

# Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Dublin 17.12.x

---

**First Published:** 2023-08-22

**Last Modified:** 2025-04-11

## 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 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 Dublin 17.12.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Dublin 17.12.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 17.12.5a

There are no new software features for this release.

## New and Changed Software Features in Cisco IOS XE 17.12.4b

There are no new features in this release.

## New and Changed Software Features in Cisco IOS XE 17.12.2

This release provides a fix for [CSCwh87343](#): Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: [cisco-sa-iosxe-webui-privesc-j22SaA4z](#).

**Table 1: New Software Features**

Feature	Description
<a href="#">Cisco Managed Cellular Activation (eSIM)</a>	<p>The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. When ordering a pluggable interface module (PIM) to provide cellular connectivity for your router, choose a PIM model with a preinstalled eSIM. The Managed Cellular Activation solution comes with a “bootstrap” cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the <a href="#">Cisco Managed Cellular Activation Configuration Guide</a>. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan.</p> <p>Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) model:</p> <ul style="list-style-type: none"> <li>• 5G Sub-6 GHz PIM, model P-5GS6-R16-GL</li> </ul> <p><b>Note</b> In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.</p>

## New and Changed Software Features in Cisco IOS XE 17.12.1a

**Table 2: New Software Features**

Feature	Description
<a href="#">Managing the SD-Routing Devices Using Cisco SD-WAN Manager</a>	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network manage system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.
<a href="#">Profile Clean-up on LTE Modems Using Factory Reset Button</a>	To clean the cellular modem completely, users can press the physical factory-reset button on the device, which enables the inbuilt <b>lte cellular-profile-cleanup</b> command to erase the configuration setup and profiles. This command is disabled by default, but can be enabled only when the factory-reset button is pressed.

Feature	Description
<a href="#">Quantum-Safe Encryption Using Post-Quantum Preshared Keys</a>	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: <ul style="list-style-type: none"> <li>• Cisco 1000 Series Integrated Services Routers</li> <li>• Cisco Catalyst 8500 Series Edge Platforms</li> </ul>
<a href="#">Support for Automatic Log Deletion</a>	This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the <b>logging purge-log buffer days</b> command.
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: <ul style="list-style-type: none"> <li>• Security Group Tag (SGT) or Destination Group Tag (DGT) Policies</li> <li>• Unidirectional IPv4 SGT Exchange Protocol (SXP) connections</li> <li>• Bidirectional IPv4 SXP connections</li> <li>• IPv4 SGT Bindings</li> <li>• IPv6 SGT Bindings</li> <li>• Security Group Access Control Entries (SG ACEs)</li> </ul>
<b>Cube Features</b>	
<a href="#">CUBE/LGW: Cover Buffer Enhancements for VoIP Trace</a>	From Cisco IOS XE Dublin 17.12.1a onwards, VoIP Trace for SIP messages displays cause code in the cover buffer.



**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 3: 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)
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)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
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)

## Resolved and Open Bugs in Cisco IOS XE 17.12.x

### Resolved Bugs in Cisco IOS XE 17.12.5a

**Table 4: Resolved Bugs in Cisco IOS XE 17.12.5a**

Bug ID	Description
<a href="#">CSCwm48190</a>	Memory leak under vDaemon process.
<a href="#">CSCwk44078</a>	GETVPN/Migrating to new KEK RSA key does not trigger GM re-registration.
<a href="#">CSCwk42190</a>	Config and dp show command do not match the dp oper output.
<a href="#">CSCwj06950</a>	DSL module gets stuck in a booting state.
<a href="#">CSCwf79399</a>	IOS-XE port-channel sub-interface overload port-channel interface must be created first and deleted.
<a href="#">CSCwj80411</a>	Deleting and adding the rules in a ZBFW policy with 510 rules results in traffic drop.
<a href="#">CSCwk86062</a>	Modem locks up after reboot of router, modem reset or cellular profile change.
<a href="#">CSCwn17454</a>	Band-select feature not working for the LM960 modem.
<a href="#">CSCwm57123</a>	Modem locks up, modem reset or cellular profile change - additional fix.
<a href="#">CSCwf77488</a>	IOSd crash after radium boot up and online.
<a href="#">CSCwk23723</a>	Mean queue calculation is incorrect on WRED hierarchical QoS.
<a href="#">CSCwm14462</a>	IPv6 flowspec nexthop redirect policy is not redirecting the traffic on IOS XE.
<a href="#">CSCwm05524</a>	Unexpected reload due to cpp-mcplo-ucode process when handling fragments with SRv6 routing.

