



Release Notes for Cisco Catalyst 8000V, Release 17.18.x



Cisco Catalyst 8000V Edge Software, Release 17.18.1a..... 3

New software features 3

Resolved issues 5

Open issues..... 6

Related resources 7

Legal information 7

Cisco Catalyst 8000V Edge Software, Release 17.18.1a

Cisco IOS XE 17.18.1a is the first release for Cisco Catalyst 8000V Edge Software in the Cisco IOS XE 17.18.x release series.

The key highlights of this release include:

- Support for deployments in Oracle Cloud Infrastructure
- Support for N4 and N2 compute instance families in Google cloud Platform (GCP)
- Support for D[s]_v5 compute instance family in Microsoft Azure
- Support for SR-IOV connectivity with Nvidia Mellanox ConnectX-6 NICs for on-premise deployments
- Support for Ubuntu 22.04 LTS
- Hosted Edge Services manages Cisco IOx applications
- Certificate Management unifies device certificates
- MVPN Ingress Replication over SRv6 simplifies multicast
- SRv6 Path MTU Discovery prevents fragmentation
- SRv6 Flex-Algo improves network resilience

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 8000V Edge Software, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Support for deployment of Catalyst 8000V in Oracle Cloud Infrastructure	<p>Oracle Cloud Infrastructure (OCI) is a cloud service that enables you to build and run a range of applications and services in a hosted environment. OCI provides high-performance compute capabilities as physical hardware instances and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network.</p> <p>From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V is supported for deployments in OCI on VM.Standard.E5.Flex compute instances for Bring Your Own License (BYOL) consumption.</p>
Ease of Use	Support for N4 and N2 compute instance families in Google cloud Platform	Cisco Catalyst 8000V supports the N2 compute instance family as well as the N4 compute instance family with gVNIC driver support for Google Cloud Platform (GCP) deployment.
Ease of Use	Support for D[s]_v5 compute instance family in Microsoft Azure	Cisco Catalyst 8000V supports the D[s]_v5 compute instance family for Microsoft Azure deployments from Cisco IOS XE 17.18.1a release.
Software Reliability	Support for Nvidia Mellanox ConnectX-6 network interface	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V supports the Nvidia Mellanox ConnectX-6 Network Interface Cards (NICs) with port speeds of up to 40 GbE. Also, the supported VNIC drivers for SR-IOV

Product impact	Feature	Description
	cards	connectivity is expanded to include CX6VF.
Ease of Use	Support for Ubuntu 22.04 LTS	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V supports Ubuntu 22.04 LTS version open-source OS on Linux.
Software Reliability	Throughput performance optimizations	From Cisco IOS XE 17.18.1a release, Cisco Catalyst 8000V delivers higher throughputs for both encrypted and unencrypted traffic. We recommend you benchmark your unique traffic profiles prior to production. The performance improvements will depend on your feature set, packet sizes, and the number of vCPU cores.
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	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 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 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.

Product impact	Feature	Description
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.
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.
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.
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 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 8000V Edge Software, Release 17.18.1a

Bug ID	Description
CSCwn42496	Devices lose all BFD sessions while control connections remain up

Bug ID	Description
CSCwn69868	Unable to come up with 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	Memory leak under vdaemon process with DTLS on SNMP polling
CSCwp24639	Device reloads after VPN configuration changes
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	VFR is not dynamically disabled after ZBFW removal
CSCwo75657	Maximum control connection is not equal to maximum OMP sessions
CSCwp91064	FTMD zero pointer dereference is seen 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.

Table 3. Open issues for Cisco Catalyst 8000V Edge Software, Release 17.18.1a

Bug ID	Description
CSCwp12196	Router 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
CSCwo42664	Keyman core files on device
CSCwp01089	EPFR-High latency times are observed on the hub device
CSCwp81539	Memory leak under cfgmgr process on SNMP polling
CSCwq20326	Device does not install service-side static route to CEF after upgrade
CSCwq40026	Unexpected reboot occurs due to Process FTMD
CSCwq68385	TLOC disabled after link is down; no automatic tunnel recovery after link restores and TLOC state is Up

Related resources

- [Cisco Catalyst 8000V Edge Software Product Page](#)
- [Cisco Catalyst 8000V Edge Software Data Sheet](#)
- [Cisco Catalyst 8000V Edge Software Installation And Configuration Guide](#)
- [Cisco Catalyst 8000V Edge Software High Availability Configuration Guide](#)
- [Troubleshooting Guide for Cisco Catalyst 8000V Edge Software](#)
- [Configure Licenses and Throughput for Cisco Catalyst 8000V Edge Software](#)

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.