Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE 17.14.x

First Published: 2024-04-29

Full Cisco Trademarks with Software License

About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on the router.

Note Cisco IOS XE 17.14.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE 17.14.x release series.

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.

New and Changed Hardware and Software Features

New and Changed Software Features in Cisco IOS XE 17.14.1a

Table 1: New Software Features

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.
MAP-T Customer Edge (CE) Support	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.

Feature	Description

Support for Suite B Ciphers with GET VPN	From Cisco IOS XE 17.14.1a, this enhancement introduces support for Suite B ciphers with GET VPN on the following platforms and its corresponding models:
	• Cisco ASR 1000 Series Aggregation Services Routers:
	  • ASR 1000 with ESP100-X
	• Cisco Catalyst 8300 Series Edge Platforms:
	  • C8300-1N1S-4T2X
	  • C8300-2N2S-6T
	• Cisco Catalyst 8200 Series Edge Platforms:
	  • C8200L-1N-4T
	• Cisco Catalyst 8500 Series Edge Platforms:
	  • C8500-12X4QC
	  • C8500L-8S4X
	• Cisco 1000 Series Integrated Services Routers:
	  • C1131
	  • C112X
	  • C116X
	  • C111X

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.
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
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
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.

Note From Cisco IOS XE Release 17.9.1a, guestshell is removed from the IOS XE software image. As a result, Zero Touch Provisioning (ZTP) python script is no longer supported on Cisco 1000 Series Integrated Services Routers. If you need to use guestshell, then download it from https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads. For more information, see Guestshell installation procedure.

Cisco ISR1000 ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases and Cisco IOS XE 17.x.x releases.

Note To identify the manufacturing date, use the **show license udi** command. For example:

```
Router#show license udi
UDI: PID:C1131-8PLTEPWB,SN:FGLxxxxLCQ6
```

The xxxx in the command output represents the manufacturing date.

- If the manufacturing date is greater than or equal to 0x2535, the manufactured ROMmon version is 17.6(1r) or higher.
- If the manufacturing date is less than 0x2535, the ROMmon will be automatically upgraded to 17.5(1r) or above when the Cisco IOS XE 17.9.x release is installed.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 or later is 17.5(1r) or later.

Note To upgrade to Cisco IOS XE Dublin 17.12.x, follow these steps:

1. If you are on a device that is running software version between Cisco IOS XE 16.x to Cisco IOS XE 17.4.x, upgrade to any IOS XE image between Cisco IOS XE 17.5.x to Cisco IOS XE 17.10.x.
2. After performing step a, upgrade to Cisco IOS XE 17.12.x.
3. For devices that are running on software version Cisco IOS XE 17.5.x or later, you can upgrade to Cisco IOS XE 17.12.x directly.

Table 2: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)
17.2.x	16.9(1r)	16.12(1r)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
17.3.x	16.12(2r)	16.12(2r)
17.4.x	16.12(2r)	16.12(2r)
17.5.x	17.5(1r)	17.5(1r)
17.6.x	17.5(1r)	17.5(1r)
17.7.x	17.5(1r)	17.5(1r)
17.8.x	17.5(1r)	17.5(1r)
17.9.x	17.5(1r)	17.5(1r)
17.10.x	17.5(1r)	17.5(1r)
17.11.x	17.5(1r)	17.5(1r)
17.12.x	17.5(1r)	17.5(1r)
17.13.x	17.5(1r)	17.5(1r)
17.14.x	17.5(1r)	17.5(1r)

Resolved and Open Bugs in Cisco IOS XE 17.14.x

Resolved Bugs in Cisco IOS XE 17.14.1a

Table 3: Resolved Bugs in Cisco IOS XE 17.14.1a

Bug ID	Description
CSCwi53951	Packets with unicast MAC get dropped on a Port Channel L2 sub-intf after a router reboot.
CSCwj25493	Device crashed twice with critical process linux_iosd_image fault on rp_0_0.

Open Bugs in Cisco IOS XE 17.14.1a

There are no open bugs for this release.

Related Information

- Hardware Installation Guide
- Software Configuration Guide
- Smart Licensing using Policy

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.