Bug ID	Description
<a href="#">CSCwj84949</a>	Unencrypted traffic due to non-functional IPSec tunnel in FLEXVPN hub and spoke setup.
<a href="#">CSCwn07540</a>	Device crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPAALIVE.
<a href="#">CSCwn77224</a>	Issue with ethernet/gig interface with second-dot1q is not working as expected.
<a href="#">CSCwm98642</a>	OMP is redistributing summary routes in the service VPN even though the exact networks do not exist.
<a href="#">CSCwn15231</a>	Device null-way audio within the same layer2.
<a href="#">CSCwk53680</a>	Inbound calls through device results in phantom calls (64.3.0, 60.1.4, 62.3.3).
<a href="#">CSCwm80356</a>	LLDP packets dropped when came through active port-channel interface.
<a href="#">CSCwi96187</a>	P-5GS6-GL FN980 modem fW upgrade failing.
<a href="#">CSCwk79454</a>	Endpoint tracker does not fail if default route is removed.
<a href="#">CSCwm59640</a>	PPPoA session down until QoS policy-map removed from dialer interface.
<a href="#">CSCwk61238</a>	RRI static not populating route after reload if stateful IPSec is configured.
<a href="#">CSCwk75459</a>	MGCP GW fails to respond with 250 OK when there is a delay from dataplane in gathering statistics.
<a href="#">CSCwk87452</a>	Procyon synchronize DTL does not wait until complete due to compiler optimization.
<a href="#">CSCwm79570</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.
<a href="#">CSCwm89600</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.
<a href="#">CSCwm79581</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.
<a href="#">CSCwm79554</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.
<a href="#">CSCwm79596</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.
<a href="#">CSCwm79577</a>	Cisco IOS and IOS XE SNMP Denial of Service vulnerabilities.

## Open Bugs in Cisco IOS XE 17.12.5a

*Table 5: Open Bugs in Cisco IOS XE 17.12.5a*

Bug ID	Description
<a href="#">CSCwn92855</a>	Breakout port fails to initialize.
<a href="#">CSCwn97600</a>	Some BFD flapping on PWK ipsec-rekey on all devices.
<a href="#">CSCwe23188</a>	Upgrade from vmanage declared successful even though device boots up with different version than requested.

## Resolved Bugs - Cisco IOS XE 17.12.4b

There are no resolved bugs in this release.

## Open Bugs - Cisco IOS XE 17.12.4b

There are no open bugs in this release.

## Resolved Bugs in Cisco IOS XE 17.12.4a

*Table 6: Resolved Bugs in Cisco IOS XE 17.12.4a*

Identifier	Headline
<a href="#">CSCwi87546</a>	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
<a href="#">CSCwj40589</a>	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
<a href="#">CSCwm60651</a>	HTX: UTD snort crash at memif_shm_peek_first_packet (handle=0x0).
<a href="#">CSCwk84047</a>	Memory Leak due to security violation by new MAC address and "Del Pend" object increases - ACE_IPV4.
<a href="#">CSCwk54544</a>	ZBFW TCAM misprogramming after rules are reordered on the device.
<a href="#">CSCwk50488</a>	Memory leak in fman_rp under acl_db.

## Open Bugs in Cisco IOS XE 17.12.4a

There are no open bugs in this release.

## Resolved Bugs in Cisco IOS XE 17.12.4

*Table 7: Resolved Bugs in Cisco IOS XE 17.12.4*

Bug ID	Description
<a href="#">CSCwj70335</a>	Crypto IKEv2 - Fragmented authentication packets detected as malformed on 3rd party vendor device.
<a href="#">CSCwj44868</a>	GETVPN COOP KS   Wrong Severity for Rekey Acknowledgement configuration mismatch log message
<a href="#">CSCwi88969</a>	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back
<a href="#">CSCwi68865</a>	Memory leak in Crypto IKEv2 due to C_NewObject
<a href="#">CSCwj09284</a>	Unexpected reboot in WLC due to SSL.
<a href="#">CSCwi40603</a>	Memory leak in the Crypto IKMP process.
<a href="#">CSCwi82405</a>	mGRE Tunnels with shared ipsec profile cause ucode crash.



