Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE 17.15.x

First Published: 2024-08-27

Full Cisco Trademarks with Software License

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

About The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note Sections in this documentation apply to all models of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

Note Cisco IOS XE 17.15.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE 17.15.x release series.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Changed Hardware and Software Features

There are no new hardware features in this release.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.

✎

Note To access CFN, you do not require an account on cisco.com.

New and Changed Hardware Features

There are no new hardware features in this release.

New and Changed Hardware Features

There are no new hardware features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.1a

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms

Feature	Description
Absolute Path for HTTP or HTTPS File Transfer	The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the **copy** command.
Cisco Umbrella Scope Credentials	From Cisco IOS XE 17.15.1a, this feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.
Enhanced NAT Management	From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the **ip nat translation max-entries cpu** command. This feature also enables streamlining NAT synchronization in redundant systems using the **ip nat settings redundancy optimized-data-sync** command.

Feature	Description
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.15.1a, Segment Routing over IPv6 dataplane supports these functionalities: • IS-IS Microloop Avoidance • IS-IS Loop-Free Alternate Fast Reroute • IS-IS Topology-Independent Loop-Free Alternate Fast Reroute • OAM Traffic Engineering
Flexible Gigabit Ethernet and Fibre Channel Services	Cisco Coarse Wavelength-Division Multiplexing (CWDM) Small Form-Factor Pluggable (SFP) solution allows you to deploy scalable Gigabit Ethernet and Fibre Channel services efficiently. These hot-swappable transceivers convert electrical signals into single-mode fiber-optic interfaces and can be connected to CWDM passive optical systems using standard SC connectors
SD-Routing License Management	This release introduces license management support for SD-Routing devices. The supported licensing workflows include license assignment or configuration, license use, and license usage reporting. Depending on the device, these workflows are performed in the Cisco Catalyst SD-WAN Manager or on the device.
Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF	You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic.
Monitoring SD-Routing Alarms	From Cisco IOS XE 17.15.1a, network administrators can monitor SD-Routing device alarms on Cisco Catalyst SD-WAN Manager. This feature enables SD-Routing devices to record and store various alarms generated by control components and routers. For more information, see Cisco SD-Routing Command Reference Guide.
Network-Wide Path Insights on SD-Routing Devices	Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network.

Feature	Description
Configure DMVPN for SD-Routing Devices	Cisco DMVPN (Dynamic Multipoint VPN) is a routing technique to build a VPN network with multiple sites without having to statically configure all devices. This technique uses tunnelling protocols and encrypted security measures to create virtual connections, or tunnels, between sites. These tunnels are dynamically created as needed, making them both efficient and cost-effective.
Enabling Flow Level Flexible NetFlow Support for SD-Routing Devices	The Flow-level Flexible NetFlow (FNF) feature allows you to monitor the NetFlow traffic and view all the flow-level FNF data that is captured including application-level statistics.
Seamless Software Upgrade for SD-Routing Devices	This feature explains how to seamlessly upgrade and onboard an existing Cisco Routing device into the Cisco SD-WAN infrastructure.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.15.x releases.

Table 2: Minimum and Recommended ROMMON Releases Supported on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

Platforms	Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X|6T	17.15.1a	17.3(4.2r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.15.1a	17.3(4.1r)	17.7(1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)
C8200L-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)

Note For Cisco Catalyst 8200 and 8200L Series Edge platforms, if your ROMMON is at a version lower than 17.6(8.1r), you can upgrade the device to IOS XE 17.15.1a using any of the following methods:

- in bundle mode, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a, OR

- in bundle mode, manually upgrade the ROMMON to 17.6(8.1r). You can then upgrade the device to 17.15.1a.

- in install mode, you can upgrade the device to IOS XE 17.15.1a; the ROMMOM is auto-upgraded to the recommended version when the device boots.

For Cisco Catalyst 8300 Series Edge platforms, if your ROMMON is at a version lower than the minimum supported version, manually upgrade the device to Cisco IOS XE 17.12.4. This will auto-upgrade the ROMMON to the recommended version. You can then upgrade the device to 17.15.1a.

