# Release Notes for Cisco Catalyst 8200 Series Edge Platforms, Cisco IOS XE Cupertino 17.7.x

**First Published:** 2021-12-17

**Last Modified:** 2023-10-16

## Full Cisco Trademarks with Software License

## About Cisco Catalyst 8200 Series Edge Platforms

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

Cisco Catalyst 8200 Series Edge Platforms are available in these models:

- C8200-1N-4T
- C8200L-1N-4T

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

**Note**
- Sections in this documentation apply to all models of Cisco Catalyst 8200 Series Edge Platforms unless a reference to a specific model is made explicitly.
- Cisco IOS XE Cupertino 17.7.1a is the first release for Cisco Catalyst 8200 Series Edge Platforms in the Cisco IOS XE Cupertino 17.7.x release series.

**Note** Starting with Cisco IOS XE Bengaluru 17.4.1, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),

- Cisco Smart License Utility (CSLU), and

- Smart Software Manager On-Prem (SSM On-Prem).

## 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.

## Hardware and Software Features-New and Changed

### New and Changed Hardware Features

*Table 1: Hardware Feature in Cisco IOS XE Cupertino 17.7.1a*

| Feature | Description |
|---|---|
| 5G LTE PIM | The 5G sub-6 GHz Pluggable Interface Module (PIM) P-5GS6-GL is supported on the Cisco Catalyst 8200 Series Edge Platforms and Cisco Catalyst 8300 Series Edge Platforms. |

### New and Changed Software Features

*Table 2: Software Features in Cisco IOS XE Cupertino 17.7.1a*

| Feature | Description |
|---|---|
| Cisco ThousandEyes Enterprise Application Hosting | The Cisco ThousandEyes Enterprise Agent Application introduces the functionality to inherit the Domain Name Server (DNS) information from the device. With this enhancement, the DNS field in vManage ThousandEyes feature template is an optional parameter. |

| Feature | Description |
|---|---|
| Install Mode for Cisco Catalyst 8000 Series Edge platforms | All the Cisco Catalyst 8000 Series Edge Platforms are now configured to boot by default in install mode instead of bundle mode. This allows you to boot the device, and upgrade or downgrade the device using a set of install commands. Install mode uses .pkg files instead of .bin file to install the package, and provides a faster installation, with increased flexibility and control. |
| Multicast - mcast group calculation | The **show ip multicast overlay-mapping** command displays an underlay group address from the overlay group address which is used to troubleshoot or configure the network. The output includes the underlay group address that is within the configured SSM (Source Specific Multicast) address range. |
| Support for NGE Cipher Suites | This feature supports the Next Generation Encryption (NGE) cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both STCAPP analog phone and SCCP DSPFarm conferencing service. These cipher suites provide confidentiality, integrity, and authenticity to validate messages. |
| **Programmability Features** | |
| Converting IOS Commands to XML | This feature helps to automatically translate IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages. |
| YANG Model Version 1.1 | Cisco IOS XE Cupertino 17.7.1a uses the YANG version 1.0; however, you can download the YANG version 1.1 from GitHub at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe folder. For inquiries related to the `migrate_yang_version.py` script or the Cisco IOS XE YANG migration process, send an email to xe-yang-migration@cisco.com. |
| **Smart Licensing Using Policy Features** | |
| Ability to save authorization code request and return in a file and simpler upload in the CSSM Web UI | If your product instance is in an air-gapped network, you can now save an SLAC request in a file on the product instance. The SLAC request file must be uploaded to the CSSM Web UI. You can then download the file containing the SLAC code and install it on the product instance. You can also upload a return request file in a similar manner. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, you must upload the SLAC request or return file in the same way as you upload a RUM report. In the required Smart Account, navigate to **Reports → Usage Data Files**. See: No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU, Saving a SLAC Request on the Product Instance, Removing and Returning an Authorization Code, Uploading Data or Requests to CSSM and Downloading a File. |
| Account information included in the ACK and **show** command outputs | A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See: show license summary, show license status, show license tech. |

| Feature | Description |
|---|---|
| CSLU support for Linux | CSLU can now be deployed on a machine (laptop or desktop) running Linux. See: CSLU, Workflow for Topology: Connected to CSSM Through CSLU, Workflow for Topology: CSLU Disconnected from CSSM. |
| Factory-installed trust code | For new hardware and software orders, a trust code is now installed at the time of manufacturing. **Note** You cannot use a factory-installed trust code to communicate with CSSM. See: Overview, Trust Code. |
| RUM Report optimization and availability of statistics | RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See: RUM Report and Report Acknowledgment, Upgrades, Downgrades, show license rum, show license all, show license tech. |
| Support for trust code in additional topologies | A trust code is automatically obtained in topologies where the product instance initiates the sending of data to Cisco Smart License Utility (CSLU)and in topologies where the product instance is in an air-gapped network. See: Trust Code, Connected to CSSM Through CSLU, Tasks for Product Instance-Initiated Communication, CSLU Disconnected from CSSM, Tasks for Product Instance-Initiated Communication, No Connectivity to CSSM and No CSLU, Workflow for Topology: No Connectivity to CSSM and No CSLU. |
| Support to collect software version in a RUM report | If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version information is *included* in the RUM report. See license smart (global config). |

