



# 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

## 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
<a href="#">Asymmetric carrier delay</a>	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 <i>Cisco 1000 Series Integrated Services Routers</i> .
<a href="#">Cisco ThousandEyes Enterprise Application Hosting</a>	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.
<a href="#">Configure Source Interface for High Speed Logging</a>	From Cisco IOS XE 17.16.1a, you can configure source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager. You can also enable HSL for your firewall messages, to allow a firewall to log records with minimum impact to packet processing.
<a href="#">DHCP support for MAP-T Customer Edge (CE)</a>	From Cisco IOS XE 17.16.1a onwards, the MAP-T CE functionality is extended to support DHCP.
<a href="#">Disablement of Weak SSH Algorithms</a>	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
<a href="#">Enhancement to the Show Cellular 0/x/0 Connection Command</a>	From Cisco IOS XE 17.16.1a, the output for the <b>show cellular 0/x/0 connection</b> command includes the following parameters: <ul style="list-style-type: none"> <li>• Access Point Name (APN), and</li> <li>• Cellular Link Uptime</li> </ul>
<a href="#">Enhanced support for binary tracing</a>	From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the <b>show logging process IOS module nhrp</b> command, without enabling DMVPN event tracing.
<a href="#">Monitoring Application Performance on SD-Routing Devices</a>	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.
<a href="#">Monitoring Crypto VPN solutions on SD-Routing devices</a>	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.

Feature	Description
<a href="#">Onboard Cisco ThousandEyes Enterprise Agent on SD-Routing Devices</a>	From Cisco IOS XE 17.16.1a, you can configure Cisco ThousandEyes Enterprise agent on SD-Routing devices to gather granular details of network and application performance. This facilitates end-to-end traffic visibility, supporting optimization and troubleshooting.
<a href="#">Speed Test Enhancement for SD-Routing Devices</a>	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.
<a href="#">Support for Enrollment over Secure Transport (EST)</a>	From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the <b>enrollment http username [http_username] password [http_password]</b> command.
<a href="#">Support to Configure Code Field Value in OAMPDU Frame</a>	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.
<a href="#">Support for Network Slicing on 5G standalone networks</a>	From Cisco IOS XE 17.16.1a, slice-type and slice-differentiator options are introduced for cellular profiles in 5G standalone networks.
<a href="#">UTD Container Management for SD-Routing Devices</a>	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.
<b>Cisco Unified Border Element (CUBE)</b>	
<a href="#">Secure Communications Interoperability Protocol (SCIP) support in CUBE</a>	<p>From Cisco IOS XE 17.16.1a onwards, support for Secure Communication Interoperability Protocol (SCIP) voice and video codec is available, that ensures secure traffic sessions between the endpoints.</p> <p><b>Preview Feature Disclaimer</b></p> <p>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.</p>



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

Identifier	Headline
<a href="#">CSCwn34457</a>	Post power cycle, unable to login to router due to error Authentication failed.
<a href="#">CSCwn19586</a>	Certificate-based MACSEC flapping when dot1x reauth timers are set and after reloading the device.
<a href="#">CSCwk20995</a>	PPPoE session with sub-interface getting stuck after the reboot.
<a href="#">CSCwm87270</a>	MKA session down with "ICV Verification of a MKPDU failed for" error on one of the interface.
<a href="#">CSCwn39447</a>	SpeedTest might work abnormally after changing system-ip.
<a href="#">CSCwn35476</a>	the cflowd source interface for sub-interface does not get pushed to the device.
<a href="#">CSCwn38464</a>	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
<a href="#">CSCwn07540</a>	Devive crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPLIVE.
<a href="#">CSCwm56800</a>	FIA Trace Packet Decode Displays Incorrect Value for Fragmentation Offset.
<a href="#">CSCwk78018</a>	Yang model does not handle properly default ikev2 authorisation policy.
<a href="#">CSCwm67178</a>	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
<a href="#">CSCwk42493</a>	Cellular interface in last-resort mode should be admin up, line protocol down.
<a href="#">CSCwm48459</a>	Software crash with Critical process vip_confid_startup_sh fault on rp_0_0 (rc=6).
<a href="#">CSCwm89225</a>	CPP crashes After Routing Table Changes.
<a href="#">CSCwk62954</a>	Multiple "match address local interface &int;" not pushed from vmanage under crypto profile.
<a href="#">CSCwj33723</a>	Config not synced between active and 3rd member of stack.
<a href="#">CSCwh01678</a>	Device FTM crash with SIG enabled.
<a href="#">CSCwk79606</a>	The PKI <b>trustpoint password</b> command only allows encryption type 0 and 7 on all IOS XE platforms.
<a href="#">CSCwm50619</a>	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
<a href="#">CSCwn29062</a>	Traceback log output on the device with "DATACORRUPTION" error logs.
<a href="#">CSCwm62981</a>	Device crashes with PKI "revocation-check ocsp none" enabled.

Identifier	Headline
<a href="#">CSCwn16770</a>	The interface status down after restarting multiple times when autoneg is disabled.
<a href="#">CSCwm74317</a>	'%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI.
<a href="#">CSCwm54978</a>	SIT-SDWAN: Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
<a href="#">CSCwm88350</a>	The <b>no autostate</b> command is not available on the device but possible to configure through CLI Add-On.
<a href="#">CSCwm77426</a>	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.

