Release Notes for Cisco ASR 1000 Series, Cisco IOS XE 17.15.x

First Published: 2024-04-30

Last Modified: 2025-03-07

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 17.15.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.15.x release series.

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 in Cisco IOS XE 17.15.2a

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.15.1a

Feature	Description
Enhanced NAT Management	From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the ip nat translation max-entries cpu command. This feature also enables streamlining NAT synchronization in redundant systems using the **ip nat settings redundancy optimized-data-sync** command.
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.15.1a, Segment Routing over IPv6 dataplane supports these functionalities: • IS-IS Microloop Avoidance • IS-IS Loop-Free Alternate Fast Reroute • IS-IS Topology-Independent Loop-Free Alternate Fast Reroute • OAM Traffic Engineering
Enhancement to SGACL Logging	This feature enhances the Security Group-based Access Control List (SGACL) logging capability by using High Speed Logging (HSL) for Cisco IOS XE devices. SGACL logging through HSL provides an efficient and reliable logging method for security events in network environments with high-traffic volumes. For more information, seeCisco IOS Security Command Reference Guide
Ethernet VPN: Enhancement to Specify Gateway IP Address	From Cisco IOS XE 17.15.1a, you can use export maps to specify the gateway IP address (GW IP address) in the Ethernet VPN (EVPN) IP prefix route and influence how routes are exported. This enhancement enables the device to make accurate routing decisions based on the specified GW IP address.
Absolute Path for HTTP or HTTPS File Transfer	The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the **copy** command. From Cisco IOS XE 17.15.1a, you must provide the absolute file path when you execute the **copy** command, to transfer the file.
Monitoring SD - Routing Alarms	From Cisco IOS XE 17.15.1a, network administrators can monitor SD-Routing device alarms on Cisco Catalyst SD-WAN Manager. This feature enables SD-Routing devices to record and store various alarms generated by control components and routers. For more information, see Cisco SD-Routing Command Reference Guide.
Network-Wide Path Insights on SD - Routing Devices	Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network.

Feature	Description
Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF	You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic.
Enabling Flow Level Flexible NetFlow Support for SD-Routing Devices	The Flow-level Flexible NetFlow (FNF) feature allows you to monitor the NetFlow traffic and view all the flow-level FNF data that is captured including application-level statistics.
Seamless Software Upgrade for SD-Routing Devices	This feature explains how to seamlessly upgrade and onboard an existing Cisco Routing device into the Cisco SD-WAN infrastructure.
Cisco Umbrella Scope Credentials	From Cisco IOS XE 17.15.1a, this feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.
SD-Routing License Management	This release introduces license management support for SD-Routing devices. The supported licensing workflows include license assignment or configuration, license use, and license usage reporting. Depending on the device, these workflows are performed in the Cisco Catalyst SD-WAN Manager or on the device.

Resolved and Open Bugs for Cisco IOS XE 17.15.x

Resolved Bugs for Cisco IOS XE 17.15.2a

Bug ID	Description
CSCwm30984	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device - CCE changes.
CSCwm31516	DSMP layer is unable to close EDSP channels if a call is disconnected before connect.
CSCwk85704	SD-Routing:"match traffic-category " through vManage add-on CLI push failed.
CSCwm07396	Few BFD sessions down after clear mka session on client.
CSCwm07651	An IOS XE Router running as a cEdge may experience an unexpected reset due to dbgd process.
CSCwm11819	Router Crash due to SIGSEGV | fman_fp_image fault on fp_0_0 (rc=139)
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwk81360	Cisco IOS-XE Router can reboot unexpectedly while configuring NAT Static Translation.
CSCwk52106	SNMP reports incorrect Transmit Power / Receive Power values for 100G AOC cables.

Bug ID	Description
CSCwm41535	DSP occasionally crashes when pcm capture is enable
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device.
CSCwm05524	Unexpected Reload Due to "cpp-mcplo-ucode" Process When Handling Fragments With SRv6 Routing.
CSCwk50488	Memory leak in fman_rp under acl_db.
CSCwk64137	High IRAM utilization at 99% in scaled flows.
CSCwk70630	17.12.02 Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwm13223	IOS-XE 17 Crashes in IOSd Due to Malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog.
CSCwi87546	Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwk53438	17.15: Process crash seen on SD-Routing TSN platform + Permission Denied errors.
CSCwk72795	Router has no statistics for the SBFD protocol.
CSCwm12851	IOS-XE 17.12.3 uses 3DES as default rekey algorithm for GETVPN.
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats.
CSCwk61133	Process IOMd memory leak due to POE TDL message.
CSCwk87452	Procyon synchronize DTL does not wait until complete due to compiler optimization.

Open Bugs for Cisco IOS XE 17.15.2a

Bug ID	Description
CSCwn13650	Multiple address range support in a local pool.
CSCwm62981	Router crashes with PKI "revocation-check ocsp none" enabled.
CSCwn52179	Traffic with TTL 2 is punted to CPU when CEF holds MPLS labels set to None.
CSCwm58500	MIP 100 stuck in booting state after ROMMON upgrade using 17.3(1r) rommon file.
CSCwn80360	vManage 20.12.4.0.03 removes NAT egress-interface option from cEdge config - CRYPTO yang changes.
CSCwn46221	"peer reactivate" CLI for FlexVPN tunnel on device does not work.

