# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE 17.15.x

**First Published:** 2024-08-26

## Full Cisco Trademarks with Software License

# Cisco 4000 Series Integrated Services Routers Overview

**Note** Cisco IOS XE 17.15.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.15.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.

**Note** See the End-of-Sale and End-of-Life Announcement for the Cisco ISR4461 Series Platform page for information about the end-of-life milestones for the Cisco ISR4461 series platform.

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 17.15.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>isr4400v2hwprogrammbb040100SPA.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 17.15.1a*

| Feature | Description |
|---|---|
| Absolute Path for HTTP or HTTPS File Transfer | The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the **copy** command.<br>From Cisco IOS XE 17.15.1a, you must provide the absolute file path when you execute the **copy** command, to transfer the file. |
| Cisco Umbrella Scope Credentials | From Cisco IOS XE 17.15.1a, this feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS. |
| Enabling Flow Level Flexible NetFlow Support for SD-Routing Devices | The Flow-level Flexible NetFlow (FNF) feature allows you to monitor the NetFlow traffic and view all the flow-level FNF data that is captured including application-level statistics. This feature is only supported on ISR4461. |
| Enhanced NAT Management | From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the **ip nat translation max-entries cpu** command. This feature also enables streamlining NAT synchronization in redundant systems using the **ip nat settings redundancy optimized-data-sync** command. |
| Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF | You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic. |
| Monitoring SD-Routing Alarms | From Cisco IOS XE 17.15.1a, network administrators can monitor SD-Routing device alarms on Cisco Catalyst SD-WAN Manager. This feature enables SD-Routing devices to record and store various alarms generated by control components and routers. For more information, see Cisco SD-Routing Command Reference Guide. |
| Network-Wide Path Insights on SD-Routing Devices | Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network. |

| Feature | Description |
|---|---|
| SD-Routing License Management | This release introduces license management support for SD-Routing devices. The supported licensing workflows include license assignment or configuration, license use, and license usage reporting. Depending on the device, these workflows are performed in the Cisco Catalyst SD-WAN Manager or on the device. |
| Seamless Software Upgrade for SD-Routing Devices | This feature explains how to seamlessly upgrade and onboard an existing Cisco Routing device into the Cisco SD-WAN infrastructure. |

## 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 17.15.1a

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

| Bug ID | Description |
|---|---|
| CSCwj51700 | CPP crashes after re-/configuring **ip nat settings pap limit ... bpa** feature in high QFP state. |
| CSCwk03686 | Crash due a segmentation fault due a negative value. |
| CSCwk42634 | %PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6). |
| CSCwk33173 | EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows. |
| CSCwk16333 | Device repeatedly crashing in FTMd due to FNF flow add. |
| CSCwj96852 | Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC. |
| CSCwk42190 | Config and dp show command do not match the dp oper output. |
| CSCwj95633 | SAIE application - no data to display for IOS XE router. |
| CSCwk39131 | Device crashed when issuing **show sdwan ftm next-hop chain all**. |
| CSCwk37351 | IOS XE Router: Unexpected reboot during PVDM OIR. |
| CSCwk22225 | FTMd crashes after receiving credentials feature template update. |
| CSCwj48909 | Coredump observed in tracker module while running cxp_sig_auto_tunnel suite. |
| CSCwk45165 | fman_fp memory meak on device. |
| CSCwj84949 | Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup. |
| CSCwj90614 | High CPU utilisation for confd_cli. |
| CSCwi81026 | BFD sessions flapping during IPSec rekey in scaled environment. |
| CSCwk39268 | sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11. |
| CSCwj76662 | High memory utilization due to "ftmd" process. |

| Bug ID | Description |
|---|---|
| CSCwj92560 | STCAPP command removed from VG410 after reload. |
| CSCwk31715 | After deleting a NAT configuration, the IP address still shows up in routing table. |
| CSCwk12524 | Device reloaded due to ezManage mobile app Service. |
| CSCwk44078 | GETVPN / migrating to new KEK RSA key does not trigger GM re-registration. |
| CSCwi99454 | FNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive. |
| CSCwk22942 | Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other. |
| CSCwj96092 | ICMP tracker type (from echo to timestamp) change causes tracker to fail. |
| CSCwj99827 | Device unexpectedly reloads due to a crash in 'vdaemon' process. |
| CSCwj23674 | Dialer interface MAX MTU for PPPOA is 1492. |
| CSCwj40223 | appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order. |
| CSCwj02401 | Router reloaded when generating admin tech while processing very high number of flows. |
| CSCwk19725 | Add FNF cache limit for show sdwan app-fwd flows. |
| CSCwj86794 | Device crashes while processing an NWPI trace. |
| CSCwk42253 | Unexpected reboot when a HTTP connection failed with 404 on a controller mode router. |
| CSCwj67591 | Chassis activate effective only after second re-try - with new uuid. |
| CSCwj32347 | DIA endpoint tracker not working with ECMP routes. |

## Open Bugs - Cisco IOS XE 17.15.1a

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

| Bug ID | Description |
|---|---|
| CSCwk75733 | Custom Applications may not be programmed properly. |
| CSCwk89256 | Speed mismatch in IOS-XE configuration after device template push. |
| CSCwk85704 | **match traffic-category** add-on CLI push failed. |
| CSCwm07651 | Device crash due to DBGD process. |
| CSCwk86355 | File transfer fails "lost connection". |
| CSCwk49806 | Router rebooted unexpectedly due to process NHRP crash. |

| Bug ID | Description |
|---|---|
| CSCwk81360 | Router can reboot unexpectedly while configuring NAT static translation. |
| CSCwk62954 | Multiple "match address local interface <int>" not pushed under crypto profile. |
| CSCwk63722 | Startup configuration failure post PKI server enablement. |
| CSCwk97092 | MKA session not coming up after shut/no shut with EVC. |
| CSCwm07564 | data-policy local-tloc-list breaks RTP media stream. |
| CSCwk54544 | ZBFW TCAM misprogramming after rules are reordered. |
| CSCwk74298 | Device denied for template push and some show commands with error application communication failure. |
| CSCwk98578 | GETVPN IPv6 crypto map not shown in interface configuration. |
| CSCwk70630 | Cannot import device certificate. |
| CSCwk97930 | Crash occurs when IPv6 packets with link-local source are forwarded. |
| CSCwm13223 | Device crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog. |
| CSCwk79454 | Endpoint tracker does not fail if default route is removed. |
| CSCwk90014 | NAT DIA traffic getting dropped due to port allocation failure. |
| CSCwi87546 | Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - lock id of 0 released. |
| CSCwk61238 | RRI static not populating route after reload if stateful IPSec is configured. |
| CSCwm12851 | Device uses 3DES as default rekey algorithm for GETVPN. |
| CSCwk95044 | SPA.smu.bin drops when packet duplication link fails-over. |
| CSCwj87028 | Device showing custom APP as "unknown" for egress traffic when using DRE Opt. |
| CSCwk20995 | PPPoE session with sub-interface getting stuck after reboot. |
| CSCwm08545 | Centralized policy policer worked per PC on the same site not per site/vpn-list. |
| CSCwf62943 | System image file is not set to packages.conf when image expansion fails due to disk space. |
| CSCwm00309 | Packets not hitting the correct data policy after modifying the action of a sequence. |

## 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 DevNet.
- 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.