# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE 17.13.x

**First Published:** 2023-12-16

## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

## Cisco 4000 Series Integrated Services Routers Overview

**Note** Cisco IOS XE 17.13.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.13.x release series.

**Note** See the End-of-Sale and End-of-Life Announcement for the Cisco ISR4200, ISR4300 and select ISR4400 Series Platform page for information about the end-of-life milestones for the Cisco 4000 Series Integrated Service Routers.

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).

**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, see 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 17.13.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_v2.0.SPA.bin<br>isr4400v2-hw-programmable.04.01.00.SPA.pkg |
| Cisco 4451-X ISR | 16.12(2r) | 19042950 | isr4400_cpld_update_v2.0.SPA.bin |
| Cisco 4431 ISR | 16.12(2r) | 19042950 | isr4400_cpld_update_v2.0.SPA.bin |
| Cisco 4351 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v2.0.SPA.bin |
| Cisco 4331 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v2.0.SPA.bin |
| Cisco 4321 ISR | 16.12(2r) | 19040541 | isr4300_cpld_update_v2.0.SPA.bin |
| Cisco 4221 ISR | 16.12(2r) | 19042420 | isr4200_cpld_update_v2.0.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 https://cfnng.cisco.com/. 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 17.13.1a*

| Feature | Description |
|---|---|
| Application Performance Monitor | The Application Performance Monitor feature introduces a simplified framework that enables you to configure intent-based performance monitors. With this framework, you can view real-time, end-to-end application performance filtered by client segments, network segments, and server segments. |
| Cisco SD-Routing Cloud OnRamp for Multicloud | Cisco SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-Routing devices. With these capabilities, the devices can access the applications hosted in the cloud. |
| Enhancements to BGP Maximum Prefix | • **Discard Extra Prefixes:** This enhancement introduces the **neighbor maximum prefix discard extra** command to drop all excess prefixes received from the neighbor when the configured value of the prefixes exceed the maximum limit.<br>• **Logging Enhancement:** The logging system is enhanced to support a per neighbor logging time every 60 seconds. |
| Initiating GARP for NAT Mapping | This feature introduces support for configuring retry time intervals for GARP messages on the BD-VIF interface. You can configure this feature using the global **ip arp nat-garp-retry** and **ip nat inside source static** commands. |
| Schedule Software Upgrade on SD-Routing Devices | With this feature, you can schedule software image upgrade on Cisco SD-Routing devices. This allows you to avoid any downtime due to the software upgrade process. |
| SD-Routing Configuration Group | The Configuration Group feature provides a simple, reusable, and structured method to configure the SD-Routing device using Cisco Catalyst SD-WAN Manager. |
| Speed Test for SD-Routing Devices | Cisco SD-WAN Manager allows you to measure the network speed and available bandwidth between a device and an iPerf3 server. The speed tests measure upload speed from the source device to the selected or specified iPerf3 server, and measure download speed from the iPerf3 server to the source device. |
| Strength Enforcement for IKE Security Association (SA) | This feature introduces an algorithm to ensure that the strength of the IKE (IKEv1 and IKEv2) SA encryption cipher is greater than or equal to the strength of its child IPsec SA encryption cipher. To enable this algorithm, use the **crypto ipsec ike sa-strength-enforcement** command. |
| Support for Flexible NetFlow Application Visibility on SD-Routing Devices | The Flexible NetFlow (FNF) feature provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Also, it provides visibility for all the traffic that passes through the VPN0 on Cisco SD-Routing devices by using the SD-Routing Application Intelligence Engine (SAIE). |

| Feature | Description |
|---|---|
| Support for Packet Capture for SD-Routing | This feature allows you to configure options to capture the bidirectional IPv6 traffic data to troubleshoot connectivity on the SD-Routing devices. |
| Support for Persistence of BGP Dynamic Neighbors | From IOS XE 17.13.1a, the device maintains the neighbor information even after the session is terminated. To configure this, use the **bgp listen persistent** command for all dynamic neighbors and **bgp listen range peer-group persistent** command for specific neighbors. |
| Support for Security-Enhanced Linux | SELinux (Security-Enhanced Linux) is a solution designed to incorporate a strong, flexible mandatory access control (MAC) architecture into Cisco IOS XE platforms.<br>From Cisco IOS XE 17.13.1a, SELinux is enabled by default in Enforcing mode for Cisco IOS XE platforms. |
| **Cisco Unified Border Element (CUBE) Features** | |
| NAT Traversal using RTP Keepalive | From Cisco IOS XE 17.13.1a onwards, using RTP keepalive packets, CUBE supports media transmission in the NAT environment. |

