Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-06

Last Modified: 2023-10-16

Full Cisco Trademarks with Software License

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 Dublin 17.11.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Dublin 17.11.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

New and Changed Hardware Features

Table 1: New Hardware in Cisco IOS XE 17.11.1a

Hardware	Description
Cisco UCS E-Series M6 Servers	Cisco UCS E-Series M6 Servers bring data center-class blade servers to the branch office. These powerful, small form-factor, x86 64-bit blade servers reside in Cisco Catalyst 8300 Series Edge platforms.
Cisco C-NIM-4X and C-NIM-8T	The Cisco C-NIM-4X and C-NIM-8T are the next generation LAN/WAN NIM modules that provide enhanced security, reliability, and performance. The Cisco C-NIM-4X module provides Small Form-Factor Pluggable (SFP) /Small Form-Factor Pluggable Plus (SFP+), 10G and 1 Gigabit connectivity and the Cisco C-NIM-8T moduel provides 1 Gigabit RJ45 connectivity to the Cisco Catalyst 8200 and 8300 Series Edge Platforms. Also, Cisco C-NIM-4X and C-NIM-8T supports Layer 2 and Layer 3 configurable ethernet NIM module.

New and Changed Software Features

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 http://www.cisco.com/go/cfn.

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

New Software Features

Table 2: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms IOS XE Dublin 17.11.1a

Feature	Description
Attaching Extended Color Communities to BGP VRF	This feature introduces new methods of attaching extended color communities to a prefix. A color community is an indicator of the bandwidth or latency level of the traffic sent to the prefix. You can attach the extended color communities to the prefix in the following ways: VRF export coloring, VRF import coloring, Route Redistribution coloring into BGP and Neighbor inbound coloring.

Feature	Description
Configure DHCP in a VPN-SIP Solution	From Cisco IOS XE 17.11.1, you can install and enable a Session Initiation Protocol Triggered VPN (VPN-SIP) router behind a home gateway. In this installation, the home gateway assigns an extension number to the tunnel interface through Dynamic Host Configuration Protocol (DHCP) instead of a fixed telephone number. This allows you to aggregate data and voice on your network and share the same physical subscriber line for both analog and digital data.
Device Telemetry	This functionality enables collection of anonymous usage telemetry data for Cisco products, which helps in continuous product improvements. From Cisco IOS XE 17.11.1a, this functionality is enabled by default.
Deprecation of Weak Ciphers	The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.
Enabling the RSRP and RSRQ Parameters for Link Recovery on LTE Modems	This feature enables the RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) parameters that detect any network issues or malfunctions as part of the link-recovery feature on LTE modems.To enable these parameters, the user can configure the **lte modem link-recovery rsrp onset-threshold** command for RSRP and **lte modem link-recovery rsrq onset-threshold** command for RSRQ.
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This feature implements RFC 8784 and Cisco Secure Key Integration Protocol (SKIP) for quantum-safe encryption of IKEv2 and IPsec packets using Post-quantum Preshared Key (PPK). The PPKs configured manually are referred to as manual PPKs and the PPKs imported from an external key source (KS) using the SKIP protocol are referred to as dynamic PPKs.This feature is applicable to all IKEv2/IPsec VPNs such as FlexVPN (SVTI-DVTI) and DMVPN, except for GETVPN.
Support for RAR PPPoE IPv6 Multicast	This feature provides support for IPv6 multicast in PPPoE-based Radio Aware Routing (RAR) networks.

Feature	Description
Support for Radio Aware Routing (RAR) and Dynamic Link Exchange Protocol (DLEP)	This feature enables Radio-Aware Routing (RAR) support on Cisco Catalyst 8000 Edge Platforms. RAR is a mechanism that uses radio signals to interact with the routing protocol OSPFv3 to signal the appearance, disappearance, and link conditions of one-hop routing neighbors. Cisco Dynamic Link Exchange Protocol (DLEP) is the latest protocol in the RAR family. DLEP provides a bidirectional, event-driven communication channel between the router and the modem/radio to facilitate communication of changing link characteristics.

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.11.x releases.

