Release Notes for Cisco ASR 1000 Series, 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.

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 Cupertino 17.8.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Cupertino 17.8.x release series.



Note Starting from IOS XE 17.5, the following consolidated platforms (or with dual IOSd) will move to monolith packaging and will not enable upgrade/downgrade using separate packages:

- ASR 1001-X
- ASR 1001-HX
- ASR1002-X
- ASR 1002-HX

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.x, 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 17.8.1a

Feature	Description
Download AnyConnect Profiles with IPSec IKEv2 VPN	This feature allows you to configure Internet Protocol Security (IPSec)-Internet Key Exchange (IKEv2) VPN to download AnyConnect profiles over SSL, for IOS-XE headends.
Enabling SNMP Trap On L2TP Tunnel Level	This feature introduces the snmp-server enable traps l2tun tunnel command using which you can enable SNMP Trap on a L2TP tunnel level.
MACSec Fallback Key Support	This feature introduces a fallback mechanism to re-establish the MKA session when it fails because of primary Pre-Shared Key (PSK) mismatch. This fallback mechanism can be configured by using the mka pre-shared-key key-chain command.
Segment Routing Flexible Algorithm Prefix SID Redistribution	When prefixes are redistributed between protocols, only Prefix SIDs for SR algorithm 0 (regular SPF) are available. With this feature, prefix SIDs are provided for all supported algorithms when a prefix is redistributed. This feature is enabled automatically when you configure redistribution of routes with strict or Flexible Algorithm SIDs.
Support for bidirectional debugging	You can now enable bidirectional debugging of traffic using debug platform condition match command.
Support for IPv6 Next Hop with BGP VPNv4, VPNv6, and EVPN Prefixes	This feature allows you to use the Multiprotocol BG (BGP-MP) capability to carry VPNv4 Network Layer Reachability Information (NLRI) in an IPv6 next hop. This helps to reduce the operating cost by carrying both VPNv4 and IPv6 over the same BGP session. VPNv4 or EVPN prefixes with IPv6 next hops and VPNv6 prefixes with non-IPv4-mapped-IPv6 next hops are not supported by the BGP peers. It is either reflected to an iBGP peer or advertised to an ASBR.
Support for Thousand Eyes Application on Routing Platforms	Cisco ThousandEyes application is a cloud-ready, enterprise network-monitoring tool that provides an end-to-end view across networks and services. This tool helps in analyzing the network performance and provides insights into the Internet and enterprise networks.
Cisco Unified Border Element (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.
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.
Programmability Feature	

Feature	Description
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.

Resolved and Open Bugs for Cisco IOS XE 17.8.x

Resolved Bugs for Cisco IOS XE 17.8.1a

Bug ID	Description
CSCwa84448	Intersite cloudsec enabled packets with <60 byte across devices getting dropped when PTP is enabled
CSCvw70446	ZBFW:Crash pointing to fw_base_flow_create () seen on the device
CSCwb22552	Abnormal Kerlog log is produced when port in shutdown state
CSCwa67851	Router traceback and reload when different encapsulation used on xconnect interfaces.
CSCvz95158	ASR1K-HX: IPSec Led doesn't lit even though module is correctly installed
CSCwa15085	Router Crash due to Stuck Thread with appnav-xe dual controller mode.
CSCvz62601	High CPU on LC process mcpcc-lc-ms and link flaps
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. SDWAN VPN : 99
CSCwa47219	Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table
CSCwa13553	Device 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
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)

Bug ID	Description
CSCvx21819	Keychain macsec key input value 0 should be restricted
CSCvt15177	Certificate Signing Request made by IOS-XE never show the Subject Alternate Name
CSCwa93930	"alarms alarm bfd-state-change syslog" command is getting rejected while reconfiguring the device.
CSCwa67398	NAT translations do not work for FTP traffic in the device
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes)
CSCwa92411	Slowness issues caused by intermittent traffic drop on ISRv ingress from GRE tunnel
CSCvz80101	Policy XML pruning without ConfD dependency
CSCvz34668	Static mapping for the hub lost on one of the spokes
CSCwa46760	Memory Utilisation value sent 0.6 always to vManage; shows wrong value 60%

Open Bugs for Cisco IOS XE 17.8.1a

Bug ID	Description
CSCwa97951	Basic feature template fails on device with TenGig interface due to negotiation auto
CSCwa95092	When Object-group used in a ACL is updated, it takes no effect
CSCwb26560	Linecard crashed on doing issu-mdr-force issu.
CSCwb04815	NHRP process taking more CPU with ip nhrp redirect configured
CSCvz65764	Peer MSS value showing incorrect
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address.
CSCwb11389	NAT translation stops suddenly(ip nat inside doesn't work)
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA
CSCwb42807	After Enforce Software Version (ZTP) completed successfully, it automatically rolled-back
CSCwa72273	ZBFW dropping return packets post upgrade.
CSCwa64955	Device loses control connections after installing new enterprise hardware wan edge cert
CSCwa49721	SDWan HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map

Bug ID	Description
CSCwb18223	SNMP v2 community name encryption problem
CSCwb16723	Traceroute not working on device with NAT
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored
CSCwb12647	Device crash for stuck threads in cpp on packet processing
CSCwb24123	Registration of spoke fails with dissimilar capabilities w.r.t to HUB.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route
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
CSCwb40139	Device fails to load bootstrap configuration with '@' in the admin password
CSCwb29362	Evaluation of IOS-XE for OpenSSL CVE-2022-0778 and CVE-2021-4160
CSCwb32635	daemon file is incomplete when running admin-tech
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

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.



Note After upgrading the ROMmon to version 17.3(1r), you cannot revert it to a version earlier than 17.3(1r) for the following platforms:

- ASR 1001-X
- ASR 1001-HX
- ASR 1002-HX

This restriction is only applicable for these platforms. If you have upgraded to ROMmon version 17.3(1r) on any other platform, reverting to an earlier version of ROMmon is permitted and does not cause any technical issues.

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.