## 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 17.13.1a

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

| Bug ID | Description |
|---|---|
| CSCwh10813 | Add verbose log to indicate grant ra-auto un configures grant auto in PKI server. |
| CSCwf25735 | QoS with more than four remarks with set-cos does not work. |
| CSCwf44703 | NAT64 prefix is not originated into OMP. |
| CSCwf80400 | IOS XE router may experience unexpected reset while executing **show utd engine standard statistics**. |
| CSCwf14607 | Crash observed exporting PKCS12 to terminal via SSH CLI. |
| CSCwf71116 | Static route keep advertising via OMP even though there is no route. |
| CSCwf45486 | OMP to BGP redistribution leads to incorrect AS_Path installation on chosen next-hop. |

### Open Bugs - Cisco IOS XE 17.13.1a

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

| Bug ID | Description |
|---|---|
| CSCwh94906 | WLC segmentation fault crash with Network Mobility Services Protocol (NMSP). |
| CSCwh84068 | Device crash after changing NAT HSL configuration. |
| CSCwh77221 | SNMP unable to poll tunnel data after a minute. |
| CSCwi15930 | Device failing to upgrade due to CDB issue. |
| CSCwi06843 | Endpoint tracker triggers a CPU hog. |

| Bug ID | Description |
|---|---|
| CSCwh76453 | Tracker for TLOC extension is down even though TLOC is up and there is ICMP reachability. |
| CSCwi14178 | Failed to connect to device : x.x.x.x Port: 830 user: vmanage-admin error: Connection failed. |
| CSCwi08171 | Router may crash due to crypto IKMP process. |
| CSCwh01678 | Device FTM crash with SIG enabled. |
| CSCwi05395 | snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs. |
| CSCwf69062 | SDRA-SSLVPN: The SSLVPN session closes with re-authentication error after some interval of time. |
| CSCwi23562 | When RADIUS is down, and there is an IKE-AUTH request received, the box stops replying to DPD packets. |
| CSCwi11807 | snmpbulkget breaks the OID appRouteStatisticsTable after minute, not returning the correct order. |
| CSCwi00369 | Device lost security parameter after upgrade. |
| CSCwi06404 | Device PKI-related crash after failing a CRL fetch. |
| CSCwi13563 | IP SLA probe for end-point-tracker does not work once endpoint tracker is changed until reload. |
| CSCwh65016 | Unexpected reboots on device due to QFP exception. |
| CSCwh73202 | IOS-XE unexpected reboot due to critical process qfp_ucode_utah fault on fp_0_0 (rc=139). |
| CSCwi15688 | Unexpected NAT translation occurs in a specific network. |
| CSCwh91136 | IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel. |
| CSCwh57544 | Silent reload due to LocalSoftADR causes crash without core file. |
| CSCwi16015 | [SIT]: SSE tunnels do not come up with dialer interface. Relax check in IKE. |
| CSCwi02383 | Interface configuration is deleted in device with an SM module after a power-cycle. |
| CSCwi19875 | Device is unable to process hidden characters in a file while trying to use bootstrap method. |
| CSCwi35177 | Router crash caused by continuous interface flap, interface associated to many IPSec interfaces |
| CSCwh52440 | IP SLA does not have checks for ICMP probes to be sent on source interface. |
| CSCwi31833 | UTD deployment failing if deployed from remote server hostname rather than IP. |

| Bug ID | Description |
|---|---|
| CSCwi30529 | AAA: Template push fails when AAA authorization is set to local. |

## 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
- End-of-Sale and End-of-Life Announcement
- 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.