Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE 17.13.x

First Published: 2023-12-16

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 17.13.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE 17.13.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 17.13.1a

Table 1: New Software Features

Feature	Description
Application Performance Monitor	The Application Performance Monitor feature introduces a simplified framework that enables you to configure intent-based performance monitors. With this framework, you can view real-time, end-to-end application performance filtered by client segments, network segments, and server segments.
Cisco SD-Routing Cloud OnRamp for Multicloud	Cisco SD-Routing Cloud OnRamp for Multicloud extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into the Cisco Catalyst SD-Routing devices. With these capabilities, the devices can access the applications hosted in the cloud.
Cisco Managed Cellular Activation (eSIM) Support for Additional PIMs	Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) models: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL • LTE CAT 18 PIM, model P-LTEAP18-GL • LTE CAT 6 PIM, models P-LTEA-EA, P-LTEA-LA • LTE CAT 7 PIM, models P-LTEA7-NA, P-LTEA7-EAL, P-LTEA7-JP
Enhancements to BGP Maximum Prefix	• Discard Extra Prefixes: This enhancement introduces the neighbor maximum prefix discard extra command to drop all excess prefixes received from the neighbor when the configured value of the prefixes exceed the maximum limit. • Logging enhancement: The logging system is enhanced to support a per neighbor logging time every 60 seconds.
Initiating GARP for NAT Mapping	This feature introduces support for configuring retry time intervals for GARP messages on the BD-VIF interface. You can configure this feature using the global ip arp nat-garp-retry and ip nat inside source static commands.
SD-Routing Configuration Group	The SD-Routing Configuration Group feature provides a simple, reusable, and structured method to configure the SD-Routing device using Cisco Catalyst SD-WAN Manager.
Schedule Software Upgrade on SD-Routing Devices	With this feature, you can schedule software image upgrade on Cisco SD-Routing devices. This allows you to avoid any downtime due to the software upgrade process.
Speed Test for SD-Routing Devices	Cisco SD-WAN Manager allows you to measure the network speed and available bandwidth between a device and an iPerf3 server. The speed tests measure upload speed from the source device to the selected or specified iperf3 server, and measure download speed from the iperf3 server to the source device.

Feature	Description
Strength Enforcement for IKE Security Association (SA)	This feature ensures that the strength of the IKE (IKEv1 and IKEv2) SA encryption cipher is greater than or equal to the strength of its child IPsec SA encryption cipher. To enable this feature, use the crypto ipsec ike sa-strength-enforcement command.
Support for Security-Enhanced Linux	SELinux (Security-Enhanced Linux) is a solution designed to incorporate a strong, flexible mandatory access control (MAC) architecture into Cisco IOS XE platforms. From Cisco IOS XE 17.13.1a, SELinux is enabled by default in Enforcing mode for Cisco IOS XE platforms.
Support for Persistence of BGP Dynamic Neighbors	From IOS XE 17.13.1a, the device maintains the neighbor information even after the session is terminated. To configure this, use the bgp listen persistent command for all dynamic neighbors and bgp listen range peer-group persistent command for specific neighbors.
Support for Packet Capture for SD-Routing	This feature allows you to configure options to capture the bidirectional IPv6 traffic data to troubleshoot connectivity on the SD-Routing devices.
Support for Flexible NetFlow Application Visibility on SD-Routing Devices	The Flexible NetFlow (FNF) feature provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Also, it provides visibility for all the traffic that passes through the VPN0 on Cisco SD-Routing devices by using the SD-Routing Application Intelligence Engine (SAIE).
Cube Features	
NAT Traversal using RTP Keepalive	From Cisco IOS XE 17.13.1a onwards, using RTP keepalive packets, CUBE supports media transmission in the NAT environment.

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

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

Resolved and Open Bugs in Cisco IOS XE 17.13.x

Resolved Bugs in Cisco IOS XE 17.13.1a

Table 3: Resolved Bugs in Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh10813	Add verbose log to indicate grant ra-auto unconfigures grant auto in PKI server.
CSCwf25735	QoS with more than four remarks with set-cos does not work.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf80400	IOS XE router may experience unexpected reset while executing **show utd engine standard statistics**.
CSCwf14607	Crash observed exporting PKCS12 to terminal via SSH CLI.
CSCwf71116	Static route keeps advertising via OMP even though there is no route.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path installation on chosen Next-Hop.

Open Bugs in Cisco IOS XE 17.13.1a

Table 4: Open Bugs in Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh94906	WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).

Bug ID	Description
CSCwi03502	Creation of CLI to push at#enadis=0, followed by at#reboot to FN980, is required when configuring Multi-PDN.
CSCwh84068	Device crash after changing NAT HSL configuration.
CSCwh77221	SNMP unable to poll SDWAN tunnel data after a minute.
CSCwi15930	Device failing to upgrade due to CDB issue.
CSCwh98286	Device reloaded with critical process qfp_ucode_radium fault on fp_0_0 (rc=139).
CSCwi11807	snmpbulkget breaks the OID appRouteStatisticsTable after minute not returning the correct order.
CSCwh76453	Tracker for TLOC extension is down even though TLOC is up and there is ICMP reachability.
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
CSCwi08171	Router may crash due to Crypto IKMP process.
CSCwh01678	Device platform FTM crash with SIG enabled.
CSCwi05395	snmpbulkget cannot get loss, latency and jitter for probe class table and class interval table OIDs.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwi23562	When RADIUS down, and there is an IKE-AUTH request received, the box stops replying to DPD packets.
CSCwi00369	Device lost security parameter after upgrade.
CSCwi06404	PKI related crash after failing a CRL fetch.
CSCwi13563	IP SLA probe for end-point-tracker does not work once endpoint tracker is changed until reload.
CSCwh65016	Unexpected reboots on device due to QFP exception.
CSCwi15688	Unexpected NAT translation occurs in a specific network.
CSCwh91136	Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwi07148	Interfaces configuration change to **negotiation auto** to **no negotiation auto** after a reboot.
CSCwi16015	SSE tunnels do not come up with dialer interface. Relax check in IKE.
CSCwi19875	Device is unable to process hidden characters in a file while trying to use bootstrap method.

Bug ID	Description
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many IPsec interfaces.
CSCwh52440	IP SLA does not have checks for ICMP probes to be sent on source interface.
CSCwi31833	UTD deployment failing if deployed from remote server hostname rather than the IP.
CSCwi30529	Template push fails when AAA authorization is set to local.

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.