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

Contents

Catalyst 8500 Edge Platform, 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.

New software features in Cisco IOS XE 17.18.2

Product impact	Feature	Description
Ease of Setup	XXXX	From Cisco IOS XE 17.18.2, you can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager .
Upgrade	IPv6 GRE-TP tunnel as protected link support for SRv6 TI-LFA with IS-IS	From Cisco IOS XE 17.18.2, this feature extends IPv6 GRE-TP tunnel as protected link support for SRv6 TILFA with ISIS.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with OSPF	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPF.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with IS-IS	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with ISIS.
Security	Infrastructure Resiliency	Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives. This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release: • **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in

Product impact	Feature	Description
		configuration files. *Recommendation*: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials. • **SSHv1** *Recommendation*: Use SSHv2. • **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption** *Recommendation*: Use SNMPv3 with authentication and encryption (authPriv). • **MD5 (authentication) and 3DES (encryption) in SNMPv3** *Recommendation*: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption. • **IP source routing based on IP header options** *Recommendation*: Do not use this legacy feature. • **TLS 1.0 and TLS 1.1** *Recommendation*: Use TLS 1.2 or later. • **TLS ciphers using SHA1 for digital signatures** *Recommendation*: Use ciphers with SHA256 or stronger digital signatures. • **HTTP** *Recommendation*: Use HTTPS. • **Telnet** *Recommendation*: Use SSH for remote access. • **FTP and TFTP** *Recommendation*: Use SFTP or HTTPS for file transfers. • **On-Demand Routing (ODR)** *Recommendation*: Use a standard routing protocol in place of CDP-based routing information exchange. • **BootP server** *Recommendation*: Use DHCP or secure boot features such as Secure ZTP.

Product impact	Feature	Description
		• **TCP and UDP small servers (echo, chargen, discard, daytime)** *Recommendation*: Do not use these services on network devices. • **IP finger** *Recommendation*: Do not use this protocol on network devices. • **NTP control messages** *Recommendation*: Do not use this feature. • **TACACS+ using pre-shared keys and MD5** *Recommendation*: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1

New software features in Cisco IOS XE 17.18.1

Table 1. New software features for Catalyst 8500 Edge Platform, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Hosted Edge Services for SD-Routing Devices	Cisco IOS XE 17.18.1a introduces Hosted Edge Services, a new monitoring feature which enables direct management of Cisco IOx applications installed on your SD-Routing edge devices. This feature delivers improved functionalities like tracking resource usage, starting or stopping Cisco IOx applications at a scale directly through Cisco Catalyst SD-WAN Manager.
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).
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 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

Product impact	Feature	Description
		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 MVPN 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 17.17.1a, 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.

Resolved issues in Cisco IOS XE 17.18.2

Table 2. Resolved issues for Cisco 8400 Edge Platform, Release 17.18.2

Bug ID	Description
CSCwr42950	SDWAN On-Demand Tunnels Do Not Expire When UMTS Is Enabled
CSCwq51935	NAT64 static entry removed when command to delete non-existent entry is applied.
CSCwe19394	cEdge: device may boot up into prev_packages.conf due to power outage

CSCwr77958	NWPI not capturing self-generated syslog traffic
CSCwj61730	Cat8500L crash when removing SGT caching on an interface
CSCwq77322	C8500-12X sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet
CSCwr24031	After upgrade to 17.15 for earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured
CSCwr49794	ISR exporters with ETA enabled are generating invalid template data errors in SNA
CSCwq98206	EPBR set interface action get missing after reboot
CSCwr25077	vDaemon crash when initializing DNS channels

Resolved issues in Cisco IOS XE 17.18.1

Table 3. Resolved issues for Catalyst 8500 Edge Platform, 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	[SITLite]: 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

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.

Open issues in Cisco IOS XE 17.18.2

Table 4. Open issues for Catalyst 8500 Edge Platform, Release 17.18.1a

Bug ID	Description
CSCws30834	cedge ignore the keepalive command under the SIG tunnel interface pushed by the vmanage
CSCws13857	Incorrect NAT translation from service-vrf to global for self-generated ICMP 11 (Time Exceeded) packets
CSCwq77458	fman crash after fnf config changes
CSCwr87083	C11xx: Not able to onboard sd-routing devices using generic bootstrap file stored in usb
CSCws12946	Cedge port forward issue with multiple ISP

Bug ID	Description
CSCws18137	Out of sync when CLI Template was attached (missing element: authentication in /ios:native/ios:line/ios:vty[ios:first='0']/ios:login/ios:authentication)
CSCwr76580	strange behavior with the Cisco Umbrella SIG tunnels configured from vManage to Umbrella.
CSCwr30573	TLOC Extension unable to program due to module boot up timing
CSCws25557	Cipher Suites TLS 1.2 for control connections
CSCwr95551	Router crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT
CSCwr08462	[C8500L-8S4X] There seems to be an issue where the NAT router is not responding to ARP requests
CSCwr44921	SDWAN C-Edge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold
CSCwr97784	Slow performance on Netconf RPC on 17.15.2a on stateless static NAT translation
CSCwr88206	FIB table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole
CSCwr84985	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
CSCwq24119	IR1835: Traceback seen when detaching the CN railways customer configs in 17.19
CSCwm97460	17.9 cEdges - Control Connection to vManage is only Attempted over Highest Priority TLOC
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwr55240	C8000v experienced Critical process ompd fault on rp_0_0
CSCwr72709	Router crash in TDM-TDM call when debug voip fpi enabled
CSCwq98154	[XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwr49475	BFD sessions flapping and not recovering - SYMNAT port not updating to data-plane
CSCwo42664	SD-WAN Edge: Periodic Service Restart May Generate Crash Files
CSCwr64257	Unexpected reload on ftmd SDWAN device
CSCws26373	cEdge experiences an unexpected reboot due to NAT in the data-plane after a policy push
CSCwp97178	v1718/polaris: flapping nat will casue bfd session down with ipsec session shown
CSCwr76176	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCwr77083	C8000v crashed in crypto library

Table 5. Open issues for Catalyst 8500 Edge Platform, 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
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	cEdge does not install service-side static route to CEF after upgrade
CSCwq40026	Unexpected Reboot due to Process FTMD

ROMmon release requirements

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

Table 6. Compatibility information for Catalyst 8500 Edge Platform, Release 17.18.1a

	DRAM	Minimum ROMmon	Recommended ROMmon
C8500-12X4QC and C8500-12X	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.

ROMmon ROMmon Release for 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:

   copy ftp:// *username:password@IP addressROMmon package file* **flash**:
5. Upgrade the ROMmon package using the following command:

   upgrade rom-monitor filename bootflash: *ROMmon package name* **all**
6. Execute **reload** command to complete the ROMmon upgrade process
7. 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