# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Cupertino 17.8.x

**First Published:** 2022-04-22

## Full Cisco Trademarks with Software License

# Cisco 4000 Series Integrated Services Routers Overview

**Note** Cisco IOS XE Cupertino 17.8.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.8.x release series.

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

| Cisco 4400 Series ISR | Cisco 4300 Series ISR | Cisco 4200 Series ISR |
|---|---|---|
| Cisco 4431 ISR | Cisco 4321 ISR | Cisco 4221 ISR |
| Cisco 4451-X ISR | Cisco 4331 ISR | |
| Cisco 4461 ISR | Cisco 4351 ISR | |

**Note** Starting with Cisco IOS XE Amsterdam 17.3.2 release, 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.

## System Requirements

The following are the minimum system requirements:

**Note** There is no change in the system requirements from the earlier releases.

- Memory: 4 GB DDR3 up to 32 GB
- Hard Drive: 200 GB or higher (Optional). The hard drive is only required for running services such as Cisco ISR-WAAS.
- Flash Storage: 4 GB to 32 GB
- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

**Note** For more information on the Cisco WAAS IOS-XE interoperability, refer to the WAAS release notes: https://www.cisco.com/c/en/us/support/routers/wide-area-application-services-waas-software/products-release-notes-list.html.

## Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

## Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE 17.8.x consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

**Note** When you upgrade from one Cisco IOS XE release to another, you may see *%Invalid IPV6 address* error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

For more information on upgrading the software, see the Installing the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

## Recommended Firmware Versions

The following table lists the recommended ROMMON and CPLD versions for Cisco IOS XE 17.2.x onwards releases.

***Table 1: Recommended Firmware Versions***

| Cisco 4000 Series ISRs | Existing ROMMON | Cisco Field-Programmable Devices | CCO URL for the CPLD Image |
|---|---|---|---|
| Cisco 4461 ISR | 16.12(2r) | 21102941 | isr_4400v2_cpld_update_v20.SPA.bin<br>isr4400v2hwprogrammable040100.SPA.pkg |
| Cisco 4451-X ISR | 16.12(2r) | 19042950 | isr4400_cpld_update_v20.SPA.bin |
| Cisco 4431 ISR | 16.12(2r) | 19042950 | isr4400_cpld_update_v20.SPA.bin |
| Cisco 4351 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v20.SPA.bin |
| Cisco 4331 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v20.SPA.bin |
| Cisco 4321 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v20.SPA.bin |
| Cisco 4221 ISR | 16.12(2r) | 19042420 | isr4200_cpld_update_v20.SPA.bin |

**Note** Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See CPLD-4-1 Release Notes.

## Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

# Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

# New and Changed Information

## New and Changed Hardware Features

There are no new hardware features for this release.

## New and Changed Software Features

*Table 2: New Software Features in Cisco IOS XE 17.8.1a*

| Feature | Description |
|---|---|
| Configuring Supplementary Voice Features | From the Cisco IOS XE 17.8.1a release, you can configure your hardware to use the SIP Line Side features such as Directed Call Park, Call Pick Up, Call Transfer, and so on. To provision these features, configure the outbound VOIP Dial-Peer, Pots Dial-Peer, Voice Card, and SIP in your hardware by performing the procedures explained in the Configuring the Supplementary Features. |
| Download AnyConnect Profiles with IPSec IKEv2 VPN | This feature allows you to configure Internet Protocol Security (IPSec)-Internet Key Exchange (IKEv2) VPN to download AnyConnect profiles over SSL, for IOS-XE headends. |
| Support for Bidirectional Debugging | You can now enable bidirectional debugging of traffic using the **debug platform condition match** command. |
| **Cisco Unified Border Element (CUBE) Features** | |
| mTLS Client CN-SAN validation | It is now possible to verify a client through the validation of the common name or subject alternate name fields in its certificate. |
| Unified Secure SRST: SHA2-Cipher-only Mode | To ensure that only the most robust cipher suites are used, Secure SRST (SCCP) may now be configured to only use TLS 1.2 Cipher Suites. Secure SIP SRST now supports the granular control of cipher suites used for both signaling (TLS) and media (SRTP). |
| Unified Secure SRST: SIP oAuth Client Registration | IP Phones, Jabber clients, and the Webex app may now failover and register to Secure SIP SRST using OAuth authentication. |
| VRF-aware Listen Port per Tenant | SIP trunks configured using the CUBE tenant feature may now be configured with a specific listen port, allowing more flexibility in routing inbound calls to the correct trunk. This feature may be used together with VRF interface binding to further control the partition and routing of calls. |
| **Programmability Features** | |
| IPSec YANG model | This feature introduces a YANG model for the **show platform hardware qfp active feature ipsec state** command. This model displays the Cisco Quantum Flow Processor (QFP) IPsec state information. You can view the different states and the number of messages exchanged for each state in QFP IPsec. With this information, you can troubleshoot issues related to IPsec flows. For more information about YANG models, see https://github.com/YangModels/yang/tree/master/vendor/cisco/xe. |

| Feature | Description |
|---|---|
| YANG Model Version 1.1 | Cisco IOS XE Cupertino 17.8.1a 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/xefolder. 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. |

## Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface requires the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol SSH/Telnet must be enabled with local authentication. This is needed for interactive commands.
- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

## Resolved and Open Bugs

This section provides information about the bugs in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 bugs are the most serious bugs. Severity 2 bugs are less serious. Severity 3 bugs are moderate bugs. This section includes severity 1, severity 2, and selected severity 3 bugs.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

**Note** If the bug that you have requested cannot be displayed, this may be due to one or more of the following reasons: the bug ID does not exist, the bug does not have a customer-visible description yet, or the bug has been marked Cisco Confidential.

## Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

### Resolved Bugs - Cisco IOS XE 17.8.1a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

| Bug ID | Description |
|---|---|
| CSCwb23043 | MACsec not working on subinterfaces using dot1q >255. |
| CSCvz34380 | Multiple Cisco Products Snort Modbus Denial of Service Vulnerability |
| CSCwa92411 | Slowness issues caused by intermittent traffic drop on device ingress from GRE tunnel. |
| CSCwa92082 | RG B2B (Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on device. |
| CSCwa13553 | QFP core due to NAT scaling issue. |
| CSCwa15132 | DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum. |
| CSCwb11389 | NAT translation stops suddenly (ip nat inside doesn't work). |
| CSCvz98373 | ZBFW: FirewallPolicy drops seen with RTSP traffic in steady state. |
| CSCwa26412 | ZBFW: OG lookups are missing from device for optimized policy. |
| CSCwa66916 | SCCP auto-configuration issues with multiple protocols. |
| CSCvy78501 | AAR not working properly as configured SLA classes are not shown under app-route stats. |
| CSCwa36699 | Prefetch CRL download fails. |
| CSCvz74773 | Discrepancies in CLI and GUI interface details (Truncating interface numbers). |
| CSCvx21819 | Keychain MACsec key input value 0 should be restricted. |
| CSCvt15177 | Certificate Signing Request made by IOS-XE never shows the Subject Alternate Name. |
| CSCwa93930 | **alarms alarm bfd-state-change syslog** command is getting rejected while reconfiguring the device. |
| CSCwa67398 | NAT translations do not work for FTP traffic on device. |
| CSCwb02851 | Device get crashed consistently with memory corruption with PPPoE dailer interface flap. |

| Bug ID | Description |
|---|---|
| CSCwa84448 | Intersite cloudsec enabled packets with <60 byte across device getting dropped when PTP is enabled. |
| CSCwa57462 | The router reloads unexpectedly due to Cellular CNM process. |
| CSCwa51443 | Incorrect check of the TCP sequence number causing return ICMP error packets to drop (ThousandEyes). |
| CSCwa78020 | ZBFW dropping packets as Input VPN ID set to 0 instead of 99. |
| CSCvz80101 | Policy XML pruning without ConfD dependency. |
| CSCvz34668 | Static mapping for the hub lost on one of the spokes. |
| CSCwa15085 | Router crash due to Stuck Thread. |
| CSCwa47219 | Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table. |
| CSCwa46760 | Memory Utilisation value sent 0.6 always to device; shows wrong value 60%. |

## Open Bugs - Cisco IOS XE 17.8.1a

All open bugs for this release are available in the Cisco Bug Search Tool.

| Bug ID | Description |
|---|---|
| CSCvz65764 | Peer MSS value showing incorrect. |
| CSCwb23632 | Command **show sdwan utd file reputation** incorrectly shows "Not connected to AMP cloud". |
| CSCwb40139 | Device fails to load bootstrap configuration with '@' in the admin password. |
| CSCvy31609 | %SELINUX-5-MISMATCH: R0/0: audispd: type=AVC msg=audit(1620855824.156:105): avc: denied{read write} |
| CSCwb11389 | NAT translation stops suddenly (ip nat inside doesn't work). |
| CSCwa84919 | "Revocation-check crl none" does not failover. |
| CSCwb42807 | After Enforce Software Version (ZTP) completed successfully, it automatically rolled back. |
| CSCwb04815 | NHRP process taking more CPU with ip nhrp redirect configured. |
| CSCwa72273 | ZBFW dropping return packets post upgrade. |
| CSCwa64955 | Device loses control connections after installing new enterprise hardware wan edge cert. |
| CSCwa49721 | HUB with firewall configured incorrectly dropping return packets when routing between VRFs. |
| CSCwb38501 | Support IGMP on voice VLAN. |

| Bug ID | Description |
|---|---|
| CSCwb25137 | [XE NAT] Source address translation for multicast traffic fails with route-map. |
| CSCwb18223 | SNMP v2 community name encryption problem. |
| CSCwb16723 | Traceroute not working with NAT. |
| CSCwb55683 | Large number of IPSec tunnel flapping occurs when underlay is restored. |
| CSCwb12647 | Device crash for stuck threads in cpp on packet processing. |
| CSCwb24123 | Registration of spoke fails with dissimilar capabilities to HUB. |
| CSCvz28950 | DMVPN phase 2 connectivity issue between two spokes. |
| CSCwb21645 | NAT traffic gets dropped when default route changes from OMP to NAT DIA route. |
| CSCwb01477 | Logging message "%IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'fman stats bipc'". |
| CSCwa08847 | ZBFW policy stops working after modifying the zone pair. |
| CSCvw50622 | NHRP network resolution not working with link-local IPv6 address. |
| CSCwb29362 | Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160. |
| CSCwb32635 | Daemon file is incomplete when running admin-tech. |
| CSCwa74499 | ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection. |
| CSCwa68540 | FTP data traffic broken when UTD IPS enabled in both service VPN. |
| CSCwa48122 | SIP OAuth http request to fetch keys from CUCM fails after bootup as interface is down. |

## Related Documentation

- Release Notes for Previous Versions of Cisco 4000 Series ISRs
- Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers
- Configuration Guides for Cisco 4000 Series ISRs
- Command Reference Guides for Cisco 4000 Series ISRs
- Product Landing Page for Cisco 4000 Series ISRs
- Datasheet for Cisco 4000 Series ISRs
- Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs
- Field Notices
- Cisco Bulletins

# 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.