| Feature | Description |
|---|---|
| Tier-Based Licenses | You can now configure tier-based throughput values if the license PID is tier-based. For example, for PID DNA-C-T0-E-3Y, you can configure Tier 0 (T0) as the throughput value on the platform. Each tier represents a throughput level. Starting with the lowest throughput level, the available tiers on the Cisco Catalyst 8200 Edge Series Platforms are: |
| | T0, Tier 1 (T1), and Tier 2 (T2) on C8200-1N-4T and C8200-1N-4T-L |
| | If you purchase a tier-based license PID, the license is displayed with the tier value in the CSSM Web UI. You can also convert the numeric throughput configuration of any existing tier-based license PIDs to a tier-based throughput value. |
| | **Note**  T2 and higher tiers require an HSECK9 license and Smart Licensing Authorization Code (SLAC).<br><br>Different platforms support different maximum throughput levels, therefore each tier means a different value for different platforms. |
| | The configuration guide provides details about how numeric throughput values map with tiers and how you can change to tier-based configuration. See Available Licenses and Licensing Models. |

## 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 Series Edge Platforms. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. To access CFN, you do not require an account on cisco.com.

## Cisco Catalyst 8200 Series Edge Platforms ROMMON Compatibility Matrix

The following table lists the supported ROMMON releases:

*Table 3: Minimum and Recommended ROMMON Releases Supported on C8200-1NT-4T and C8200L-1N-4T*

| Platforms | Cisco IOS XE Release | Minimum ROMMON Release Supported for IOS XE | Recommended ROMMON Release Supported for IOS XE |
|---|---|---|---|
| C8200-1N-4T | 17.6.1 | 17.4(2r) | 17.4(2r) |
| C8200L-1N-4T | 17.6.1 | 17.5(1.1r) | 17.5(1.1r) |

## 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.

## Resolved Bugs for Cisco IOS XE 17.7.2

| Bug ID | Description |
|---|---|
| CSCwa17720 | Router rebooted due to watchdogs after issuing the commands sh crypto mib ipsec commands |
| CSCwa11150 | E1 configurations (under Serial interface) lost after reload. |
| CSCwa76260 | IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - DES, 3DES, DH1/2/5 |
| CSCwa49902 | MGCP automatic configuration fails after IOS-XE upgrade |
| CSCwa15085 | Router Crash due to Stuck Thread with appnav-xe dual controller mode. |
| CSCvx28426 | Router may crash due to Crypto IKMP process |
| CSCwa80474 | IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - PSB Security Compliance - MD5, SHA1 |
| CSCwa15132 | DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum |
| CSCwa01293 | ZBFW: Optimized policy traffic failure due to OG edit error |
| CSCwa18177 | Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed |

## Open Bugs for Cisco IOS XE 17.7.2

| Bug ID | Description |
|---|---|
| CSCvz65764 | Peer MSS value showing incorrect |
| CSCwb78228 | Platform rebooted unexpectedly with reason "LocalSoft" |
| CSCwb25137 | Source address translation for multicast traffic fails with route-map |
| CSCwb78423 | Excessive packet loss observed during DMVPN tunnel flapping |
| CSCwb66749 | when configuration ip nat inside/outside on VASI interface, ack/seq number abnormal |
| CSCwb55683 | Large number of IPSec tunnel flapping occurs when underlay is restored |
| CSCwb74821 | yang-management process confd is not running, controller mode |
| CSCwa13553 | QFP core due to NAT scaling issue |
| CSCwb11389 | NAT translation stops suddenly (ip nat inside doesn't work) |
| CSCwb51238 | Router reload unexpectedly two times when enter netflow show command |
| CSCwb61073 | BQS Failure - QoS policy is missing in hardware for some Virtual-Access tunnels after session flaps |
| CSCwa66916 | SCCP auto-configuration issues with multiple protocols |

