



# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE 17.14.x

---

**First Published:** 2024-04-30

## 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 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 17.14.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.14.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 17.14.1a

Feature	Description
<a href="#">DC-PE Router in Cisco ACI to SR-MPLS Hand-off</a>	From Cisco IOS XE 17.14.1a, Cisco ASR 1000 Series Aggregation Services Routers and Cisco Catalyst 8500 Series Edge Platforms can be used as intermediate DC-PE devices in Cisco ACI to SR-MPLS hand-off interconnection. SR-MPLS hand-off is an interconnection option that enables Cisco ACI to WAN interconnect using Segment Routing (SR) MPLS underlay.

Feature	Description
Enhanced IS-IS Fast Flooding	The IS-IS Fast Flooding feature optimizes LSP transmission to accelerate network convergence by dynamically adjusting the LSP rate based on receiver capability. From Cisco IOS XE 17.14.1a, IS-IS Fast Flooding can be configured using the <b>router isis lsp-fast-flooding</b> command. The LSP transmission can be further customized with arguments such as <b>max-lsp-tx</b> , <b>psnp-interval</b> , and <b>per-interface</b> within the same router isis command, and enhanced by using the <b>isis remote-psnp-delay</b> command. This feature is disabled by default, and requires manual configuration to enable.
Enhancement to the <b>show reload-history</b> Command	From Cisco IOS XE 17.14.1a, the <b>show reload-history</b> command is modified to <b>show reload history</b> . The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.
Increase in L2TPv3 Scalability	From Cisco IOS XE 17.14.1a, the capacity for unidimensional scalability of L2TPv3 tunnel is increased to 12,000 for the following platforms: <ul style="list-style-type: none"> <li>• Cisco ASR 1000 Series Aggregation Services Routers using RP3 with ESP200-X and ESP100-X</li> <li>• Cisco Catalyst 8500 Series Edge Platforms</li> </ul> The scalability is increased to 8000 for Cisco Catalyst 8500L-8S4X Platform.
IP Endpoint Delay Measurement and Liveness Monitoring	This feature enables you to measure the end-to-end delay and monitor liveness towards either a specified IPv4 or IPv6 endpoint. From Cisco IOS XE 17.14.1a, you can be configure this feature using the performance-measurement endpoint and performance-measurement delay-profile endpoint commands.
QFP Drops Threshold and Warning	From Cisco IOS XE 17.14.1a, this feature enables you to configure the warning threshold for each drop cause, and the total QFP drop in packets per second. If the configured threshold exceeds, then a rate-limited syslog warning is generated. You can configure the threshold using the <b>platform qfp drops threshold</b> command.

Feature	Description
<a href="#">Support for Suite B Ciphers with GET VPN</a>	<p>From Cisco IOS XE 17.14.1a, this enhancement introduces support for Suite B ciphers with GET VPN on the following platforms and its corresponding models:</p> <ul style="list-style-type: none"> <li>• Cisco ASR 1000 Series Aggregation Services Routers: <ul style="list-style-type: none"> <li>• ASR 1000 with ESP100-X</li> </ul> </li> <li>• Cisco Catalyst 8300 Series Edge Platforms: <ul style="list-style-type: none"> <li>• C8300-1N1S-4T2X</li> <li>• C8300-2N2S-6T</li> </ul> </li> <li>• Cisco Catalyst 8200 Series Edge Platforms: <ul style="list-style-type: none"> <li>• C8200L-1N-4T</li> </ul> </li> <li>• Cisco Catalyst 8500 Series Edge Platforms: <ul style="list-style-type: none"> <li>• C8500-12X4QC</li> <li>• C8500L-8S4X</li> </ul> </li> <li>• Cisco 1000 Series Integrated Services Routers: <ul style="list-style-type: none"> <li>• C1131</li> <li>• C112X</li> <li>• C116X</li> <li>• C111X</li> </ul> </li> </ul>
<a href="#">Configuration Group Enhancements</a>	<p>This release introduces support for the following in Cisco SD-WAN Manager:</p> <ul style="list-style-type: none"> <li>• Transport Profiles</li> <li>• Management Profile</li> <li>• Service Profile</li> <li>• CLI Profile</li> <li>• Policy Object Profile</li> </ul>

