Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Cupertino 17.8.x

First Published: 2022-04-22

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.

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 Cupertino 17.8 is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Cupertino 17.8.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	Description
Support for Wi-Fi 6 enablement	Support for Wi-Fi6 is introduced on C1131 models.
Support for LACP on Cisco 1100 Terminal Services Gateway and Cisco 1131 Series	This feature provides support for LACP (Link Aggregation Control Protocol) on Cisco 1100 Terminal Services Gateway and Cisco ISR 1131 Series. LACP helps increase the bandwidth of connections, can be used in multiple locations in the network and facilitates the automatic creation of EtherChannels by exchanging packets between the ethernet ports.
Programmability Features	
IPSec YANG model	This feature introduces an YANG model for the show platform hardware qfp active feature ipsec state command. This model displays the Cisco Quantum Flow Processor (QFP) IPsec state information. You can view the different states and the number of messages exchanged for each state in QFP IPsec. With this information, you can troubleshoot issues related to IPsec flows. For more information about YANG models, see https://github.com/YangModels/yang/tree/master/vendor/cisco/xe
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.8.1a uses the YANG version 1.0; however, you can download the YANG version 1.1 from GitHub at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe folder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG migration process, send an email to xe-yang-migration@cisco.com.
Cube Features	
mTLS Client CN-SAN validation	It is now possible to verify a client through the validation of the common name or subject alternate name fields in its certificate.
Unified Secure SRST: SHA2-Cipher-only Mode	To ensure that only the most robust cipher suites are used, Secure SRST (SCCP) may now be configured to only use TLS 1.2 Cipher Suites. Secure SIP SRST now supports the granular control of cipher suites used for both signaling (TLS) and media (SRTP).
Unified Secure SRST: SIP oAuth Client Registration	IP Phones, Jabber clients, and the Webex app may now failover and register to Secure SIP SRST using OAuth authentication.
VRF-aware Listen Port per Tenant	SIP trunks configured using the CUBE tenant feature may now be configured with a specific listen port, allowing more flexibility in routing inbound calls to the correct trunk. This feature may be used together with VRF interface binding to further control the partition and routing of calls.

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 recommended ROMmon version is 17.6(1r).
- If the manufacturing date is less than 0x2535, you can upgrade to the recommended ROMmon version 17.5(1r) or later.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 to 17.7 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)
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)

Resolved Bugs in Cisco IOS XE 17.8.1a

Bug ID	Description
CSCwb23043	MACsec not working on subinterfaces using dot1q >255
CSCvz34380	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability
CSCwa78020	ZBFW dropping packets as Input VPN ID set to 0 instead of 99. device VPN : 99
CSCwa47219	Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table
CSCwa13553	QFP core due to NAT scaling issue
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
CSCwb11389	NAT translation stops suddenly (ip nat inside doesn't work)
CSCvz98373	ZBFW : FirewallPolicy drops seen with RTSP traffic in steady state
CSCwa26412	ZBFW: OG lookups are missing from device for optimized policy
CSCwa66916	SCCP auto-configuration issues with multiple protocols
CSCwa98047	After device upgrade, dns config set to NONE
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop
CSCvy78501	AAR not working properly as configured SLA classes are not shown under app-route stats
CSCwa36699	Prefetch CRL Download Fails
CSCvz74773	Discrepancies in CLI and GUI interface details (Truncating interface numbers)
CSCvx21819	Keychain macsec key input value 0 should be restricted
CSCwb08186	E1 R2 - dnis-digits cli not working
CSCvt15177	Certificate Signing Request made by IOS-XE never show the Subject Alternate Name
CSCwa07494	IPsec tunnel not passing traffic when IPSec tunnel is sourced from VASI interface
CSCwa67398	NAT translations do not work for FTP traffic
CSCwa93930	Alarms alarm bfd-state-change syslog command is getting rejected while reconfiguring the device.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop
CSCwa92411	Slowness issues caused by intermittent traffic drop on device ingress from GRE tunnel
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop
CSCvz80101	Policy XML pruning without ConfD dependency

Bug ID	Description
CSCvz34668	Static mapping for the hub lost on one of the spokes
CSCwa15085	Router crash due to stuck thread
CSCwa46760	Memory Utilisation value sent 0.6; shows wrong value 60%
CSCwb02851	Device gets crashed consistently with memory corruption with pppoe dailer interface flap
CSCwa84448	Intersite cloudsec enabled packets with 60 byte across devices getting dropped when PTP is enabled

Open Bugs in Cisco IOS XE 17.8.1a

Bug ID	Description
CSCvz65764	Peer MSS value showing incorrect
CSCwa48122	SIP OAuth http request to fetch keys from CUCM fails after bootup as interface is down
CSCwb23632	Command shows 'Not connected to AMP cloud'.
CSCwb40139	Device fails to load bootstrap configuration with @ in the admin password
CSCwb32635	Daemon file is incomplete when running admin-tech
CSCwb11389	NAT translation stops suddenly (ip nat inside does not work)
CSCwb42807	After Enforce Software Version (ZTP) completed successfully, it automatically rolled-back
CSCwb33796	HTTP/DNS client source-interface not used in service VPN for upgrade download request
CSCwb04815	NHRP process taking more CPU with ip nhrp redirect configured
CSCwa72273	ZBFW dropping return packets post device upgrade
CSCwa64955	Loses control connections after installing new enterprise hardware wan device
CSCwa49721	HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb38501	Support IGMP on voice vlan
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb18223	SNMP v2 community name encryption problem
CSCwb16723	Traceroute not working on device with NAT
CSCwb12647	Device crash for stuck threads in cpp on packet processing

Bug ID	Description
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCwb27486	New Key for NBAR app and NBAR category without OGREF optimized
CSCwa84919	Revocation-check crl none does not failover
CSCwb01477	Logging message %IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client fman stats bipc
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address.
CSCwb29362	Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160
CSCwa00293	QFP Crash due to device Flow-Exporter pending query
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route
CSCwb55683	Large number of IPsec tunnel flapping occurs when underlay is restored
CSCwb24123	Registration of spoke fails with dissimilar capabilities to HUB

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.