Bug ID	Description
<a href="#">CSCwj34578</a>	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
<a href="#">CSCwi55183</a>	"crypto pki certificate pool" in running configuration
<a href="#">CSCwk15127</a>	Failure to communicate a period of time after the stp status changes
<a href="#">CSCwh37024</a>	PnP gets stuck when Verizon cellular backhaul is used
<a href="#">CSCwj45130</a>	Segmentation Fault - Process = IPSec dummy packet process
<a href="#">CSCwj88872</a>	IPSec tunnel fails to establish due to error IPSec policy invalidated proposal
<a href="#">CSCwi59854</a>	'show sdwan policy service-path' command gives inconsistent results with app name specified
<a href="#">CSCwi84767</a>	Memory dump outputs appear without debugs enabled in SSL VPN code
<a href="#">CSCwj38106</a>	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for a RA VPN connection
<a href="#">CSCwh73320</a>	NAT pool does not work under prefix 16. Available address = zero
<a href="#">CSCwi89822</a>	Unexpected reboot due cpp ucode on the router.
<a href="#">CSCwh86053</a>	ENH: Config Parser Issue for NAT with Extendable and Redundancy
<a href="#">CSCwj42249</a>	Disabling PMTU-Discovery with MTU Change and BFD Flap Breaks Packet Duplication
<a href="#">CSCwh16595</a>	Flex: Peer failed to up after shut/noshut L2 port with SFP inserted and switchport mode configured
<a href="#">CSCwi78365</a>	Trim installed certificate on upgrade
<a href="#">CSCwj72888</a>	Reload in tcp_sanity due to l4 pointer not set
<a href="#">CSCwi93784</a>	(SWI case 01257768)FW upgrade does not work properly on P-LTE-MNA with 17.12.1a and 17.12.2 IOS
<a href="#">CSCwj33292</a>	AnyConnect connection through IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend
<a href="#">CSCwi60071</a>	ipv6 PREFIX delegation is not working on ADSL PPPOA
<a href="#">CSCwj06622</a>	segmentation fault and core files are seen on IOS-XE in controller-manged SD-WAN due to speedtest
<a href="#">CSCwi16111</a>	ipv6 tcp adjust-mss not working after delete and reconfigure
<a href="#">CSCwj29947</a>	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot
<a href="#">CSCwj25619</a>	ISR1K 17.12.2 Auto-negotiation fails to endpoint hardcoding 10/half

Bug ID	Description
<a href="#">CSCwf87975</a>	Router crashed when port-channel interface flap with scale of per-tunnel QoS policies.

## Open Bugs in Cisco IOS XE 17.12.4

*Table 8: Open Bugs in Cisco IOS XE 17.12.4*

Bug ID	Description
<a href="#">CSCwj79987</a>	C1121X SD-WAN Router does not establish BFD sessions after upgrade to 17.9.3a or 17.9.4a
<a href="#">CSCwi03502</a>	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN
<a href="#">CSCwk31560</a>	NAT Command not readable after reloaded
<a href="#">CSCwk42493</a>	Cellular interface in last-resort mode should be admin up, line protocol down
<a href="#">CSCwk44078</a>	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration
<a href="#">CSCwj06950</a>	C1117 - DSL module gets stuck in a booting state
<a href="#">CSCwk58303</a>	Watchdog crash during IPv6 cef adjacency routines
<a href="#">CSCwk63722</a>	Startup Configuration Failure Post PKI Server Enablement
<a href="#">CSCwj77594</a>	IOS XE Controller Mode - WAN IP is allowed to be configured as SYSTEM IP
<a href="#">CSCwk54544</a>	SD-WAN ZBFW TCAM misprogramming after rules are reordered on c8300
<a href="#">CSCwb47658</a>	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
<a href="#">CSCwj90614</a>	High CPU utilisation for confd_cli
<a href="#">CSCwk03686</a>	Crash due a segmentation fault due a negative value
<a href="#">CSCwi96692</a>	**** Unable to Install HSEC K9 Licence for PID C1111-8PLTELAWF & C1111X-8P ****
<a href="#">CSCwk31715</a>	After deleting a NAT configuration, the IP address still shows up in routing table.
<a href="#">CSCwh45389</a>	C9800: Key manager crash after hostname change with usage keys
<a href="#">CSCwk12524</a>	Device reloaded due to ezManage mobile app Service.
<a href="#">CSCwk65071</a>	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after Cellular interface flap
<a href="#">CSCwf91481</a>	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.

