Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Dublin 17.10.x

First Published: 2022-12-16

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.

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 ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.



Note For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers datasheet.

For information on the End-of-Life and End-of-Sale Announcements for Cisco ASR 1000 Series routers, refer to the ASR 1000 Series End-of-Life and End-of-Sale Notices.



Note Cisco IOS XE Dublin 17.10.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Dublin 17.10.x release series.

Instead, use the **install add file bootflash:<file name> activate commit** command to upgrade using a single image that combines all the separate packages improves the boot time.

Starting from IOS XE 17.6, the ISSU on Cisco ASR 1000 Series Aggregation Services Routers will migrate to an install workflow that provides step-by-step upgrade/downgrade commands.

The ISSU load version commands will be deprecated and these commands include:

- abortversion
- acceptversion
- checkversion
- commitversion
- config-sync
- image-version
- loadversion
- runversion.

Additionally, dual IOSd ISSU commands and Bundle mode ISSU workflows will also be disabled.

Note The In-Service Software Upgrade (ISSU) in ASR 1000 is being migrated to an install workflow that provides a step-by-step upgrade/downgrade. Starting from IOS-XE 17.6.1, the following items will be disabled:

- The ISSU load version command set including **issu loadversion, issu runversion, issu acceptversion,** and **issu commitversion.**
- Dual IOSd ISSU commands.
- Bundle mode ISSU workflow.

Note Starting with Cisco IOS XE 17.3.2, 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 Features

There are no new hardware features for this release.

New and Changed Software Features

Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.10.1a

Feature	Discription
Layer 2 BGP VXLAN EVPN	Border Gateway Protocol (BGP) Ethernet VPN (EVPN) Virtual Extensible LAN (VXLAN) is a campus and data center network solution for Cisco devices that run on Cisco IOS XE software. This feature allows Layer 2 segments to be supported across an IP core therefore allowing improved scalability with infrastructure. It also provides all the benefits of Layer 3 topologies.
New Filtering Options for show isis database command	This enhancement includes new filtering options for the **show isis database** command to support increased scale, view information on neighbours or prefixes and display both router capability information and raw TLV encoding.
Segment Routing Absolute One-Way Link Loss Measurement for GRE-IPSec Tunnel	This feature provides a mechanism for link loss measurement for point-to-point GRE-IPSec tunnel and identifies paths that meet specified loss criteria.
Stateful Network Address Translations using VRF with CGN	This feature introduces support to enable stateful NAT64 translations with Carrier Grade NAT (CGN) enabled within Virtual routing and forwarding (VRF) instances in a network.
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.
Cisco Unified Border Element (CUBE) Features	
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.

Resolved and Open Bugs for Cisco IOS XE 17.10.x

Resolved Bugs for Cisco IOS XE 17.10.1a

Bug ID	Description
CSCwd06372	Rapid memory exhaustion due to excessive logging.
CSCwc78021	Standby WLC crash @ fman_acl_remove_default_ace.

Bug ID	Description
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= "<interrupt level>".
CSCwb55514	Crash seen after enabling **platform qos port-channel-aggregate**.
CSCwb35303	X25 FRMR seen when switching from XOT to low speed serial.
CSCwc77981	Device crashed - track the fman-fp's memory leak caused by cond-debug.
CSCwd03869	CEF DPI load-balancing causes out of order packets.
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.
CSCwc70511	Router reloads unexpectedly during NHRP processing.
CSCwc26669	TLB miss for lock address during FNF cache lookup.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.

Open Bugs for Cisco IOS XE 17.10.1a

Bug ID	Description
CSCwd25107	Interface VLAN1 placed in "shutdown" state when configured with **ip address pool**.
CSCwd23810	IOS-XE: A high CPU utilization caused by NHRP.
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwd30578	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
CSCwd61255	Data Plane Crash on device when making QoS configuration changes.
CSCwd63984	High Churn rate results in IPSEC failing triggering a crash.
CSCwd68111	Device object group called in ZBFW gives error after upgrade.
CSCwc65697	Device crashing and restarting during call flow with new image.
CSCwd53205	IKEv2 The RRI routes are intermittently disappearing from a FlexVPN hub.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwa96399	Configuring "entity-information" xpath filter causes syslogs to print, does not return data.

Bug ID	Description
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.

ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html.

Related Documentation

- Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers
- Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers
- Configuration Guides for ASR 1000 Series Aggregation Services Routers
- Product Landing Page for ASR 1000 Series Aggregation Services Routers
- Datasheet for ASR 1000 Series Aggregation Services Routers
- Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers
- Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide
- Field Notices
- Cisco Bulletins

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.

© 2022 Cisco Systems, Inc. All rights reserved.