Table 3: Minimum and Recommended ROMMON Releases Supported on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms respectively

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	17.10.1a	17.3(1r)	17.3(5r)
C8300-2N2S-4T2X|6T	17.10.1a	17.3(1.2r)	17.3(4.1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.10.1a	17.4(1r)	17.4(3r)
C8200L-1N-4T	17.10.1a	17.5(1.1r)	17.5(2r)

Resolved and Open Bugs for Cisco IOS XE 17.11.x

Resolved Bugs in Cisco IOS XE 17.11.1a

Identifier	Headline
CSCwd47940	PMTU discovery is not working after interface flap.
CSCwe91988	Need to disable CSDL compliance check for NPE images.
CSCwd65945	LR Interface which has NAT enabled is chosen for webex traffic.
CSCwd41236	On the Cisco Catalyst 8200-1N-4T, **show version** points to */harddisk/core directory*, but file is present in */bootflash/core directory*.

Identifier	Headline
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd45363	IPSEC throughput level / ambiguous outputs.
CSCwe28204	Control connection over L3 Tloc extension failing as no NAT table entry created.
CSCwe34808	FMAN FP leak due to the **show platform software punt-policer**command.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwd89012	Tested flap-based auto-suspension - Minimum duration value - no results as expected.
CSCwd30578	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
CSCwd79089	Devices crashes when sending Full line rate of traffic with >5 Intel AX210 stations.
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN Call disconnects.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwc72588	Router should not allow weak cryptographic algorithms to be configured for IPsec.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with ip address pool.
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature.
CSCwe00946	System crashes after disabling endpoint-tracker on tunnel interfaces.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd61255	Data Plane crashes on Catalyst 8000 Series devices when making Per-Tunnel QoS configuration changes with scale.
CSCwe01015	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwc37465	Unable to push *no-alias* option on static NAT mapping from management system.
CSCwc67625	OU field is deprecated from CA/B forum certificate authorities.
CSCwd49309	Ucode crash is seen on the device with traffic pointing to segfault in coff handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity.

Identifier	Headline
CSCwd46921	Device is not connecting to second vSmart after both assigned vSmart is down.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through the device.
CSCwc99453	Enable **license feature hseck9** command on the Cisco Catalyst 8200L platform.
CSCwe60059	Device crashes when using dial-peer groups with STCAPP.
CSCwd15487	[MBPL Integration] kernel crash is observed when modem-power-cycle is executed.
CSCwd67654	FNF stats are getting populated with unknown in egress/ingress interface in vpn0.
CSCwd38943	GETVPN: KS reject registration from a public IP.
CSCwb59113	BFD session gets nat translated with static ip over Dialer interface.
CSCwe03614	CWMP: MAC address of ATM interface is not included in Inform message.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwd85580	Device reloads after set **ospfv3 authentication null** command.
CSCvy23366	Cisco Catalyst 8300-2N2S + UCSE: Kernel crash on Cisco Catalyst 8300-2N2S with UCSE module.
CSCwd06923	Stale ip alias left after NAT statement got removed.
CSCwc48427	BFD issues with clear_omp -> non-PWK + non-VRRP scenario only.
CSCwd28593	Control connection flap of assigned vSmart after shutting down other assigned vSmart.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd68994	ISAKMP profile does not match as per configured certificate maps.

Open Bugs in Cisco IOS XE 17.11.1a

Identifier	Headline
CSCwd42523	Same label is assigned to different VRFs.
CSCwd35047	Failed to ping gateway while configuring shared LOM with console te1 interface until router reload.
CSCwd45508	Device does not form BFD across Serial link when upgrading the image.

Identifier	Headline
CSCwd76364	Device may experience unexpected reload.
CSCwe49509	Some BFD tunnel went down after migration.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwe40024	98% memory utilization on the device.
CSCwe35574	DPDK RX buffer is getting corrupted and causing device to crash.
CSCwd68111	Object group called in Zone-base Firewall gives error after upgrade.
CSCwe39011	GARP on port up/up status from Catalyst 8300 and C8500L device is not received by remote peer device.
CSCwe49684	BFD sessions keeps flapping intermittently.
CSCwe52971	BFD tunnels remain in down state.
CSCwe47915	Inter-vrf route leaking not working and packet drop seen due to IPv4 no route.

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 Marketplace.
- 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.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The 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.