



# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE 17.14.x

---

**First Published:** 2024-04-29

## 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](http://www.cisco.com/go/offices).

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)

## Cisco 4000 Series Integrated Services Routers Overview




---

**Note** Cisco IOS XE 17.14.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.14.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 17.14.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	<a href="#">isr_4400v2_cpld_update_v2.0.SPA.bin</a> <a href="#">isr4002hwprogrammable040100SPA.pkg</a>
Cisco 4451-X ISR	16.12(2r)	19042950	<a href="#">isr4400_cpld_update_v2.0.SPA.bin</a>
Cisco 4431 ISR	16.12(2r)	19042950	<a href="#">isr4400_cpld_update_v2.0.SPA.bin</a>
Cisco 4351 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v2.0.SPA.bin</a>
Cisco 4331 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v2.0.SPA.bin</a>
Cisco 4321 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v2.0.SPA.bin</a>
Cisco 4221 ISR	16.12(2r)	19042420	<a href="#">isr4200_cpld_update_v2.0.SPA.bin</a>



**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://cfngng.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 17.14.1a*

Feature	Description
<a href="#">Enhanced IS-IS Fast Flooding</a>	The IS-IS Fast Flooding feature optimizes LSP transmission to accelerate network convergence by dynamically adjusting the LSP rate based on receiver capability. From Cisco IOS XE 17.14.1a, IS-IS Fast Flooding can be configured using the <b>router isis lsp-fast-flooding</b> command. The LSP transmission can be further customized with arguments such as <b>max-lsp-tx</b> , <b>psnp-interval</b> , and <b>per-interface</b> within the same router isis command, and enhanced by using the <b>isis remote-psnp-delay</b> command. This feature is disabled by default, and requires manual configuration to enable.
<a href="#">Enhancement to the show reload-history Command</a>	From Cisco IOS XE 17.14.1a, the <b>show reload-history</b> command is modified to <b>show reload history</b> . The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.
<a href="#">Support for 4096 Key Pair</a>	Cisco Voice Gateway (VG) series devices use 2048 RSA key as the default encryption policy. From Cisco IOS XE 17.14.1a, Cisco VG400 Voice Gateway and Cisco VG420 Voice Gateway support 4096 key pair with SHA256 hash function for TLS handshake process. For enhanced security and protection during data transmission, you can enable the 4096 key pair encryption using the <b>crypto pki trustpoint 4k_keypair</b> command.
<a href="#">Configure Secure Service Edge</a>	Secure Service Edge is a cloud solution that provides seamless, transparent, and secure Direct Internet Access (DIA) to protect against internet-based threats. This solution can be configured through Policy Groups by using Cisco SD-WAN Manager.
<a href="#">Configuration Group Enhancements</a>	This release introduces support for the following in Cisco SD-WAN Manager: <ul style="list-style-type: none"> <li>• Transport Profiles</li> <li>• Management Profile</li> <li>• Service Profile</li> <li>• CLI Profile</li> <li>• Policy Object Profile</li> </ul>
<a href="#">View Unmodelled Commands on SD-Routing Devices</a>	After an SD-Routing device is deployed, you can view the unmodelled commands on Cisco SD-WAN Manager. The list of unmodelled commands are regenerated if the device reboots.

Feature	Description
YANG Configurational Model Support for SD-Routing Devices	<p>This release introduces support for the following YANG Configurational Models:</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• MPLS</li> <li>• RSVP</li> <li>• SNMP</li> <li>• AAA</li> <li>• QoS</li> <li>• ACL</li> <li>• DHCP</li> </ul>
Support to Configure VPN Solutions for SD-Routing devices	<p>This release introduces support for the following VPN solutions:</p> <ul style="list-style-type: none"> <li>• FlexVPN</li> <li>• GETVPN</li> <li>• DMVPN</li> <li>• L3VPN</li> </ul> <p>These VPN solutions can be configured by using <b>Configuration &gt; Configuration Groups &gt; CLI Add-on Profile</b> option in Cisco SD-WAN Manager.</p>
<b>Cisco Unified Border Element (CUBE) Features</b>	
<a href="#">Secure SIP with TLS 1.3 support</a>	<p>From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of <a href="#">Transport Layer Security (TLS) version 1.3 and associated cipher suites</a>.</p>

## 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 17.14.1a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh94906</a>	WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
<a href="#">CSCwi49846</a>	FTMD crashed when SIG GRE tunnels configs are removed.
<a href="#">CSCwi55725</a>	SDR CLI config group issue.
<a href="#">CSCwi61369</a>	Device may unexpectedly reload due to SIGABRT.
<a href="#">CSCwi35716</a>	AAR backup preferred color not working as expected.
<a href="#">CSCwi53306</a>	Unknown appID in ZBFW HSL log.
<a href="#">CSCwf84567</a>	Unexpected reload after re-connecting.