| Bug ID | Description |
|---|---|
| CSCvz94966 | Throughput drop of 10% |
| CSCvz89354 | Router Crashes Due to CPUHOG When Walking ciscoFlashMIB |
| CSCwb79141 | UCODE Crash with mpass function |
| CSCwb08186 | E1 R2 - dnis-digits cli not working |
| CSCvz91309 | Crash due to IOSXE-WATCHDOG due to management port traffic storm |
| CSCwb12647 | Crash for stuck threads in cpp on packet processing |
| CSCwa48512 | CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also |
| CSCwb41907 | CPP uCode crash due to ipc congestion from dp to cp |
| CSCwb74917 | Incorrectly drops ip fragments due to reassembly timeout |
| CSCwa67398 | NAT translations do not work for FTP traffic |
| CSCwb76509 | Assert failure while showing FTM (Forwarding Traffic Manager) data in NH TYPE switch case |
| CSCwa84919 | "Revocation-check crl none" does not failover |
| CSCwb78173 | CSDL failure: IPSec QM Use of DES by encrypt proc is denied |
| CSCwb46649 | NAT translation don't show (or use) correct timeout value for an established TCP session |
| CSCwb68897 | "Total output drops" counter in "show interface" on Port-channel doesn't work properly |
| CSCwb02142 | Traceback: fman_fp_image core after clearing packet-trace conditions |
| CSCwb29362 | Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160 |
| CSCvz34668 | Static mapping for the hub lost on one of the spokes |
| CSCwa74499 | ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection |
| CSCwb76866 | CSDL failure: Use of MD5 by IPSEC key engine is denied |
| CSCwa68540 | FTP data traffic broken when UTD IPS enabled in both service VPN |
| CSCwb79138 | After the upgrade starts dropping GRE tunnel packets |

## Resolved Bugs for Cisco IOS XE 17.7.1a

| Bug ID | Description |
|---|---|
| CSCvz98446 | Device crashed when changing Debug Level. |
| CSCvz58895 | IOS-XE unable to export elliptic curve key. |

| Bug ID | Description |
|---|---|
| CSCvy38743 | CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on device after reload. |
| CSCwa26599 | FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed. |
| CSCvz71436 | Call Placing issue from SCCP phones. |
| CSCvz84437 | Unexpected reload due IPV6 UDP fragment header in VxLAN. |
| CSCvw16093 | Secure key agent trace levels set to Noise by default. |
| CSCvt66541 | Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted. |
| CSCvz21812 | QoS policy update with "random-detect dscp" configuration get rejected on device side. |
| CSCvx62167 | Route-map corruption when configured using Netconf with ncclient manager. |
| CSCvy42216 | "switchport trunk native vlan xx" gets removed during upgrade. |
| CSCvy93946 | Removal of SHA-1 HMAC Impacting ability to SSH. |
| CSCvy53885 | ip pim rp-candidate command removed after reload when group list is configured. |
| CSCvy22343 | Crash after reapplying BGP/ attempt to initialize an initialized wavl tree. |
| CSCvy99942 | Netconf: Logging to syslog stops working in certain scenarios |
| CSCvy54964 | Large tx/rx rate on Dialer interface in show interface output. |
| CSCvy27721 | IOS-XE Router may experience unexpected reboot with X25 RBP |
| CSCvy08748 | OSPF summary-address isn't generated though candidate exists |
| CSCvy63983 | vManage showing wrong interface status in GUI |
| CSCvy69555 | unable to fetch eigrp prefix, nexthop, omptag, and route origin |
| CSCvz04059 | Replicated EBGP routes from global table replacing native IBGP routes in VRF |
| CSCvy64796 | RIP Yang offset-list with interface config not shown in ios running-config |
| CSCvz89043 | Prevent SIP services from being blocked even if license usage ACK was not received |

## Open Bugs for Cisco IOS XE 17.7.1a

| Bug ID | Description |
|---|---|
| CSCwa07494 | IPSec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface. |
| CSCwa11150 | E1 configurations (under Serial interface) lost after reload. |
| CSCwa20814 | cEdge: cEdge device hitting vulnerability CVE 2008-5161. |

| Bug ID | Description |
|--------|-------------|
| CSCwa46001 | VRRP traffic sent while the device boots will congest the interface queue causing taildrops. |
| CSCvz72871 | Multicast traffic received over DMVPN tunnel are dropped on RP and not forwarded downstream. |
| CSCwa27659 | Virtual VRRP IP address unreachable from the BACKUP VRRP. |
| CSCvz41067 | IP Community-list config out of sync in SDWAN and IOS-XE. |
| CSCwa22665 | Memory leak in scaled EIGRP DMVPN implementation due to EIGRP: mgd_timer. |
| CSCvw06937 | cEdge: SNMv3 traps failing with initial configuration. |
| CSCvz86580 | Unable to remove the BGP neighbor statement through vManage template. |
| CSCvz20285 | SDWAN image info not updated in packages.conf when upgrading in autonomous mode. |
| CSCvz19526 | Track IPv6 address validation issue. |

## Related Documentation

- Hardware Installation Guide for Catalyst 8200 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.

## 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.