Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.1a

Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.1a

Cisco 17.18.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.18.x release series.

The key highlights of this release include these features and enhancements:

● Monitoring & Observability

● Cellular, IPv6, Voice, Virtualization

● SRv6 Enhancements

● Security and SASE enhancements

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1.   New software features for Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Hosted Edge Services for SD-Routing Devices	From Cisco IOS XE 17.18.1a release, Cisco Catalyst SD-WAN Manager supports deployment of IOx applications such as Cyber Vision, Thousand Eyes, UTD, and so on. The support to monitor these applications is introduced through Hosted Edge Services monitoring dashboard which offers a simplified user experience for overseeing IOx container applications across multiple devices. The Hosted Edge Services monitoring dashboard is introduced on Cisco Catalyst SD-WAN Manager version 20.18.x.
Ease of setup	Cisco Secure Routers Swim and Onboarding Tool	Cisco IOS XE 17.18.1a introduces the Cisco Secure Routers Swim and Onboarding tool that helps customers upgrade and onboard autonomous hardware devices to cloud-hosted or on-premises Catalyst Cisco SD-WAN Manager.
Licensing Process	Licensing compliance, reporting, and notification enhancements	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Licensing Process	Product Analytics for routers	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when you start your router. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of use	Managing NGFW Policies from Security Cloud Control	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this integration, you can share objects and policies as well as make

Product impact	Feature	Description
		configuration templates to promote policy consistency across devices.
Security	Custom IPS signature sets	From Cisco IOS XE 17.18.1a release, Custom IPS signature sets are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets.This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	Certificate Management on SD-Routing Devices	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Upgrade	MVPN Ingress Replication (IR) over SRv6	This feature enables the transport of IPv4 Multicast traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	SRv6 Path MTU Discovery	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.
Upgrade	SRv6 Flex-Algo with TI-LFA and uLoop Avoidance	From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Licensing Process	Product Analytics for routers	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of Use	MAP-T Border Router (BR) Enhancements	The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Table 2.   Resolved issues for Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.1a

Bug ID	Description
CSCwn12594	17.16 SIG zscaler ipsec - vpn credentials for primary tunnel not created
CSCwn42496	SDWAN-SIT: Encore crashed @bfd_send_and_detect_sleep_time during soak run
CSCwn69868	Unable to come up control connections with Controllers after Controllers added and down/up
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
CSCwo84428	cEdge: Memory leak under vdaemon process with DTLS on SNMP polling
CSCwp07901	C8500 : CPP crash while processing fragments of a jumbo frame
CSCwp24639	Device reload after vpn config changes on SDWAN
CSCwm27749	Speed test download / Throughput issue on C8200 platform seen with IPSEC ESP-NULL transform using Zscaler
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
CSCwo05703	SD-WAN: VFR is not Dynamically Disables After ZBFW Removal
CSCwo75657	Maximum control connection not equal to maximum omp sessions - cEdge
CSCwp91064	FTMD cero pointer dereference leading to crash
CSCwo18836	Transition Fugazi/C8500L from FBD to NSFBD

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 3.   Open issues for Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.1a

Bug ID	Description
CSCwp12196	cEdge router unexpectedly reloads due to memory corruption on a notification queue in FTMd
CSCwq27426	cEdge: BFD session down due to unencrypted outbound BFD packets despite active IPsec SA

Bug ID	Description
CSCwe19394	cEdge: device may boot up into prev_packages.conf due to power outage
CSCwo42664	17.12 - keyman core files on cEdge
CSCwo66099	SDWAN cEdge Service Side BFD flaps
CSCwp01089	EPFR-High latency times are observed on the hub device (Cisco Catalyst 8500-12X Edge Platform).
CSCwp81539	cEdge: Memory leak under cfgmgr process on SNMP polling
CSCwq20326	Behavior change for OMP and CEF may require network redesign if internal site prefixes overlap
CSCwq40026	Unexpected Reboot due to Process FTMD
CSCwq68385	TLOC Disabled After Link Down—No Automatic Tunnel Recovery After Link Restores and TLOC State Is Up

Compatibility

ROMmon release requirements

This section lists the ROMmon version required for your Catalyst 8500 model:

Table 4. Compatibility information for Catalyst 8500 Edge Platform, Release 17.18.1a

Platforms	DRAM	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8500-12X4QC and C8500-12X	16 GB(default)	17.2(1r)	17.11(1r)
	16 GB(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		17.10(1r)	17.14(1r)

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.

What's new in the ROMmon Release

This section lists changes in the ROMmon package

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 data issue in data wipe feature.
CSCwq68385	TLOC Disabled After Link Down–No Automatic Tunnel Recovery After Link Restores and TLOC State Is Up

ROMmon Release for C8500-12X4QC, C8500L-8S4X	Fixes
17.14(1r)	CSCwf98337 - Evaluation of C8500L-8S4X for Intel 2023.3 IPU and SMRAM vulnerabilities CSCwe21026 - Evaluation of C8500L-8S4X for Intel 2023.1 IPU and SMM vulnerabilities

Upgrade ROMmon

To upgrade the ROMmon version of your device, use these steps:

1. Check the existing version of ROMmon by using show rom-monitor r0 command. If you are installing Cisco IOS XE software on a new device, skip this step.

2. Review Minimum and Recommended ROMmon Releases to identify the recommended version of ROMmon software for the device you plan to upgrade.

3. Go to https://software.cisco.com/# and download the ROMmon package file.

4. Copy the ROMmon file to flash drive:

5. copy ftp:// username:password@IP addressROMmon package file flash:

6. Upgrade the ROMmon package using the following command:

7. upgrade rom-monitor filename bootflash: ROMmon package name all

8. Execute reload command to complete the ROMmon upgrade process

9. Execute show rom-monitor r0 command to ensure the ROMmon software is upgraded.

Related resources

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge Platforms

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.