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 ROMMON Compatibility Matrix 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 address_*ROMmon 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.

Resolved and Open Bugs for Cisco IOS XE 17.15.1a

Resolved Bugs in Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwj51700	CPP crashes after re-/configuring **ip nat settings pap limit ... bpa** feature in high QFP state.
CSCwk03686	Crash due a segmentation fault due a negative value.
CSCwk42634	%PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6).

Identifier	Headline
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk16333	Device repeatedly crashing in FTMd due to FNF flow add.
CSCwj96852	Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC.
CSCwj95633	SAIE application - no data to display for IOS XE router.
CSCwk39131	Device crashed when issuing **show sdwan ftm next-hop chain all**.
CSCwk37351	IOS XE router: unexpected reboot during PVDM OIR.
CSCwk22225	FTMd crashes after receiving credentials feature template update.
CSCwj48909	Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk23723	Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwk45165	fman_fp memory leak on device.
CSCwj16153	10G front-panel port does not go down on single mode fiber when Rx side goes down.
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup.
CSCwj90614	High CPU utilisation for confd_cli.
CSCwi81026	BFD sessions flapping during IPSec rekey in scaled environment.
CSCwk39268	sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11.
CSCwj76662	High memory utilization due to "ftmd" process.
CSCwj92560	STCAPP command removed from device after reload.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk44078	GETVPN / migrating to new KEK RSA key does not trigger GM re-registration.
CSCwi99454	FNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.

Identifier	Headline
CSCwj96092	ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	Device unexpectedly reloads due to a crash in 'vdaemon' process.
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492.
CSCwj02401	Router reloaded when generating admin tech while processing very high number of flows.
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwk19725	add FNF cache limit for show sdwan app-fwd flows.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwj67591	Chassis activate effective only after second re-try - with new uuid.
CSCwj32347	DIA endpoint tracker not working with ECMP routes.
CSCwj41728	Unable to install the TE agent using http link in CLI

Open Bugs in Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwi76516	esim cellular configuration tamplate deployemt fails.
CSCwk75733	Custom applications may not be programmed properly.
CSCwk89256	Speed mismatch in IOS-XE configuration after device template push.
CSCwm07994	Router crash with stuck threads.
CSCwk85704	**match traffic-category** add-on CLI push failed.
CSCwj01917	After upgrade, cellular interface IP ADDRESS NEGOTIATED mismatching.
CSCwm01269	Speed test is giving better result from TLOC extension from the secondary router.
CSCwj76689	Device configuration lost after .bin upgrade.
CSCwk86355	File transfer fails: "lost connection".
CSCwk49806	Router rebooted unexpectedly due to process NHRP crash.
CSCwk81360	Router can reboot unexpectedly while configuring NAT static translation.
CSCwk62954	Multiple "match address local interface <int>" not pushed under crypto profile.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk97092	MKA session not coming up after shut/no shut with EVC.

Identifier	Headline
CSCwm07564	data-policy local-tloc-list breaks RTP media stream.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered.
CSCwk74298	Device denied for template push and some show commands with error application communication failure.
CSCwk98578	GETVPN IPv6 crypto map not shown in interface configuration.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwk70630	Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded.
CSCwm13223	Device crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog.
CSCwk79454	Endpoint tracker does not fail if default route is removed.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.
CSCwi87546	Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - lock id of 0 released.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwm12851	Device uses 3DES as default rekey algorithm for GETVPN.
CSCwk95044	SPA.smu.bin drops when packet duplication link fails-over.
CSCwj87028	Device showing custom APP as "unknown" for egress traffic when using DRE Opt.
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwm08545	Centralized policy policer worked per PC on the same site not per site/vpn-list.
CSCwf62943	System image file is not set to packages.conf when image expansion fails due to disk space.
CSCwm00309	Packets not hitting the correct data policy after modifying the action of a sequence.

Related Documentation

- Hardware Installation Guide for Catalyst 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.