Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-17

Full Cisco Trademarks with Software License

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.

New and Changed Software Features

Note Cisco IOS XE Cupertino 17.7.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Cupertino 17.7.x release series.

Table 1: Software Features

Feature	Description
EVPN VPWS over Preferred Path Fallback Disable	This enhancement allows you to configure an EVPN-VPWS over a preferred path using SR-TE policy. The command **preferred-path segment-routing traffic-eng policy** includes the fallback disable option, which allows you to configure fallback behaviour.
Flexible NetFlow Support on BD-VIF	This feature introduces Flexible NetFlow (FNF) support on Bridge Domain Virtual IP Interfaces (BD-VIF). Flexible Netflow provides improved optimization and performance, enhanced security, and increased flexibility and scalability to the network. You can configure FNF on a BD-VIF using the **ip flow monitor** command.
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.
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.
Tunnel protection for IPIP with NAT-T	When you configure the tunnel protection on an IPIP tunnel, the NAT-T configuration on the IPsec tunnel works as expected. However, the incoming packets are not processed though the Internet Security Association and Key Management Protocol and IPsec Security Association are correctly generated. To ensure that the tunnel protection on the IPIP tunnel works seamlessly, configure the tunnel mode GRE IP on both endpoints.
Programmability Features	
Converting IOS Commands to XML	This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages.

Feature	Description
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 a 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 a 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 show command 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.
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.

Feature	Description
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
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)
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. Each tier represents a throughput level. Starting with the lowest throughput level, the available tiers on the Cisco Catalyst 8500 Edge Series Platforms are Tier 2 (T2), and Tier 3 (T3) on C8500L-8S4X T3 on C8500-12X and C8500-12X4QC 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.

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.

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 and Open Bugs for Cisco IOS XE 17.7.2

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE 17.7.2

Bug ID	Headline
CSCwa17720	Device rebooted due to watchdogs after issuing the commands sh crypto mib ipsec commands
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCwb03662	Device CDP/LLDP not working when 10GE interface enabled with MACsec
CSCvz59621	Device MKA Session not coming up on EVC
CSCwa76962	Overruns and performance issues observed with crypto configuration enabled on device

Bug ID	Headline
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 device
CSCwb23043	MACsec not working on subinterfaces using dot1q >255 between devices
CSCwa15085	Devices Crash due to Stuck Thread with appnav-xe dual controller mode.
CSCwa98144	Devices - no negotiation auto command changing to negotiation auto after reload
CSCwa80474	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - MD5, SHA1
CSCvx28426	Device may crash due to Crypto IKMP process
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 for Cisco IOS XE 17.7.2

Bug ID	Headline
CSCvz65764	Peer MSS value showing incorrect
CSCwb78228	Device rebooted unexpectedly with reason "LocalSoft"
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb78423	Excessive packet loss observed during DMVPN tunnel flapping
CSCwb66749	ack/seq number abnormal when configration ip nat inside/outside on VASI intereface
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored
CSCwb74821	yang-management process confd is not running
CSCwa13553	Device QFP core due to NAT scaling issue
CSCwb11389	NAT translation stops suddenly(ip nat inside doesn't work)
CSCwb51238	Router reload unexpectedly two times when enter netflow show command
CSCwb61073	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps
CSCwa66916	Device SCCP auto-configuration issues with multiple protocols
CSCvz94966	Device throughput drop of 10% from 17.3 to 17.6 Release
CSCvz89354	Device running 17.x.x Crashes Due to CPUHOG When Walking ciscoFlashMIB
CSCwb79141	Device UCODE Crash with mpass function
CSCwb08186	E1 R2 - dnis-digits cli not working
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm
CSCwb12647	Device crash for stuck threads in cpp on packet processing

Bug ID	Headline
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also
CSCwb41907	CPP uCode crash 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 in 4451-x
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
CSCwb46649	NAT translation dont show (or use) correct timeout value for an established TCP session
CSCwb68897	"Total output drops" counter in "show interface" on Port-channel doesn't 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
CSCwb79138	Device after the upgrade starts dropping GRE tunnel packets

Resolved and Open Bugs for Cisco IOS XE 17.7.1a

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE 17.7.1a

Bug ID	Headline
CSCvz98446	VG400 crashed when changing Debug Level
CSCvy38743	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on ISR1100X after reload
CSCvy27721	IOS-XE Router may experience unexpected reboot with X25 RBP
CSCwa10915	ASR 1000 PFRv3: Elephant flow will trigger performance monitor exporting more than 50% byte loss
CSCvy42216	"switchport trunk native vlan xx" gets removed when upgrading from 16.12.x to 17.3.3
CSCvy53885	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.
CSCvy08748	OSPF summary-address isn't generated though candidate exists
CSCvy99942	Netconf: Logging to syslog stops working in certain scenarios
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager
CSCvw16093	Secure key agent trace levels set to Noise by default
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
CSCvy93946	Removal of SHA-1 HMAC Impacting ability to SSH
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed
CSCvz58895	IOS-XE unable to export elliptic curve key
CSCvy22343	Crash after reapplying BGP/ attempt to initialize an initialized wavl tree
CSCvz84437	C8500L Unexpected reload due IPV6 UDP fragment header in VxLAN
CSCvy63983	vManage showing wrong interface status in GUI

Open Bugs for Cisco IOS XE 17.7.1a

Bug ID	Headline
CSCwa07494	IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface

Bug ID	Headline
CSCwa20814	Device hitting vulnerability CVE 2008-5161
CSCvz74322	"Shutdown" command visible in running config after reload of ASR 1002-HX
CSCwa46001	VRRP traffic sent while the device boots will congest the interface queue causing taildrops
CSCvz94966	ASR 1000 and C8500 throughput drop of 10% from 17.3 to 17.6 Release
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
CSCvz91913	C8500-12X4QC: Bay 2 startup config of 40Gbps not applied on reload
CSCvw06937	SNMv3 traps failing with initial configuration
CSCvz80012	C8500L as a border device fails to pass traffic in sda fabric - VxLAN GPE broken
CSCvz86580	Unable to remove the BGP neighbor statement through vManage template.
CSCvz20285	Image info not updated in packages.conf when upgrading in autonomous mode
CSCwa01804	Router ASR 1000 C8500 ucode crash with PPE DTL transfer error during IP reassembly
CSCwa10915	ASR 1000 PFRv3: Elephant flow will trigger performance monitor exporting more than 50% byte loss

ROMmon Release Requirements

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

DRAM	ROMmon version
16 GB(default)	17.2(1r)
32 GB	17.2(1r)
64 GB	17.3(2r)

Related Documentation

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

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.