Bug ID	Description
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwn07671	Tracker group with IP and DNS name tracker elements goes down when DNS query is failing
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
CSCwn80352	vManage 20.12.4.0.03 removes NAT egress-interface option from cEdge config - NAT yang changes.
CSCwn44339	IOS XE 17 - Router crash due to failed DLC license conversion when contacting CSSM.
CSCwm74060	IOSD chasfs task crashes when retrieving platform info.
CSCwn92976	PPP is not establishing when l2tp over IPsec.
CSCwn53778	Unexpected reload on router (FMAN QOS).
CSCwn40794	IOS-XE crash PKI: Failed to load cert chain for trustpoint.
CSCwn31739	Router crashes when EPC is configured on 100Gb link.
CSCwn65589	DMVPN Tunnel bounces a 2nd time after RP3 failover and recovery.
CSCwn59851	Unexpected reload Critical process linux_iosd_image fault on rp_0_0 (rc=139).
CSCwn83135	SD-WAN: Unable to Reach Inband Management IP on Standby Firewall HA Device.
CSCwn36533	vmanage_system and loopback65529 interfaces using DOD ip range and need to disable it.

Resolved Bugs for Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwj51700	CPP crashes after re-/configuring "ip nat settings pap limit ... bpa" feature in high QFP state.
CSCwk42634	%PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6).
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk16333	cEdge repeatedly crashing in FTMd Due to FNF Flow Add.

Bug ID	Description
CSCwj95633	SDWAN: SAIE Application - No Data to Display over Vmanage for IOS XE router.
CSCwj96852	Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC.
CSCwk39131	cEdge crashed when issuing "show sdwan ftm next-hop chain all" .
CSCwk22225	FTMd crashes after receiving credentials feature template update from vmanage.
CSCwj48909	17.14 Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk45165	fman_fp Memory Leak on device.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwk56504	In NAT64 scenario, IPv4 packets that needs translation might be dropped by router.
CSCwj90614	High CPU utilisation for confd_cli.
CSCwi81026	SDWAN BFD Sessions Flapping During IPSec Rekey in Scaled Environment.
CSCwk39268	[2.3.7.x] sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11.
CSCwj76662	cEdge - High memory utilization due to "ftmd" process.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwj96092	20/17.14: ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	cEdge unexpectedly reloads due to a crash in 'vdaemon' process.
CSCwi99454	cEdgeFNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive.
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwj02401	cEdge: Router reloaded when generating admin tech while processing very high number of flows.
CSCwk19725	Add FNF cache limit for show sdwan app-fwd flows for CSCwj02401.
CSCwj86794	Router crashes while processing an NWPI trace.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.

Bug ID	Description
CSCwj67591	20.14:SD-Routing Brownfield - chassis activate effective only after second re-try - with new uuid.
CSCwj54638	Device : EVC Q-in-Q configuration may filter out certain vlans.
CSCwj32347	DIA Endpoint tracker not working with ECMP routes.

Open Bugs for Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwk79454	Endpoint Tracker does not fail if default route is removed.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwk95044	17.12.03. CSCwj42249.SPA.smu.bin drops when Packet Duplication link fails-over.
CSCwk86355	File transfer fails from vManage 20.9.5 /home/admin to cEdge 17.6.5 bootflash: "lost connection".
CSCwk75733	Custom Applications may not be programmed properly.
CSCwk49806	Router running IOS 17.06.05 rebooted unexpectedly due to process NHRP crash.
CSCwi87546	Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwk98578	Router / XE 17 / GETVPN ipv6 crypto map not shown in interface configuration.
CSCwk89256	vManage/IOS-XE 17.9.3 speed mismatch in IOS-XE configuration after device template push for router.
CSCwk62954	Multiple "match address local interface <int>" not pushed from vmanage under crypto profile.
CSCwj87028	cflowd showing custom APP as "unknown" for egress traffic when using DRE Opt.
CSCwk81360	Cisco IOS-XE Router can reboot unexpectedly while configuring NAT Static Translation.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device.
CSCwk74298	cEdge denied for template push and some show commands with error application communication failure.
CSCwm00309	Packets not hitting the correct data policy after modifying the action of a sequence.
CSCwk98006	Unable to Establish NAT Translations with ZBFW enabled.

Bug ID	Description
CSCwf62943	cEdge: system image file is not set to packages.conf when image expansion fails due to disk space.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.
CSCwk70630	17.12.02 Cannot import device certificate.
CSCwk85704	SD-Routing:"match traffic-category " through vManage add-on CLI push failed.
CSCwm12851	IOS-XE 17.12.3 uses 3DES as default rekey algorithm for GETVPN
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwk97092	17.15: MKA session not coming up after shut/no shut with EVC.
CSCwm07564	cEdge: data-policy local-tloc-list breaks RTP media stream.
CSCwm08545	Centralized Policy Policer worked per PC on the same site not per site/vpn-list.
CSCwm13223	IOS-XE 17 Crashes in IOSd Due to Malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog.

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-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.

© 2024–2025 Cisco Systems, Inc. All rights reserved.