



Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Dublin 17.10.x

First Published: 2022-12-16

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 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 Dublin 17.10.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.10.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).



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 17.10.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 isr4002hwprogrammable4000SPA.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 <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 17.10.1a

Feature	Description
Enable Configuring DHCPv4 Client Option 124	This feature provides the ip dhcp client vendor-class command that helps you configure the DHCP client to carry option 124 data in DHCPv4, along with the interface MAC address or user-defined string. When the option 124 data in DHCPv4 is disabled, it disables sending the option 124 in DHCPv4 messages. By default, the DHCPv4 client sends device PID as the value for option 124.
Enable Configuring DHCPv6 Client Option 16	This feature provides the ipv6 dhcp client vendor-class command that helps you configure the DHCPv6 client to carry option 16 data in DHCPv6, along with the interface MAC address or user-defined string. When the option 16 data in DHCPv6 is disabled, it disables sending the option 16 in DHCPv6 messages. By default, the DHCPv6 client sends device PID as the value for option 16.
Packet Tracer with UDF Offset	Using this feature you can configure to match the packets based on user defined field position and length. This can be used by an ACL to match packets that cannot be classified easily with the traditional Layer 3 and Layer 4 field information.
Support for Secure Real-time Transport Protocol (SRTP) Dual-Tone Multi-Frequency (DTMF) Interworking	This feature provides support for Dual-Tone Multi-Frequency (DTMF) interworking between Cisco Unified Communications Manager (CUCM) and Secure Software MTP in pass-through mode. It is supported on both CUCM and Cisco IOS XE software.
Cisco Unified Border Element (CUBE) Features	
YANG model enhancements for Unified SRST and CUBE	Additional YANG configuration models are included in this release to enable Unified SRST secure calling, applications for CUBE, and additional codecs for voice class codec lists.

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 17.10.1a

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

Bug ID	Description
CSCwc70511	Router reloads unexpectedly during NHRP processing.
CSCwb35303	X25 FRMR seen when switching from XOT to low speed serial.
CSCwc77981	Device crashed - track the FMAN-FP's memory leak caused by cond-debug.
CSCwc29735	Improve debug for reload at crypto_dev_proxy_ipc_ipsec_sa crt_hdlr when scale exceed limit.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linstate down.
CSCwc88791	DSL: erroneous atm interface counter at DSL retraining.

Bug ID	Description
CSCwc78021	Standby WLC crash @ fman_acl_remove_default_ace.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.

Open Bugs - Cisco IOS XE 17.10.1a

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

Bug ID	Description
CSCwd25107	Interface Vlan1 placed in shutdown state when configured with ip address pool .
CSCwd23810	IOS-XE: High CPU utilization caused by NHRP.
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
CSCwd61255	Data Plane crash on device when making QoS configuration changes.
CSCwd35047	Failed to ping gateway while configuring Shared LOM with console, te1 interface, until router reload.
CSCwc65697	Device crashing and restarting during call flow with new image.
CSCwd53205	IKEv2 RRI routes are intermittently disappearing from a FlexVPN hub.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgac1_alloc.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwd12828	Segmentation fault crash in CCSIP_SPI_CONTROL process.
CSCwd74089	CUBE call leak at FPI layer.
CSCwc66646	Unexpected reload due to segmentation fault in the CCSIP_SPI_CONTROL process.
CSCwc23645	When using SRTP with higher ciphers, CUBE is inserting distortion in voice.
CSCwc57959	Device crashed in SSP load test.

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.