Bug ID	Description
<a href="#">CSCwk52677</a>	C1118-8P / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process
<a href="#">CSCwi96187</a>	P-5GS6-GL FN980 modem fW upgrade is failing.
<a href="#">CSCwh91136</a>	IOS XE:Traffic not encrypted and dropped over IPSEC SVTI tunnel
<a href="#">CSCwj23674</a>	Dialer interface MAX MTU for PPPOA is 1492
<a href="#">CSCwj84949</a>	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup
<a href="#">CSCwk20995</a>	PPPoE session with sub-interface getting stuck after reboot
<a href="#">CSCwk30527</a>	IKEv2 session is down after reload if identity local address is assigned to interface on Switch
<a href="#">CSCwk22942</a>	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
<a href="#">CSCwi31110</a>	Traceback seen @_nhp_cache_delete due to negative global cache count.

### Resolved Bugs - Cisco IOS XE 17.12.3a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwk21189</a>	Template attach fail with unknown element: ssh-version in /ios:native/ios:ip/ios:ssh
<a href="#">CSCwk20843</a>	PPPoE with NAT DIA feature validation failed post upgrade.

### Resolved Bugs in Cisco IOS XE 17.12.3

*Table 9: Resolved Bugs in Cisco IOS XE 17.12.3*

Bug ID	Description
<a href="#">CSCwh73350</a>	Router keeps crashing when processing a firewall feature.
<a href="#">CSCwh18120</a>	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
<a href="#">CSCwh68508</a>	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
<a href="#">CSCwi28227</a>	NAT HSL logging vrf-filter is not working.
<a href="#">CSCwh77221</a>	SNMP unable to poll tunnel data after a minute.
<a href="#">CSCwh96578</a>	SKA_PUBKEY_DB leak in TDL.
<a href="#">CSCwh69765</a>	Security policy w/IPS external syslog config failing generation for specific models.

Bug ID	Description
<a href="#">CSCwh87619</a>	ZBFW is unable to detect packets on TenGig interface.
<a href="#">CSCwi06843</a>	Endpoint tracker triggers a CPU hog.
<a href="#">CSCwh80441</a>	Cosmetic 3G issue causing distress to customers - modem WCDMA 900 is displayed as unknown.
<a href="#">CSCwh10813</a>	Add verbose log to indicate grant ra-auto to undo configuring the grant auto in PKI server.
<a href="#">CSCwi60312</a>	Device does not boot up in full configuration.
<a href="#">CSCwh93257</a>	Device creates crooked NAT entry if 2 or more IP phones from NAT outside register to the same server.
<a href="#">CSCwi59121</a>	Mobile-app causing excessive authorization attempts with a null username.
<a href="#">CSCwi08171</a>	Router may crash due to crypto IKMP process.
<a href="#">CSCwi49231</a>	Device audio loss for 4 seconds.
<a href="#">CSCwi06404</a>	PKI crash after failing a CRL fetch.
<a href="#">CSCwh50510</a>	Router unexpectedly reloads during Trustpool retrieval for SIP TLS certificate.
<a href="#">CSCwh75800</a>	Router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
<a href="#">CSCwi28781</a>	EPBR generates error when the policy is added and deleted multiple times.
<a href="#">CSCwh45169</a>	Unexpected reboot while displaying information from cleared SSS session.
<a href="#">CSCwh70449</a>	PMTUD incorrectly converging without attempting to learn a higher MTU.
<a href="#">CSCwh96415</a>	Cannot disable the DMVPN logging.
<a href="#">CSCwi25737</a>	Router should discard IKE notification messages with incorrect DOI.
<a href="#">CSCwh50628</a>	Race condition crash on IOS-XE device.
<a href="#">CSCwf86207</a>	Frame relay DTE router crashes due to EXMEM exhaustion.
<a href="#">CSCwh72869</a>	cpp_mcplo_ucose crash with port-channel and NAT.
<a href="#">CSCwh99399</a>	FTMD crash observed in ENCS platform while running PWK suite.
<a href="#">CSCwi51326</a>	CPP CP SVR crash after decoding all packets to text (using l2 copy) on FIA trace.
<a href="#">CSCwi76087</a>	ATO: Session fails to come up when the tunnel is repeatedly shut and no shut in a loop (similar to customer unplugging and plugging in a cable).
<a href="#">CSCwi55379</a>	IPsec traffic is being dropped on strongswan when PPK is implemented.
<a href="#">CSCwi63042</a>	Packet drops observe between LISP EID over GRE tunnel.

