Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE 17.15.x

First Published: 2024-08-27

Last Modified: 2025-03-07

Full Cisco Trademarks with Software License

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 17.15.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE 17.15.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 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

Table 1: New Software Features

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.
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 Software Defined (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 Software Defined (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.
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.
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.
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.

Note From Cisco IOS XE Release 17.9.1a, guestshell is removed from the IOS XE software image. As a result, Zero Touch Provisioning (ZTP) python script is no longer supported on Cisco 1000 Series Integrated Services Routers. If you need to use guestshell, then download it from https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads. For more information, see Guestshell installation procedure.

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 manufactured ROMmon version is 17.6(1r) or higher.
- If the manufacturing date is less than 0x2535, the ROMmon will be automatically upgraded to 17.5(1r) or above when the Cisco IOS XE 17.9.x release is installed.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 or later is 17.5(1r) or later.

Note To upgrade to Cisco IOS XE Dublin 17.12.x, follow these steps:

1. If you are on a device that is running software version between Cisco IOS XE 16.x to Cisco IOS XE 17.4.x, upgrade to any IOS XE image between Cisco IOS XE 17.5.x to Cisco IOS XE 17.10.x.
2. After performing step a, upgrade to Cisco IOS XE 17.12.x.
3. For devices that are running on software version Cisco IOS XE 17.5.x or later, you can upgrade to Cisco IOS XE 17.12.x directly.

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)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
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)
17.9.x	17.5(1r)	17.5(1r)
17.10.x	17.5(1r)	17.5(1r)
17.11.x	17.5(1r)	17.5(1r)
17.12.x	17.5(1r)	17.5(1r)
17.13.x	17.5(1r)	17.5(1r)
17.14.x	17.5(1r)	17.5(1r)
17.15.x	17.5(1r)	17.5(1r)

Resolved and Open Bugs in Cisco IOS XE 17.15.x

Resolved Bugs in Cisco IOS XE 17.15.2a

Table 3: Resolved Bugs in Cisco IOS XE 17.15.2a

Bug ID	Description
CSCwk86062	Modem locks up after reboot of router, modem reset or cellular profile change.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SD-WAN Manager tunnels.
CSCwm31516	DSMP layer is unable to close EDSP channels if a call is disconnected before connect.

Bug ID	Description
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - lock id of 0 released.
CSCwk81360	Cisco IOS-XE router can reboot unexpectedly while configuring NAT static translation.
CSCwk53438	Process crash seen on SD-Routing TSN platform, permission denied errors.
CSCwk85704	match traffic-category through SD-WAN Manager add-on CLI push failed.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk75459	MGCP GW fails to respond with 250 OK when there is a delay from the dataplane in gathering statistics.
CSCwk64137	High IRAM utilization at 99% in scaled flows.
CSCwk70630	Cannot import device certificate.
CSCwm07651	An IOS XE router running as a cEdge may experience an unexpected reset due to dbgd process.
CSCwk61133	Process IOMd memory leak due to POE TDL message.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on router.
CSCwm30984	SD-WAN ZBFW TCAM misprogramming after rules are reordered on router - CCE changes.
CSCwm05524	Unexpected reload due to cpp-mcplo-ucode process when handling fragments with SRv6 routing.
CSCwk50488	Memory leak in fman_rp under acl_db.
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE.
CSCwm13223	Device crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog.

Open Bugs in Cisco IOS XE 17.15.2a

Table 4: Open Bugs in Cisco IOS XE 17.15.2a

Bug ID	Description
CSCwm48190	Memory leak under vDaemon process.
CSCwm62981	Device crashes with PKI **revocation-check ocsp none** enabled.
CSCwn77224	Issue with ethernet/gig interface with second-dot1q is not working as expected.
CSCwn80360	Device removes NAT egress-interface option from cEdge config - CRYPTO yang changes.

Bug ID	Description
CSCwn35772	CCP crashed during UTD policy config application.
CSCwn17454	Band-select feature not working for the LM960 modem.
CSCwe87276	Telit firmware regression break introduced with 32.00.116 FW.
CSCwn46221	**peer reactivate** CLI for FlexVPN tunnel on device does not work.
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.
CSCwn54408	radio-profile config can not be shutdown.
CSCwn16770	Interface status down after restarting multiple times when autoneg is disabled.
CSCwn38464	Unable to configure stream on cellular interface.
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwm67178	Cannot configure MD5 for the hash under the IKEv2 proposal when compliance shield is disabled.
CSCwn80352	Device removes NAT egress-interface option from cEdge config - NAT yang changes.
CSCwm74060	IOSD chasfs task crashes when retrieving platform information.
CSCwn82715	DSL SFP: VDSL/ADSL lines are flapping in customer site.
CSCwn92976	PPP is not establishing when l2tp over IPsec.
CSCwi40697	Modem may not come back up from FW upgrade with LM960A18 and FN980 modems.
CSCwn40794	Device crash PKI: Failed to load cert chain for trustpoint.
CSCwm88350	**no autostate** command is not available on CLI C1121X-8PLTEP but possible to configure via CLI Add-On.
CSCwn15736	See UNDEFINED profile 3 created when SIM or FW is switched.
CSCwn31739	Device crashes when EPC is configured on 100Gb link.
CSCwn65589	DMVPN tunnel bounces for the second time after RP3 failover and recovery.
CSCwn59851	Unexpected reload critical process linux_iosd_image fault on rp_0_0 (rc=139).
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwn83135	Unable to reach inband management IP on standby firewall HA device.

