Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE 17.16.x

First Published: 2024-12-22

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 17.16.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE 17.16.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 17.16.1a

Table 1: New Software Features

Feature	Description
Asymmetric carrier delay	Asymmetric Carrier Delay allows you to configure separate delay times for link-up and link-down event notification on physical interfaces. From Cisco IOS XE 17.16.1a, asymmetric carrier delay is supported on *Cisco 1000 Series Integrated Services Routers.*
Cisco ThousandEyes Enterprise Application Hosting	Cisco ThousandEyes is a network intelligence platform that enables you to monitor the network traffic paths across internal, external, and internet networks in real time, and helps to analyze the network performance. From Cisco IOS XE 17.16.1a, Cisco ThousandEyes application is supported on Cisco 1000 Series Integrated Services Routers.
Disablement of Weak SSH Algorithms	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
Enhancement to the Show Cellular 0/x/0 Connection Command	From Cisco IOS XE 17.16.1a, the output for the **show cellular 0/x/0 connection** command includes the following parameters: • Access Point Name (APN), and • Cellular Link Uptime
Enhanced support for binary tracing	From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the **show logging process IOS module nhrp** command, without enabling DMVPN event tracing.
Monitoring Application Performance on SD-Routing Devices	In Cisco IOS XE 17.16.1a, you can now monitor TCP and RTP traffic on DMVPN tunnels for IKEv2 traffic using Application Response Time (ART) monitor and Media monitor respectively. This functionality is only supported on DMVPN tunnels with IKEv2 encryption.
Monitoring Crypto VPN solutions on SD-Routing devices	If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts, and events. Having high visibility into the network can help identify errors in real time therefore reducing the network down time.
UTD Container Management for SD-Routing Devices	When Cisco IOS-XE autonomous devices transition to Cisco SD-Routing mode, the Unified Threat Defense (UTD) Container Migration feature ensures that existing container functionalities are preserved. From Cisco IOS XE 17.16.1a you can detect, upgrade, and manage UTD Security Virtual Images through Cisco Catalyst SD-WAN Manager. For devices without pre-existing containers, you can also install and manage UTD images using policy groups.

Feature	Description
Speed Test Enhancement for SD-Routing Devices	From Cisco IOS XE 17.16.1a, Cisco Catalyst SD-WAN Manager enables site-to-site speed tests to measure bandwidth between devices over DMVPN tunnels. These tests check upload speed from the source device to the destination, and measure download speed from destination to the source device.
Support for Enrollment over Secure Transport (EST)	From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the **enrollment http username [http_username] password [http_password]** command.
Support to Configure Code Field Value in OAMPDU Frame	From Cisco IOS XE 17.16.1a release, the Dying Gasp feature enables you to configure the organization code field value in the OAMPDU frame.
Support for Network Slicing on 5G standalone networks	From Cisco IOS XE 17.16.1a, slice-type and slice-differentiator options are introduced for cellular profiles in 5G standalone networks.
Cisco Unified Border Element (CUBE)	
Secure Communications Interoperability Protocol (SCIP) support in CUBE	From Cisco IOS XE 17.16.1a onwards, Secure Communication Interoperability Protocol (SCIP) voice and video codec that ensures secure traffic sessions between the endpoints. **Preview Feature Disclaimer** The Secure Communications Interoperability Protocol (SCIP) feature in Cisco IOS XE 17.16.1a release is available in 'preview' mode as it includes limited functionality or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Cisco Technical Support provides reasonable effort support for features in preview mode. There is no Service Level Objective (SLO) in response times for features in preview mode; response times may be slow.

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)
17.14.x	17.5(1r)	17.5(1r)
17.15.x	17.5(1r)	17.5(1r)

Resolved and Open Bugs in Cisco IOS XE 17.16.x

Open Bugs in Cisco IOS XE 17.16.1a

Table 3: Open Bugs in Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwn32668	L2 traffic go to blackhole due to mac-route originated from blocked node after power-cycle
CSCwn09185	Traffic loss observed on minimal values with time based policy-map.
CSCwn26353	BFD sessions through TLOC-Ext do not come up when IPv6 is dynamically changed.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwn12594	SIG zscaler IPsec - VPN credentials for primary tunnel not created.
CSCwm71639	The cpp_cp_svr crash noticed when configured service-policy to a Dialer interface.
CSCwn24226	GETVPN mismatch in GMs reported across COOP.
CSCwn40906	Devices crash observed when optimizing encrypted traffic with DRE.
CSCwn34457	Post power cycle, unable to login to router due to error Authentication failed.

Identifier	Headline
CSCwn19586	Certificate-based MACSEC flapping when dot1x reauth timers are set and after reloading the device.
CSCwk20995	PPPoE session with sub-interface getting stuck after the reboot.
CSCwm87270	MKA session down with "ICV Verification of a MKPDU failed for" error on one of the interface.
CSCwn39447	SpeedTest might work abnormally after changing system-ip.
CSCwn35476	the cflowd source interface for sub-interface does not get pushed to the device.
CSCwn38464	Unable to configure stream on cellular interface.

Resolved Bugs in Cisco IOS XE 17.16.1a

Table 4: Resolved Bugs in Cisco IOS XE 17.15.1a

Identifier	Headline
CSCwn07540	Devive crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE.
CSCwm56800	FIA Trace Packet Decode Displays Incorrect Value for Fragmentation Offset.
CSCwk78018	Yang model does not handle properly default ikev2 authorisation policy.
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down.
CSCwm48459	Software crash with Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwm89225	CPP crashes After Routing Table Changes.
CSCwk62954	Multiple "match address local interface <int>" not pushed from vmanage under crypto profile.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwh01678	Device FTM crash with SIG enabled.
CSCwk79606	The PKI **trustpoint password** command only allows encryption type 0 and 7 on all IOS XE platforms.
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
CSCwn29062	Traceback log output on the device with "DATACORRUPTION" error logs.
CSCwm62981	Device crashes with PKI "revocation-check ocsp none" enabled.
CSCwn16770	The interface status down after restarting multiple times when autoneg is disabled.

Identifier	Headline
CSCwm74317	'%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI.
CSCwm54978	SIT-SDWAN: Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
CSCwm88350	The **no autostate** command is not available on the device but possible to configure through CLI Add-On.
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call.

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 results 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.