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

First Published: 2024-04-29

Full Cisco Trademarks with Software License

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	isr_4400v2_cpld_update_v20.SPA.bin isr4400v2hwprogrammbb040100.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 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 17.14.1a

Feature	Description
Enhanced IS-IS Fast Flooding	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 **router isis lsp-fast-flooding** command. The LSP transmission can be further customized with arguments such as **max-lsp-tx**, **psnp-interval**, and **per-interface** within the same router isis command, and enhanced by using the **isis remote-psnp-delay** command. This feature is disabled by default, and requires manual configuration to enable.
Enhancement to the **show reload-history** Command	From Cisco IOS XE 17.14.1a, the **show reload-history** command is modified to **show reload history**. The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.
Support for 4096 Key Pair	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 **crypto pki trustpoint 4k_keypair** command.
Configure Secure Service Edge	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.
Configuration Group Enhancements	This release introduces support for the following in Cisco SD-WAN Manager: • Transport Profiles • Management Profile • Service Profile • CLI Profile • Policy Object Profile
View Unmodelled Commands on SD-Routing Devices	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	This release introduces support for the following YANG Configurational Models: • BGP • MPLS • RSVP • SNMP • AAA • QoS • ACL • DHCP
Support to Configure VPN Solutions for SD-Routing devices	This release introduces support for the following VPN solutions: • FlexVPN • GETVPN • DMVPN • L3VPN These VPN solutions can be configured by using **Configuration** > **Configuration Groups** > **CLI Add-on Profile** option in Cisco SD-WAN Manager.
Cisco Unified Border Element (CUBE) and SRST Features	
CUBE: Secure SIP with TLS 1.3 support	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of Transport Layer Security (TLS) version 1.3 and associated cipher suites.
SRST: Secure SIP with TLS 1.3 support	Starting from Cisco Unified SRST 14.4 release, the SRST security feature is enhanced to support TLS version 1.3 and associated ciphers.

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

Bug ID	Description
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
CSCwj25493	Device crashed twice with critical process linux_iosd_image fault on rp_0_0.
CSCwi40603	Memory leak in the crypto IKMP process.
CSCwf08658	Devices will flap the BFD sessions if we are in a non-equilibrium state and have symmetric NAT.
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many IPsec interfaces.
CSCwi60266	Device with enterprise certificates not forming control connections with controllers after upgrade.
CSCwi67983	Tracker state log is missing when DNS query fails.
CSCwi53951	Packets with unicast MAC get dropped on a port channel L2 sub-intf after a router reboot.
CSCwb25507	CWMP: Add vendor specific parameter for NBAR protocol pack version.
CSCwi53549	Router crash with reason "Critical process fman_fp_image fault on fp_0_0 (rc=134)".
CSCwi82548	Crash in IKEv2 cluster load balancer.
CSCwi51381	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
CSCwi78365	Trim installed certificate on upgrade.
CSCwi85293	IKEv2 IPv6 cluster load balance: Secondary in cluster unable to connect to cluster in case of FVRF.
CSCwi86698	No error message while using multicast address as system-ip in SD-Routing device.
CSCwj06622	Segmentation fault and core files are seen on IOS-XE due to speedtest.
CSCwi16111	**ipv6 tcp adjust-mss** not working after delete and reconfigure.
CSCwi62230	SIG tunnel: 'SIG STATEâ is showing blank value.
CSCwj27545	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
CSCwj40589	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
CSCwi81026	BFD sessions flapping during IPSec rekey in scaled environment.

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