Release Notes for Cisco 8300 Series Secure Routers, Release 17.18.x

Contents

Cisco 8300 Series Secure Routers, Release 17.18.x

Cisco 17.18.1a is the first release for Cisco 8300 Series Secure Routers 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

For information on the hardware features supported on the Cisco 8300 Series Secure Routers, refer to the Cisco 8300 Series Secure Routers datasheet.

New software features

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

New software features for Cisco IOS XE 17.18.1a

Table 1. New software features for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Support to upgrade Firmware	From Cisco IOS XE 17.18.1a release, you can now upgrade the firmware image for cellular module, LTE module, or Wi-Fi module of supported devices using Cisco Catalyst SD-WAN Manager, without configuring and managing multiple commands for each device and its associated modules.
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).
Ease of use	Managing NGFW	Security Cloud Control (SCC) is a cloud-based multi-device manager that

Product impact	Feature	Description
	Policies from Security Cloud Control	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 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.
Ease of use	Configure cellular band select for cellular interfaces on SD-Routing devices	You can select specific frequency bands to which the device can connect to, allowing optimized connection depending on location and network availability. This configuration can be done using Feature Parcels in Catalyst Cisco SD-WAN Manager.
Ease of use	Configure logging of crash dump events for cellular interfaces on SD-Routing devices	You can configure the device to collect the crash dump logs by enabling the boot-and-hold mode on the device using the lte modem crash-action boot-and-hold command.
Ease of use	Reset cellular profile for cellular interfaces on SD-Routing devices	You can reset the cellular network profile settings on a specific interface to a factory default state using the cellular<slot> lte profile reset command.
Ease of use	Enable diagnostic monitoring for SD-Routing devices	You can enable diagnostic monitoring log capture for devices with cellular interfaces using Catalyst Cisco SD-WAN Manager.
Ease of Use	Show drops command	The *show drops* command is introduced in Cisco IOS XE 17.18.1a. This command consolidates multiple platform and protocol-specific debugging tools into a single, user-friendly interface, enabling network operators to efficiently identify the root causes of packet drops. By streamlining the troubleshooting process, this feature significantly improves operational efficiency and network performance.
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

Product impact	Feature	Description
		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	Crypto Throughput Logging	Starting with Cisco IOS XE 17.18.1a, network administrators can monitor and manage crypto throughput drops on Cisco Catalyst 8300 and Catalyst 8200 Series Edge Platforms. This feature sends syslog messages to notify you when crypto throughput drops, offering better visibility and management.
CUBE Features		
Ease of use	Enhanced support for serviceability in SIP recording	From Cisco IOS XE 17.18.1a onwards, serviceability is enhanced to display consolidated information on forked and associated anchor call legs.
Upgrade	Third-Party GUID capture for correlation between call transfers and SIP-based recording	From Cisco IOS XE 17.18.1a onwards, the Third-Party GUID capture for correlation between calls and SIP-based recording is extended to support transmission of globally unique identifiers (GUIDs) to the recording server during call transfers.
Upgrade	IOS UC apps reports smart licensing flex subscription entitlement tag	From Cisco IOS XE 17.18.1a onwards, CUBE and SRST smart licensing reports flex subscription entitlement tag on all the supported platforms.

Resolved issues

This table lists the resolved 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. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Resolved issues in Cisco IOS XE 17.18.1a

Table 2. Resolved issues for Cisco 8300 Series Secure Routers, Release 17.18.1a

Bug ID	Description
CSCwo05703	VFR is not dynamically disabled after ZBFW removal.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically

Bug ID	Description
	changed.
CSCwo84428	Memory leak under vdaemon process with DTLS on SNMP polling.
CSCwm27749	Speed test download / Throughput issue on device seen with IPSEC ESP-NULL transform using Zscaler.
CSCwo75657	Maximum control connection not equal to maximum omp sessions.
CSCwp15042	Module stays down without hw slot reload.
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole.
CSCwn69868	Unable to come up control connections with controllers after controllers added and down/up.
CSCwp24639	Devices reload after vpn config changes.
CSCwn42496	Encore crashed @bfd_send_and_detect_sleep_time during soak run.
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
CSCwp91064	FTMD cero pointer deference 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. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Open issues in Cisco IOS XE 17.18.1a

Table 3. Open issues for Cisco 8300 Series Secure Routers, Release 17.18.1a

Bug ID	Description
CSCwq40026	Unexpected Reboot due to Process FTMD.
CSCwq20326	Device does not install service-side static route to CEF after upgrade.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage.
CSCwo42664	Keyman core files on device.
CSCwp01089	EPFR-High latency times are observed on the hub device.

Bug ID	Description
CSCwp12196	Device unexpectedly reloads due to memory corruption on a notification queue in FTMd.
CSCwq27426	BFD session down due to unencrypted outbound BFD packets despite active IPsec SA.
CSCwq68385	TLOC Disabled After Link Down- No Automatic Tunnel Recovery After Link Restores and TLOC State Is Up.

Compatibility

ROMMON compatibility matrix

The table lists the ROMMON releases supported in Cisco IOS XE 17.18.x releases.

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8375-E-G2	17.18.1a	17.15(3.2r)	Not applicable

Related resources

- Hardware Installation Guide for Cisco 8300 Series Secure routers
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco 8300 Series Secure Routers Software Configuration Guide

Legal information