Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Dublin 17.10.x

First Published: 2022-12-16

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.

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 Dublin 17.10.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Dublin 17.10.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

Table 1: New Software Features

Feature	Discription
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.
5G LTE PIM	The 5G sub-6 GHz Pluggable Interface Module (PIM) P-5GS6-GL is supported on the Cisco 1000 Series Integrated Services Routers.
Support for YANG Operational Model in the GETVPN architecture	This feature enables the YANG operational model in the GETVPN architecture to support the crypto gdoi command which was previously enabled only for the CLI and SNMP models.
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.

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 and recommended ROMmon version is 17.6(1r).
- If the manufacturing date is less than 0x2535, the ROMmon will be automatically upgraded to 17.5(1r) 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.

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)
17.3.x	16.12(2r)	16.12(2r)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
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)

Resolved and Open Bugs in Cisco IOS XE 17.10.x

Resolved Bugs in Cisco IOS XE 17.10.1a

Table 3: Resolved Bugs in Cisco IOS XE 17.10.1a

Bug ID	Description
CSCwc70511	Router reloads unexpectedly during NHRP processing.
CSCwb35303	X.25 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_hndlr when scale exceed limit.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down IPsec tunnel interface- stuck at linestate down.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPsec SA.

Open Bugs in Cisco IOS XE 17.10.1a

Table 4: Open Bugs in Cisco IOS XE 17.10.1a

Bug ID	Description
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with IP address pool.
CSCwd23810	IOS-XE: A high CPU utilization caused by NHRP.

Bug ID	Description
CSCwd45402	MSR Unicast-To-Multicast not working if destination and source are the same in service reflect configuration.
CSCwd61255	Data plane crash on device when making QoS configuration changes.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwd39219	Device SMS archive does not work when FTP transaction is of VRF.
CSCwd47937	Device roll back does not work.
CSCwd53205	IKEv2 the RRI routes are intermittently disappearing from a FlexVPN hub.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = crypto IKMP.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router.
CSCwc65697	Device crashing and restarting during call flow with new image.
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 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.