Feature	Description
Support to Configure VPN Solutions for SD-Routing devices	<p>This release introduces support for the following VPN solutions:</p> <ul style="list-style-type: none"> <li>• FlexVPN</li> <li>• GETVPN</li> <li>• DMVPN</li> <li>• L3VPN</li> </ul> <p>These VPN solutions can be configured by using <b>Configuration &gt; Configuration Groups &gt; CLI Add-on Profile</b> option in Cisco SD-WAN Manager.</p>
YANG Configurational Model Support for SD-Routing Devices	<p>This release introduces support for the following YANG Configurational Models:</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• MPLS</li> <li>• RSVP</li> <li>• SNMP</li> <li>• AAA</li> <li>• QOS</li> <li>• ACL</li> <li>• DHCP</li> </ul>
<a href="#">View Unmodelled Commands on SD-Routing Devices</a>	After an SD-Routing device is deployed, you can view the unmodelled commands on Cisco SD-WAN Manager. The list of unmodelled commands are regenerated when the device reboots.
<a href="#">Configure Secure Service Edge</a>	Secure Service Edge is a cloud solution that provides seamless, transparent, and secure Direct Internet Access (DIA) to protect against internet-based threats. This solution can be configured through Policy Groups by using Cisco SD-WAN Manager.
<a href="#">Voltage and Current Metrics</a>	Power Entry Module (PEM) sensors are critical components in the device that are responsible for monitoring various aspects of the power supply, such as voltage, current, and sometimes temperature, to ensure the device operates within safe and efficient parameters. From Cisco IOS XE 17.14.1a, you can use the show environment command to display the PEM sensor readings in mV (milli-volt) and mA (milli-ampere) for your devices.
<b>Programmability Features</b>	
gNMI: Stream Subscriptions with On-Change Mode	gNMI telemetry supports on-change subscriptions on the same set of models as other telemetry protocols.
gNMI - SubscribeResponse with sync_response	The sync_response is a boolean field that is part of the SubscribeResponse response message. The sync_response message is sent after the first update message.

Feature	Description
<b>Cisco Unified Border Element (CUBE) Features</b>	
<a href="#">Secure SIP with TLS 1.3 support</a>	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of <a href="#">Transport Layer Security (TLS) version 1.3 and associated cipher suites</a> .

## Resolved and Open Bugs for Cisco IOS XE 17.14.x

### Resolved Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
<a href="#">CSCwh94906</a>	Device WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
<a href="#">CSCwi49846</a>	ftmd crashed when SIG GRE tunnels configs are removed.
<a href="#">CSCwi55725</a>	CLI config group issue.
<a href="#">CSCwi61369</a>	Device may unexpectedly reload due to SIGABRT.
<a href="#">CSCwi35716</a>	AAR backup preferred color not working as expected.
<a href="#">CSCwi53306</a>	Unknown appID in ZBFW HSL log.
<a href="#">CSCwf84567</a>	Unexpected reload after reconnecting.
<a href="#">CSCwi14178</a>	Failed to connect to device: x.x.x.x Port: 830 user: vmanage-admin error: Connection failed.
<a href="#">CSCwj25493</a>	Device crashed twice with Critical process linux_iosd_image fault on rp_0_0
<a href="#">CSCwi40603</a>	Memory leak in the Crypto IKMP process.
<a href="#">CSCwf08658</a>	Edge devices will flap the BFD sessions if we are in a non-equilibrium state and have symmetric NAT.
<a href="#">CSCwi35177</a>	Device crash caused by continuous interface flap, interface associated with many IPSec interfaces.
<a href="#">CSCwj34010</a>	TLOC extension is missing on the interface in device leading to incorrect control.
<a href="#">CSCwi60266</a>	Device with enterprise certificates not forming control connections with controllers after upgrade.
<a href="#">CSCwi67983</a>	Tracker state log is missing when DNS Query fails.
<a href="#">CSCwi53951</a>	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a device reboot.
<a href="#">CSCwb25507</a>	CWMP: Add vendor specific parameter for NBAR protocol pack version.