Bug ID	Description
<a href="#">CSCwi79584</a>	Upgrade failure for a routing device through the management system due to a modified system configuration.
<a href="#">CSCwi30529</a>	AAA: Template push fail when AAA authorization is set to local.

## Open Bugs in Cisco IOS XE 17.12.3

Table 10: Open Bugs in Cisco IOS XE 17.12.3

Bug ID	Description
<a href="#">CSCwi03502</a>	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
<a href="#">CSCwj08744</a>	Unexpected reload when using <b>show running-config full   format</b> .
<a href="#">CSCwi16111</a>	<b>ipv6 tcp adjust-mss</b> not working after delete and reconfigure.
<a href="#">CSCwi46997</a>	NAT command not readable after reloaded.
<a href="#">CSCwi67621</a>	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).

## Resolved Bugs in Cisco IOS XE 17.12.2

Table 11: Resolved Bugs in Cisco IOS XE 17.12.2

Bug ID	Description
<a href="#">CSCwf67564</a>	Device observes memory leak at process "SSS Manager".
<a href="#">CSCwf60151</a>	Memory leak with pubd.
<a href="#">CSCwh60190</a>	<b>ip name-server</b> command not pushed.
<a href="#">CSCwf56463</a>	IOS process crash during VRRP hash table lookup.
<a href="#">CSCwh11858</a>	Device running IOS-XE crashes when removing FQDN ACL.
<a href="#">CSCwf99906</a>	NTP authentication removed after reload using more than 16 bytes.
<a href="#">CSCwf59173</a>	Segmentation fault at IPv6 BGP backup route notification.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot.
<a href="#">CSCwf41084</a>	Extranet multicast code improvements for better handling of data structure.
<a href="#">CSCwh04884</a>	VC down due to control-word negotiation.
<a href="#">CSCwf26494</a>	BDI + NTP configuration puts DMI process in degraded mode.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating TP generates an invalid TP.

Bug ID	Description
<a href="#">CSCwf82676</a>	CPU usage mismatch in <b>show sdwan system status</b> vs <b>show proc cpu platform</b> .
<a href="#">CSCwf49390</a>	crashes@crypto_map_unlock_map_head.
<a href="#">CSCwe91898</a>	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running <b>show crypto</b> commands.
<a href="#">CSCwh44986</a>	Device to host C1117-4PLTE loopback unreachable.
<a href="#">CSCwh30377</a>	Data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
<a href="#">CSCwh20734</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
<a href="#">CSCwh01425</a>	ITU channel configuration seems not working on device.
<a href="#">CSCwh20577</a>	Crashed by TRACK client thread at access invalid memory location.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot on C1117-4PLTEEA.
<a href="#">CSCwh36801</a>	Crash in IP Input process during tunnel encapsulation.
<a href="#">CSCwh41497</a>	DDNS update retransmission timer fails to work with a traceback error.
<a href="#">CSCwd39219</a>	SMS archive does not work when ftp transaction is of VRF.
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload.
<a href="#">CSCwh29805</a>	Custom-app based policy triggering protocol deactivation and CPP traceback with traffic failure.
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCwf80191</a>	Flowspec on device will not revoke.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config.
<a href="#">CSCwh00332</a>	B2B NAT: when configuration ip nat inside/outside on VASI interface, ack/seq number abnormal.
<a href="#">CSCwh08948</a>	Show platform hardware throughput crypto/ambiguous outputs.
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a> .
<a href="#">CSCwh96700</a>	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