Bug ID	Description
<a href="#">CSCwi14178</a>	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
<a href="#">CSCwj25493</a>	Device crashed twice with critical process linux_iosd_image fault on rp_0_0.
<a href="#">CSCwi40603</a>	Memory leak in the crypto IKMP process.
<a href="#">CSCwf08658</a>	Devices will flap the BFD sessions if we are in a non-equilibrium state and have symmetric NAT.
<a href="#">CSCwi35177</a>	Router crash caused by continuous interface flap, interface associated to many IPsec interfaces.
<a href="#">CSCwi60266</a>	Device with enterprise certificates not forming control connections with controllers after upgrade.
<a href="#">CSCwi67983</a>	Tracker state log is missing when DNS query fails.
<a href="#">CSCwi53951</a>	Packets with unicast MAC get dropped on a port channel L2 sub-intf after a router reboot.
<a href="#">CSCwb25507</a>	CWMP: Add vendor specific parameter for NBAR protocol pack version.
<a href="#">CSCwi53549</a>	Router crash with reason "Critical process fman_fp_image fault on fp_0_0 (rc=134)".
<a href="#">CSCwi82548</a>	Crash in IKEv2 cluster load balancer.
<a href="#">CSCwi51381</a>	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
<a href="#">CSCwi78365</a>	Trim installed certificate on upgrade.
<a href="#">CSCwi85293</a>	IKEv2 IPv6 cluster load balance: Secondary in cluster unable to connect to cluster in case of FVRF.
<a href="#">CSCwi86698</a>	No error message while using multicast address as system-ip in SD-Routing device.
<a href="#">CSCwj06622</a>	Segmentation fault and core files are seen on IOS-XE due to speedtest.
<a href="#">CSCwi16111</a>	<b>ipv6 tcp adjust-mss</b> not working after delete and reconfigure.
<a href="#">CSCwi62230</a>	SIG tunnel: 'SIG STATE' is showing blank value.
<a href="#">CSCwj27545</a>	Router crashing due to FTMD.

### Open Bugs - Cisco IOS XE 17.14.1a

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwj40589</a>	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
<a href="#">CSCwi81026</a>	BFD sessions flapping during IPsec rekey in scaled environment.



Bug ID	Description
<a href="#">CSCwj49941</a>	dns-snoop-agent has TCAM entry with all zeros for some regex patterns.
<a href="#">CSCwj09284</a>	Unexpected reboot in WLC due to SSL.
<a href="#">CSCwj40223</a>	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
<a href="#">CSCwj27108</a>	Not balancing traffic to default route.
<a href="#">CSCwj48421</a>	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: received IPSEC packet has invalid SPI.
<a href="#">CSCwi59854</a>	<b>show sdwan policy service-path</b> command gives inconsistent results with app name specified.
<a href="#">CSCwj42448</a>	APN password in plain text when Cellular controller profile is configured.
<a href="#">CSCwj30334</a>	CVLA ucode crash when attempting merge on used block.
<a href="#">CSCwj26085</a>	Control connections in TLS goes to 'trying' state with UTD.
<a href="#">CSCwj32347</a>	DIA endpoint tracker not working with ECMP routes.
<a href="#">CSCwj45177</a>	"dmidecode: command not found" error seen executing <b>show sdwan certificate validity</b> .
<a href="#">CSCwe92181</a>	Device traceback and reload after detecting a fatal error in qfp-ucode-radium.
<a href="#">CSCwj34578</a>	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
<a href="#">CSCwj31354</a>	Template push failure due to service timestamps.
<a href="#">CSCwj02628</a>	Speed-test not working for device.
<a href="#">CSCwj13681</a>	Device can only store 64 FQDN patterns, but config accepts more than 64.

## 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.