Identifier	Headline
<a href="#">CSCwi53549</a>	Device crash with reason: Critical process fman_fp_image fault on fp_0_0 (rc=134).
<a href="#">CSCwi82548</a>	Crash in IKEv2 Cluster Load Balancer.
<a href="#">CSCwi51381</a>	TrapOID of CISCO-BFD-STATE-CHANGE is different from MIB file.
<a href="#">CSCwh09033</a>	Device unable to boot with module.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwi78365</a>	Trim installed certificate on upgrade.
<a href="#">CSCwi85293</a>	IKEv2 IPv6 Cluster Load balance: Secondary in cluster unable to connect to cluster in case of FVRF.
<a href="#">CSCwi86698</a>	No error message while using multicast address as system-ip in device.
<a href="#">CSCwj06622</a>	Segmentation fault and core files are seen on OS in controller-managed due to speedtest.
<a href="#">CSCwi16111</a>	IPv6 TCP adjust-MSS not working after delete and reconfigure.
<a href="#">CSCwi62230</a>	SIG tunnel: 'SIG STATE' is showing blank value.
<a href="#">CSCwf98902</a>	Unexpected reboot on OS during longevity test.
<a href="#">CSCwj27545</a>	Device crashing due to ftmd.
<a href="#">CSCwi62239</a>	%MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback management VRF then removing it.

### Open Bugs for Cisco IOS XE 17.14.1a

Identifier	Headline
<a href="#">CSCwj04575</a>	Device crashed during SNMPwalk when removing SFP.
<a href="#">CSCwj25508</a>	Device reports incorrect DOM values over SNMP.
<a href="#">CSCwj48393</a>	Service with no priority is not working as expected.
<a href="#">CSCwj48421</a>	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: received IPSEC packet has an invalid SPI.
<a href="#">CSCwj03621</a>	Ping with smaller packet size is failing on MACSEC enabled port.
<a href="#">CSCwj09284</a>	Unexpected reboot in device due to SSL.
<a href="#">CSCwj40589</a>	Endpoint tracker using DNS does not log DOWN message when DNS server reachability is lost.
<a href="#">CSCwj26085</a>	Control connections in TLS with mode manage goes to trying state with UTD.
<a href="#">CSCwj45177</a>	"dmidecode: command not found" error seen executing <b>show certificate validity</b> .

Identifier	Headline
CSCwj34578	NAT46 translations are dropped when device is also Carrier Supporting Carrier CE.
CSCwi81026	BFD Sessions Flapping During IPSEC Rekey in Scaled Environment.
CSCwj45130	Segmentation Fault - Process = IPSEC dummy packet process.
CSCwi59854	<b>show policy service-path</b> command gives inconsistent results with app name specified.
CSCwj02661	UTD signature update failure and device not recording the update.
CSCwj43905	Unexpected reboot due to uCode failure.
CSCwj02628	Speed-test not working for the device.
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented.
CSCwj40223	AppRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns the wrong order.
CSCwj49946	Device   cpp-mcplo-ucode   None PPPoE get session.
CSCwj32347	DIA Endpoint tracker not working with ECMP routes when Loopback is used as Source.
CSCwj27108	Device not balancing traffic to default route.
CSCwj49941	DNS-snoop-agent has TCAM entry with all zeros for some regex patterns.
CSCwj31354	Template push failure due to service timestamps.
CSCwj30334	CVLA uCode crash when attempting merge on used block.
CSCwj13681	Device can only store 64 FQDN patterns, but the configuration allows entry of more than 64.

## 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 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.