## Open Bugs in Cisco IOS XE 17.12.2

**Table 12: Open Bugs in Cisco IOS XE 17.12.2**

Bug ID	Description
<a href="#">CSCwh58252</a>	IPv6 SPD min/max defaulting to values 1 and 2.
<a href="#">CSCwh14083</a>	High CPU due to MPLS MIB poll.
<a href="#">CSCwh22981</a>	WNCD process crashes.
<a href="#">CSCwh99513</a>	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
<a href="#">CSCwh90851</a>	pubd process showing high CPU utilization.
<a href="#">CSCwh83532</a>	1Gig int on device using GLC-SX-MMD are down/down after changing connection.
<a href="#">CSCwh96891</a>	Memory leak with pubd.
<a href="#">CSCwh91085</a>	Convergence improvement after device reboot with mVPN profile 14.
<a href="#">CSCwh58919</a>	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
<a href="#">CSCuu85298</a>	FIB/LFIB inconsistency after BGP flap.
<a href="#">CSCwf83684</a>	IOS XE router may experience "%FMANRP_QOS-4-MPOLCHECKDETAIL:" errors.
<a href="#">CSCwh59926</a>	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.
<a href="#">CSCwh24280</a>	Mismatch between the resource allocation and "app-resource profile custom" configuration.
<a href="#">CSCwh82668</a>	Incorrect local MPLS label in CEF after BGP flap.
<a href="#">CSCwh95036</a>	Cisco IOS-XE IPv6 based subscription telemetry does not work.
<a href="#">CSCwh99464</a>	Guestshell connectivity not working with NAT overload.
<a href="#">CSCwh30928</a>	SDA - using "spt-threshold infinity" and having LHR+FHR can cause the S,G to be pruned on the RP.
<a href="#">CSCwh01738</a>	Unexpected reload when using rsh/rcmd.
<a href="#">CSCwh04124</a>	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
<a href="#">CSCwh67285</a>	WLC unable to get telemetry data due to pubd unexpected reload and fail.
<a href="#">CSCwh96332</a>	Device crash due to dhcpd_binding_check.
<a href="#">CSCwh56940</a>	Site tag change wncd working/failing EAP-TLS.
<a href="#">CSCwh44418</a>	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.

Bug ID	Description
<a href="#">CSCwh46559</a>	LLDP location information not sent when configured.
<a href="#">CSCuv36790</a>	<b>clear bgp</b> command does not consider AFIs when used with update-group option.
<a href="#">CSCwh02698</a>	Device sending incomplete SGT to ISE.
<a href="#">CSCwh05869</a>	Only portion of HSRP config being pushed via CLI ADDON template.
<a href="#">CSCwf53750</a>	"match pktlen-range" does not work with GRE/IPSEC GRE.
<a href="#">CSCwh60107</a>	In the show tech file, "enable secret" does not get hidden.
<a href="#">CSCwh45579</a>	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
<a href="#">CSCwh95024</a>	ISIS crash in local uloop.
<a href="#">CSCwh41155</a>	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.
<a href="#">CSCwh31485</a>	Member interface config not applied with mis-match in packages.conf files.
<a href="#">CSCwh72437</a>	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
<a href="#">CSCwi00680</a>	Router unexpectedly reloads while using DHCP for ISG.
<a href="#">CSCwh96823</a>	IOS-XE router not installing classless-static-routes from DHCP option 121.
<a href="#">CSCwh77706</a>	SVL, 10G link on the active chassis will go down after reload.
<a href="#">CSCwh02592</a>	Device sync fails when device prompt comes along with device banner and TACACS is used.
<a href="#">CSCwh84850</a>	Unexpected reboot in device due to SISF and STP initialization.
<a href="#">CSCwh64903</a>	Crash on device polling SPA sensor data.
<a href="#">CSCwh53432</a>	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
<a href="#">CSCwh21796</a>	Password getting visible for the mask-secret in show logging.
<a href="#">CSCwh50104</a>	Upgrade failing with config check track-id-name.
<a href="#">CSCwf59929</a>	CTS CORE process crash after configuring role based ACL.
<a href="#">CSCwh81471</a>	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
<a href="#">CSCwh93772</a>	Option 121 never requested by IOS-XE client.
<a href="#">CSCwh06087</a>	[IPv6 BGP] multiple sourced paths present for the same prefix.
<a href="#">CSCwh29120</a>	IP SPD queue thresholds are out of range.



