Release Notes for Cisco Catalyst 8400 Series Secure Routers, 17.18.1a

Contents

Catalyst 8400 Series Secure Routers, Release 17.18.1a

Cisco 17.18.1a is the first release for Cisco Catalyst 8400 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
- 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 Catalyst 8400 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.
C8400 Series Secure Routers Licensing	C8000 Series Secure Routers Licensing	C8400 Series Secure Routers supports platform-based licensing, a way of grouping licenses and devices based on platform-classes. A platform class is a hierarchical categorization based on the product family and place in the network. In this platform-based licensing model, Essentials and Advantage licenses are available. License portability is supported across devices within the same platform class and usage of the same license across different modes is also possible.
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 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

Product impact	Feature	Description
		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.
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 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

Product impact	Feature	Description
		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.
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.
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 Catalyst 8400 Edge Platform, Release 17.18.1a

Bug ID	Description
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
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
CSCwm72336	CXP with Data Policy redirect-DNS via overlay causes blackhole
CSCwp91064	FTMD cero pointer dereference leading to crash
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
CSCwm27749	Speed test download / Throughput issue on C8200 platform seen with IPSEC ESP-NULL transform using Zscaler
CSCwo75657	Maximum control connection not equal to maximum omp sessions - cEdge
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole
CSCwp91064	FTMD cero pointer dereference leading to crash
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.

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

Table 3. Open issues for Catalyst 8400 Edge Platform, Release 17.18.1a

Bug ID	Description
CSCwp01089	EPFR-High latency times are observed on the hub device
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
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwq40026	Unexpected Reboot due to Process FTMD
CSCwp01089	EPFR-High latency times are observed on the hub device (Cisco Catalyst 8500-12X Edge Platform).
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
CSCwq40026	Unexpected Reboot due to Process FTMD

Related resources

- Hardware Installation Guide for Cisco 8400 Series Secure Routers
- Software Configuration Guide for Cisco 8400 Series Secure Routers
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms

.

Legal information