Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-06

Full Cisco Trademarks with Software License

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 Dublin 17.11.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.11.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 17.11.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 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 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 17.11.1a

Feature	Description
Configure DHCP in a VPN-SIP Solution	From Cisco IOS XE 17.11.1a, you can install and enable a Session Initiation Protocol Triggered VPN (VPN-SIP) router behind a home gateway. In this installation, the home gateway assigns an extension number to the tunnel interface through Dynamic Host Configuration Protocol (DHCP) instead of a fixed telephone number. This allows you to aggregate data and voice on your network and share the same physical subscriber line for both analog and digital data.
Deprecation of Weak Ciphers	The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.
Enabling the RSRP and RSRQ Parameters for Link Recovery on LTE Modems	This feature enables the RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) parameters that detect any network issues or malfunctions as part of the link-recovery feature on LTE modems.To enable these parameters, the user can configure the **lte modem link-recovery rsrp onset-threshold** command for RSRP and **lte modem link-recovery rsrq onset-threshold** command for RSRQ.

Feature	Description	
Redirecting Deprecated LISP Commands to Revised Versions	The following LISP commands have been revised:	
	Old Command	New Command
	show ip/ipv6 lisp all	**show lisp service ipv4/ipv6**
	show ip/ipv6 lisp instance-id alt	**show lisp instance-id ipv4/ipv6 alt**
	show ip/ipv6 lisp instance-id database	**show lisp instance-id ipv4/ipv6 database**
	show ip/ipv6 lisp forwarding	**show lisp ipv4/ipv6 instance-id forwarding**
	show ip/ipv6 lisp instance-id	**show lisp instance-id**
	show ip/ipv6 lisp locator-table	**show lisp locator-table**
	show ip/ipv6 lisp instance-id map-cache	**show lisp instance-id ipv4/ipv6 map-cache**
	show ip/ipv6 lisp instance-id route-import	**show lisp instance-id ipv4/ipv6 route-import**
	show ip/ipv6 lisp instance-id smr	**show lisp instance-id ipv4/ipv6 smr**
	show ip/ipv6 lisp instance-id statistics	**show lisp instance-id ipv4/ipv6 statistics**
	show lisp site	**show lisp server**
	show lisp site detail	**show lisp instance-id ipv4/ipv6 server detail**
	show lisp site name	**show lisp instance-id ipv4/ipv6 server name**
	show lisp site summary	**show lisp instance-id ipv4/ipv6 server summary**
	show lisp site rloc	**show lisp instance-id ipv4/ipv6 server rloc**
Cisco Unified Border Element (CUBE) Features		
Unified SRST: Concurrent use of Webex Calling Survivability Gateway and Unified SRST	From Cisco IOS XE Dublin 17.11.1a onwards, concurrent use of Cisco Webex Calling Survivability Gateway and Unified SRST is supported on the same router.	
Smart Licensing Using Policy Features		

Feature	Description
Snapshots for Product Activation Key (PAK) licenses	Starting with Cisco IOS XE Dublin 17.11.1a, the PAK-managing library is discontinued and the provision to *take* a snapshot is no longer available. Software images from Cisco IOS XE Dublin 17.11.1a onwards rely only on the snapshotted information about PAK licenses. For more information, see: Snapshots for PAK Licenses. If you have a PAK license without a snapshot, and you want to upgrade to Cisco IOS XE Dublin 17.11.1a or a later release, you will have to upgrade twice. First upgrade to one of the releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release.

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 17.11.1a

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

Bug ID	Description
CSCwd47940	PMTU Discovery is not working after interface flap.
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
CSCwc79115	Device Policy commit failure notification and alarm from vsmart.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd67198	uCode crash seen on device after stopping NWPI trace.
CSCwe28204	Control connection over L3 TLOC extension failing as no NAT table entry created.
CSCwe34808	FMAN FP leak due to the **punt-policer** command.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwd89012	Tested flap-based auto-suspension - minimum duration value - no results as expected.
CSCwe29430	Critical process fpmd fault on rp_0_0 (rc=134).
CSCwe07055	Device frequent reloads.
CSCwd79089	Device crash when sending full line rate of traffic with >5 Intel AX210 stations.
CSCwd87195	NAT configuration with redundancy, mapping ID and match-in-vrf options with no-alias support.
CSCwd81357	QoS Classification not working for DSCP or ACL + MPLS EXP.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCwd44439	Device crashing at fman_sdwan_nh_indirect_delete_from_hash_table.

Bug ID	Description
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwc72588	Router should not allow weak cryptographic algorithms to be configured for IPsec.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with **ip address pool**.
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature.
CSCwe00946	System crash after disabling endpoint-tracker on tunnel interfaces.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd61255	Data Plane crash on device when making per-tunnel QoS configuration changes with scale.
CSCwe01015	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwe27241	NBAR classification error with custom app-aware routing policy.
CSCwc37465	Unable to push no-alias option on static NAT mapping from management system.
CSCwc67625	OU field is deprecated from CA/B Forum Certificate Authorities.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity.
CSCwd46921	Device is not connecting to second vSmart after both assigned vSmart is down.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router.
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwd15487	Kernel crash is observed when modem-power-cycle is executed.
CSCwd67654	FNF stats are getting populated with unknown in egress/ingress interface in vpn0.
CSCwd38943	GETVPN: KS reject registration from a public IP.
CSCwb59113	BFD session gets nat translated with static IP over dialer interface.
CSCwe03614	CWMP : MAC address of ATM interface is not included in Inform message.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.

Bug ID	Description
CSCwe69783	Device can lose its config during a triggered resync process if lines are in an off-hook state.
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwd85580	Device unexpected reload after **set ospfv3 authentication null** command.
CSCwd65945	LR Interface which has NAT enabled is chosen for Webex traffic.
CSCwe37184	Device seeing out of service on switch modules with new DC power supply.
CSCwd06923	Stale IP alias left after NAT statement got removed.
CSCwc48427	BFD issues with clear_omp -> non-PWK + non-VRRP scenario only.
CSCwd28593	Control connection flap of assigned vSmart after shutting down other assigned vSmart.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps.
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences.
CSCwe91988	Need to disable CSDL compliance check for NPE images.

Open Bugs - Cisco IOS XE 17.11.1a

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

Bug ID	Description
CSCwe70717	Websocket media forking is not happening on expected Websocket server on device.
CSCwd42523	Same label is assigned to different VRFs.
CSCwd45508	Device does not form BFD across serial link when upgrading.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwe49509	Some BFD tunnel went down after migrating.
CSCwe37123	Device uses excessive memory when configuring ACLs with Large Object Groups.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwe40024	98% memory utilization.

Bug ID	Description
CSCwd68111	Object group called in ZBFW gives error after upgrade.
CSCwe49684	BFD sessions keeps flapping intermittently.
CSCwe52971	BFD tunnels via Starlink remain in down state.

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.