Bug ID	Description
<a href="#">CSCwh14953</a>	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value.
<a href="#">CSCwh89096</a>	Device unexpected reload.
<a href="#">CSCwh99597</a>	After migration MAC/IP only MAC is advertised.
<a href="#">CSCwh75992</a>	"BGP Router" process crash.
<a href="#">CSCwh48058</a>	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.
<a href="#">CSCwh76920</a>	Memory leak in linux_iosd-imag due to SNMP.
<a href="#">CSCwh75112</a>	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.
<a href="#">CSCwh73350</a>	Device keeps crashing when processing a firewall feature.
<a href="#">CSCwh94906</a>	WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
<a href="#">CSCwh68508</a>	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
<a href="#">CSCwi01046</a>	PoE module is not providing enough power to bring the ports after an unexpected reload.
<a href="#">CSCwh16901</a>	HSEC license installation from the workflow does not complete.
<a href="#">CSCwh77221</a>	SNMP unable to poll SDWAN tunnel data after a minute.
<a href="#">CSCwh10813</a>	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
<a href="#">CSCwh79161</a>	WP7607 Requires shut/no shut to populate IP address from modem to host.
<a href="#">CSCwh57544</a>	Silent reload due to LocalSoftADR causes crash without core file.
<a href="#">CSCwh50510</a>	Device crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
<a href="#">CSCwh75800</a>	CUBE router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
<a href="#">CSCwh73320</a>	NAT pool does not working under prefix 16. Available address = zero.
<a href="#">CSCwh96700</a>	Carrier grade NAT reaching max host entries and failing to translate due to gatekeeper.
<a href="#">CSCwh45169</a>	Unexpected reboot while displaying information from cleared SSS session.
<a href="#">CSCwh70449</a>	PMTUD incorrectly converging without attempting to learn a higher MTU.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwh83228</a>	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running.
<a href="#">CSCwh91136</a>	IOS XE: Traffic not encrypted and dropped over IPSEC SVTI tunnel.

Bug ID	Description
<a href="#">CSCwh96415</a>	Cannot disable DMVPN logging in.
<a href="#">CSCwh12093</a>	Enable SoS/ROC feature for DSL.
<a href="#">CSCwf86207</a>	Frame relay DTE router crashes due to EXMEM exhaustion.

## Resolved Bugs in Cisco IOS XE 17.12.1a

**Table 13: Resolved Bugs in Cisco IOS XE 17.12.1a**

Bug ID	Description
<a href="#">CSCwe82666</a>	Not all HSL entries get pushed to device if more than 1 HSL entries are configured via vManage.
<a href="#">CSCwe31226</a>	Issues/discrepancies around CPU alarms generated and sent to vManage from cEdge.
<a href="#">CSCwe43341</a>	TLS control-connections down, traffic from controller dropped with SDWAN implicit ACL drop.
<a href="#">CSCwe18124</a>	MACSEC remains marked as SECURED, but randomly the traffic stops working.
<a href="#">CSCwe18276</a>	Route-map not getting effect when its applied in OMP for BGP routes.
<a href="#">CSCwf83850</a>	With Pure IPv6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in wan int G1.
<a href="#">CSCwb74821</a>	Unexpected behavior due to unstable power source.
<a href="#">CSCwe81182</a>	(EPC, packet-trace) for IPsec running COFF (Crypto OFFLOAD).
<a href="#">CSCwe93905</a>	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
<a href="#">CSCwe90501</a>	Upgrade fails due to advertise aggregate with vrf.
<a href="#">CSCwe85195</a>	AAR: BoW feature ignoring color preference from tiered transport preference configuration
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwd53710</a>	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes 30 sec.
<a href="#">CSCwe66318</a>	NAT entries expire on standby router.
<a href="#">CSCwf83985</a>	With pure IPv6 overlay, vbond vpn 0 ge0/0 interface if-oper-status down after power off/on.
<a href="#">CSCwd84599</a>	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
<a href="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwe70374</a>	Device punt-policer is not configurable.

