Cisco DNA Center also provides workflows for the installation and removal of the Smart Licensing Authorization Code (SLAC) for a product instance, if applicable.
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.
	Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem
	Minimum Required SSM On-Prem Version: Version 8, Release 202102
	Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3

Note On the Cisco DNA Center GUI, you can generate a SLAC only for HSECK9 licenses, and only for certain product instances. See the configuration guide for details

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the features, platform, and software image support on Cisco Catalyst 8500 Series Edge Platforms. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

ROMmon Release Requirements

Use the following tables to determine the ROMmon version required for your Catalyst 8500 model:

Table 2: Minimum and Recommended ROMmon Releases

	DRAM	Minimum Rommon	Recommended Rommon
C8500-12X4QC & C8500-12X	16GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	All variants	17.10(1r)	17.10(1r)
C8500L-8S4X	-	17.8(2r) - available from Cisco IOS XE 17.9.1a release	-
	-	17.10(1r)- available from Cisco IOS XE 17.10.1a release	-

Note In case of C8500L-8S4X platform, the ROMmon image is bundled with the Cisco IOS XE software image which ensures that when the device is booted up, the ROMmon image is also automatically upgraded to the recommended version.

Table 3: ROMmon Release per Platform

C8500-12X4QC & C8500-12X	17.2(1r)
	17.3(1r)
	17.11(1r)
C8500-20X6C	17.10(1r)
C8500L-8S4X	17.8(2r)
	17.10(1r)

Table 4: What's New in the ROMMon Release

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.3(1r)	Supports 64GB DRAM for C8500-12X4QC & C8500-12X
17.10 (1r)	Added support for new platform C8500-20X6C
17.11(1r)	Fixed a issue in data wipe feature

ROMmon Release for C8500L-8S4X	Fixes
17.10(1r)	CSCwa41877 - Fixes for Intel 2021.2 IPU
	CSCwb67177 - Fixes for Intel 2022.1 IPU
	CSCwb60723 - Fixes for CPU temperature
	CSCwb60863- Fixes for TAM_LIB_ERR_WRITE_FAILURE error

Resolved Caveats - Cisco IOS XE 17.3.8a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Caveats in Cisco IOS XE Amsterdam 17.3.8a

There are no open caveats in this release

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release

Open Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

There are no resolved caveats in this release.

Open Caveats in Cisco IOS XE Amsterdam 17.3.7

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwb23043	MACsec not working on subinterfaces using dot1q > 255 between devices.
CSCwc06967	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3.
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwc13013	IPSec Key Engine process holding memory continuously and not freeing up.
CSCwa17720	Device rebooted de to watchdogs after issuing the commands s**how crypto mib ipsec** commands.
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async.
CSCwb91026	Traffic is hitting wrong sequence in the data policy.
CSCwb25913	After configuring match input-interface on class-map, device goes into a reboot loop.
CSCwb04815	NHRP process taking more CPU with ip nhrp redirect configured.
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post cedge upgrade to 17.3.4.
CSCwb25137	NAT: Source address translation for multicast traffic fails with route-map.
CSCvy69405	Device Appnav-XE connections are going as passthrough unsupported .
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwa67398	NAT translations do not work for FTP traffic in the device.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes).
CSCwb24123	Registration of spoke fails with dissimilar capabilities w.r.t to HUB.
CSCvw16093	Secure key agent trace levels set to Noise by default.
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA

Identifier	Headline
CSCwb14020	Serial interface stuck in "line protocol is down" state after it went down and it is recovered.
CSCwb15331	Keyman memory leak using public keys.
CSCvy30606	catalyst 9800 fails to update sdn-network-infra-iwan key after 1 year
CSCwb76988	IKEv2 fragmentation causes wrong message ID used for EAP authentication.
CSCwb99793	CRL verification failure result 400 Bad Request with DigiCert
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwb95559	Packet Sanity failed for Resolution Reply on Spoke due to missing SMEF capability.
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN.

Open Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Headline
CSCwb72336	ICMP traceroute return packet not classified based on forward override port information.
CSCwa76570	Device crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut.
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.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCvy79601	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy configuration.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCvz53819	ZBFW : AR standby drops seen on Nnw active during RG switchover.
CSCvz63684	EWC Ha pair Expereincing IOS Tracebacks, followed by KEYMAN crash.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon
CSCwc25291	NIM-LTE-EA No Data - Requires Subslot reload to recover.