Bug ID	Description
CSCwn36533	Device interface using DOD ip range.

Resolved Bugs in Cisco IOS XE 17.15.1a

Table 5: Resolved Bugs in Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwj83844	Default queue size is too low for configure QoS bandwidth.
CSCwj51700	CPP crashes after reconfiguring 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	Device repeatedly crashing in FTMd due to FNF flow add.
CSCwj96852	Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC.
CSCwj06950	DSL module gets stuck in a booting state.
CSCwj95633	SAIE application - No data to display over vManage for IOS XE router.
CSCwk39131	Device crashed when issuing **show sdwan ftm next-hop chain all**.
CSCwk22225	FTMd crashes after receiving credentials feature template update from vManage.
CSCwj48909	Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk23723	Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwj31476	DSL device feature template suite fails with CONFD ERROR no switchport access vlan 4.
CSCwk45165	fman_fp Memory Leak on device.
CSCwj84949	Unencrypted traffic due to non-functional IPSec tunnel in FLEXVPN hub and spoke setup.
CSCwj90614	High CPU utilisation for confd_cli.
CSCwi81026	SDWAN BFD sessions flapping during IPSec rekey in scaled environment.
CSCwk39268	sdn-network-infra-iwan failing to renew with "hash sha256" >
CSCwj76662	High memory utilization due to ftmd process.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.

Bug ID	Description
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk44078	GETVPN/Migrating to new KEK RSA key does not trigger GM re-registration.
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492.
CSCwk22942	Unable to build two IPSec SAs with same sourceor destination where one peer is PAT'd through the other.
CSCwj96092	ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	Device 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.
CSCwj02401	Router reloaded when generating admin tech while processing very high number of flows.
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwk19725	Add FNF cache limit for show sdwan app-fwd flows for CSCwj02401.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.
CSCwj67591	SD-Routing brownfield - chassis activate effective only after second re-try - with new uuid.
CSCwj32347	DIA endpoint tracker not working with ECMP routes.
CSCwj41728	Unable to install the TE agent using http link in CLI

Open Bugs in Cisco IOS XE 17.15.1a

Table 6: Open Bugs in Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwk75733	Custom applications may not be programmed properly.
CSCwk89256	Speed mismatch in IOS XE configuration after device template push for device.
CSCwk85704	sd-routing:match traffic-category through vManage add-on CLI push failed.
CSCwk28794	SNMP returns incorrect value for the interface when using switchport.
CSCwk86355	File transfer fails from vManage 20.9.5 /home/admin to cEdge 17.6.5 bootflash: lost connection.

Bug ID	Description
CSCwk49806	Router rebooted unexpectedly due to process NHRP crash.
CSCwk81360	Cisco IOS-XE router can reboot unexpectedly while configuring NAT static translation.
CSCwk62954	Multiple match address local interface <int> not pushed from vManage under crypto profile.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk97092	MKA session not coming up after shut/no shut with EVC.
CSCwm07564	Data-policy local-tloc-list breaks RTP media stream.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on device.
CSCwk74298	Device denied for template push and some show commands with error application communication failure.
CSCwk86062	LTE NIM-EM7455, Modem Locks Up after reboot of router, modem reset or cellular profile change.
CSCwk98578	**ipv6 crypto map** not shown in interface configuration.
CSCwk70630	Cannot import device certificate.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwm13223	Crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog.
CSCwk79454	Endpoint tracker does not fail if default route is removed.
CSCwi40697	Modem may not come back up from FW upgrade with LM960A18 and FN980 modems.
CSCwk52677	DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level/iomd process.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.
CSCwi87546	Device unexpectedly rebooted 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.
CSCwm12851	Device uses 3DES as default rekey algorithm for GETVPN.
CSCwk95044	CSCwj42249.SPA.smu.bin drops when packet duplication link fails-over.
CSCwj87028	Cflowd showing custom APP as unknown for egress traffic when using DRE opt.
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwm08545	Centralized policy policer worked per PC on the same site not per site/vpn-list.

Bug ID	Description
CSCwf62943	System image file is not set to packages.conf when image expansion fails due to disk space.
CSCwm00309	Packets not hitting the correct data policy after modifying the action of a sequence.

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 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.