Bug ID	Description
<a href="#">CSCwe73408</a>	For some error condition platform_properties may double free.
<a href="#">CSCwd42523</a>	Same label is assigned to different VRFs
<a href="#">CSCwe12194</a>	Auto-update cycle incorrectly deletes certificates.
<a href="#">CSCwe57239</a>	All usb internal communication is closed when using <b>platform usb disable</b> command.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
<a href="#">CSCwe85421</a>	cEdge BFD session down with interface flap.
<a href="#">CSCwe83169</a>	Pseudowire control word not working on device.
<a href="#">CSCwe95606</a>	Double GR_Additional log enablement defect.
<a href="#">CSCwe31471</a>	Segmentation fault in SDWAN PB rx when per-tunnel qos config withdraw.
<a href="#">CSCwe89404</a>	No way audio when using secure Hardware conference with secure endpoints.
<a href="#">CSCwd39257</a>	IOS-XE cpp crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwe63222</a>	Certificate output is not getting changed on renew when cloud certificate authorization is automated.
<a href="#">CSCwe70642</a>	AAR overlay actions are applied to DIA traffic.
<a href="#">CSCwa96399</a>	Configuring entity-information xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwe79007</a>	cEdge unexpected reload when doing ips test with UTD ips engine.
<a href="#">CSCwe31281</a>	Autotunnel IPsec tracker: Tracker does not come up at all on vEdge.
<a href="#">CSCwd93401</a>	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
<a href="#">CSCwd76648</a>	Port-channel DPI Load-balancing not utilizing all the member-links.
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device.
<a href="#">CSCwb39206</a>	Enable VFR CLI in sdwan mode.
<a href="#">CSCwe85022</a>	Telstra Cert: FN980 modem is showing 4 additional NR bands support - 1, 3, 7, and 28.

## Open Bugs in Cisco IOS XE 17.12.1a

Table 14: Open Bugs in Cisco IOS XE 17.12.1a

Bug ID	Description
<a href="#">CSCwf70854</a>	Changes to speed on the interface via CLI/GUI does not go through unless first done via shell access.
<a href="#">CSCwf72079</a>	Device unexpectedly reloads due to LocalSoft.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating TP generates an invalid TP.
<a href="#">CSCwh06870</a>	APN password in plain text when cellular controller profile is configured.
<a href="#">CSCwf87292</a>	Punt keep alive failure crash on device controller managed apparently due to for us data packets.
<a href="#">CSCwf83850</a>	With pure IPv6, minimal bootstrap unable to onboard non-fabric - IPv6 config missing in wan int G1.
<a href="#">CSCwf94294</a>	Misprograming during vpn-list change under data policy.
<a href="#">CSCwf55145</a>	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
<a href="#">CSCwf94052</a>	BFD going down for newly onboarded device.
<a href="#">CSCwf61720</a>	No licenses in use after upgrading from traditional to Smart Licensing IOS-XE versions.
<a href="#">CSCwf80927</a>	Speed tests to internet from device triggered.
<a href="#">CSCwf84522</a>	Unexpected rebooted while classifying packet with CTF (Common Flow Table).
<a href="#">CSCwf44703</a>	NAT64 prefix is not originated into OMP.
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running <b>show crypto</b> commands
<a href="#">CSCwf77252</a>	SIP calls not working on device with ZBFW enabled.
<a href="#">CSCwf96416</a>	Can not access any <b>show sdwan</b> commands at all.
<a href="#">CSCwf67564</a>	Device observes Memory Leak at process SSS Manager.
<a href="#">CSCwf34171</a>	Configure replace command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot.
<a href="#">CSCwf69062</a>	SDRA-SSLVPN : The SSL VPN session closes with re-authentication error after some interval of time.
<a href="#">CSCwf79264</a>	Traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped.
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload.

Bug ID	Description
<a href="#">CSCwf45486</a>	OMP to BGP redistribution leads to incorrect AS_Path installation on chosen Next-Hop.
<a href="#">CSCwh01313</a>	Unexpected reboot due qfp uCode due to IPSec functions.
<a href="#">CSCwf95527</a>	BFD entries removed.
<a href="#">CSCwe26895</a>	Router has Local Soft ADR crash, writes flat core, and reloads.
<a href="#">CSCwh01318</a>	Multiple crashes observed on platform due to memory exhaustion.
<a href="#">CSCwf71116</a>	Static route keep advertising via OMP even though there is no route.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config
<a href="#">CSCwh00332</a>	B2B NAT: when configuration <b>ip nat inside/outside</b> on VASI interface, ack/seq number abnormal.
<a href="#">CSCwf49390</a>	Crashes@crypto_map_unlock_map_head.
<a href="#">CSCwh67812</a>	Unable to configure <b>crypto map</b> on a physical interface due to which crypto map-based VPN's cannot be formed.

## 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.