Identifier	Headline
CSCwb14888	Unable to remove "switchport mode access" and "switchport nonegotiate" at the same time.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwc39865	Subscriber Session getting stuck and needs clearing it manually.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface.
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp.
CSCwb46968	Device template attachment causes pppoe commands to be removed from ethernet interface.
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk.
CSCwa76260	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - DES, 3DES, DH1/2/5.
CSCvu77711	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCvv55742	GETVPN-ipv6 & LISP support on the device.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCvx28426	Router may crash due to Crypto IKMP process.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

There are no resolved caveats in IOS XE Amsterdam 17.3.5 release.

Open Caveats in IOS XE Amsterdam 17.3.5

There are no open caveats in IOS XE Amsterdam 17.3.5 release

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvv05682	C8500-12X4QC box crashed @ stile code with 17.3.1 FC1 image
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy

Caveat ID Number	Description
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvw05211	Pre-mature session deletion leading to churn and lower TPS at scale
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
CSCvw90220	Crash at #12 0x00007f010f4cb9db in cpp_bqs_rm_yoda_get_flush_obj while subscriber bringup
CSCvw92643	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel.
CSCvw94434	BQS crash seen at cpp_qm_event_proc_defer_cb
CSCvw98579	BQS crash seen in 17.3 while bringing up 30k PPPOE sessions
CSCvx11702	C8500-12X4QC: Traffic drops on 10G interface with large packet size 9000bytes with High priority.
CSCvx23159	FW-4-ALERT_ON: (target:class)-():getting aggressive seen when no half open feature configed
CSCvx32670	Wrong reload reason reflected after a power outage.
CSCvx34623	SIT : IOS exception seen and ASR reboots when a netconf is issued to get interface details
CSCvx36146	DCHP offer frame getting dropped on cEdge ISR4431 due to Policy
CSCvx36205	Removing and Adding Bulk ACL leads to dataplane programming failure
CSCvx36763	Zone Based Firewall on cEdge router dropping web traffic with the reason Zone-pair without policy
CSCvx43798	SIT 17.5.1 02/01: Stby switch reloaded due to config mismatch during telemetry push from DNAC.
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx51664	For-us Icmp packets are collected by cflowd which against the data-policy
CSCvx53049	Crash when TPOOL is updating and 'wr mem' is issues at same time
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
CSCvx58099	C8500-12X4QC does not send logs to vManage when harddisk is not installed
CSCvx64640	Data plane VPLS traffic generating Control Word on all Label Switched Headers
CSCvx64846	"show sdwan policy service-path/tunnel-path" command cause device crash

Caveat ID Number	Description
CSCvx72682	[DMM/SLM test issue] CFM crash when using physical port, DMM/SLM doesn't work on EVC
CSCvx73741	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
CSCvx77203	[17.5] Router crashed when sending traffic through non-SDWAN interface with DIA NAT + debug enabled
CSCvx78215	An IOS XE device might crash at DoubleExceptionVector
CSCvx88246	Packets dropped due to firewall + data policy interop issue
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy06736	Config out of sync after upgrading to 17.4.1
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets
CSCvy32673	C8500-12X4QC /1hx-Interface doesn't come up when reboot/upgrade device with autoneg enabled on 10G SFP+ Port
CSCvy67720	[FNF] Need to force DTL read after PLU lookup in fnf_build_do_ipv4_fast

Open Caveats in IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin .

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvt83998	"install add file harddisk:" fails on C8500-12X/C8500-12X4QC .
CSCvt97326	ASR 1000: harddisk usage is always zero in "show platform resource" for consolidated platforms
CSCvv94743	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
CSCvw50512	C8500-12X/C8500-12X4QC: Factory-reset doesn't format harddisk in 16GB/32GB/64GB variants

Open Caveats in IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCvv05682	C8500-12X4QC box crashed @ stile code with 17.3.1 FC1 image
CSCvv28030	C8500-12X4QC: IQDFZ profile degraded by 8% after BLD_POLARIS_DEV_LATEST_20200801_051231
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvw87256	ASR 1000 cpp_cp_svr crash with frequent underlay route removal and tunnel source changed every 1 second
CSCvv06039	Activation fails Error on 4221 with Failed to check active partition info
CSCvx58099	C8500-12X4QC Chassis Type "MCP1GD" not allowed

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Guide for Access and Edge Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge Platforms