

Release Notes for Cisco 1100 Terminal Services Gateway, Cisco IOS XE Release 26.2.x

First Published: 2026-04-24

Last Modified: 2026-09-28

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 1100 Terminal Services Gateway

Cisco 1100 Terminal Services Gateway are terminal servers that provides asynchronous connections to the console ports for Cisco devices.

Table 1: Base Models of the Cisco 1100 Terminal Services Gateway

Base Models	Asynchronous Ports	NIM Slot	Switch	Memory
C1100TG-1N32A	32	Yes	None	2GB Dram/ 4GB flash
C1100TG-1N24P32A	32	Yes	24 port L2 Switch	4GB Dram/ 4GB flash
C1100TGX-1N24P32A	32	Yes	24 port L2 Switch	8GB Dram/ 8GB flash



Note Starting with Cisco IOS XE Amsterdam 17.3.2, 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 Enhanced Hardware and Software Features

New and Changed Hardware Features in Cisco IOS XE 26.2.1

There are no new hardware features in this release.

New and Changed Software Features in Cisco IOS XE 26.2.1

Table 2: New software features for Release 26.2.1

Product Impact	Feature	Description
Hardware reliability	Resilient Infrastructure Changes	

Product Impact	Feature	Description
		As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: The RADIUS client appends the Message-Authenticator attribute (Attribute 80 HMAC-MD5) to all outgoing Access-Request packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). The RADIUS client drops incoming Access-Accept, Access-Reject, and Access-Challenge packets if the Message-Authenticator packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80. Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the ip proxy-arp command explicitly if required. The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the

Product Impact	Feature	Description
		ip http secure-server command. The IOS XE device rejects unauthenticated NTP Mode 6 and Mode 7 control queries (monlist) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (telnet, ftp, tftp, http) are enabled in the configuration. Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance. For more information, refer Resilient Infrastructure.
Ease of setup	EVPN VPWS over SRv6	This feature adds support for EVPN VPWS over SRv6 transport. EVPN VPWS uses EVPN signalling and SRv6 encapsulation to provide point-to-point Layer 2 VPN service between provider edge devices.
Ease of use	Port settings for speed, duplex, and auto-negotiation	Configure speed, duplex, and negotiation auto in a single command.
Ease of use	Discontiguous Subnet Mask Support for IPv4 Network Object Groups	Adds support for discontiguous subnet mask entries in IPv4 data prefixes and IPv4 network object groups used by NGFW Policy. You can use discontiguous subnet mask entries in IPv4 source and destination match conditions, rule sets, object groups, and deploy-time data prefix variables.

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Changes in behavior in Cisco IOS XE 26.2.1

Table 3: Changes in behavior in Cisco IOS XE 26.2.1

Description	Behavior change
The ip nat translation nonpat-timeout keyword allows configuring a timeout from 0 to 536870 seconds or setting it to never.	Refer to the ip nat translation (timeout) command.
DHCP relay is always enabled by Cisco IOS and provide status verification for cellular modems	Refer to the Configuring the DHCP Client section.
Certificate hexadecimal data appears under crypto pki certificate chain in show running-config by default. Starting with Cisco IOS XE Release 26.2, configure the crypto pki certificate hidehex command hides certificate hexadecimal data from show running-config output while retaining the certificate chain and entry.	Refer to the Certificate Hexadecimal Data Output Example .
The procedure for configuring a trustpoint for EST is updated.	Refer to the Configure a trustpoint for EST section.

Resolved and Open Bugs

Resolved Bugs in Cisco IOS XE 26.2.1

Table 4: Resolved bugs in Cisco IOS XE 26.2.1

Identifier	Headline
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwv02835	[IOS XE] 6VPE: Locally terminated IPv6 traffic fails over BDI interface
CSCww00071	Router crashed while decrypting NAT-T IPsec traffic with CTS SGT enabled
CSCwv52757	UDP packets multicast destination not seen on FIA-Trace nor EPC over xconnect
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwv67035	Ikev2 PPK Unable To Switch Back to PSK When 'Required' Is Used in Keyring
CSCwu49303	Memory Leak in cpp_sp_svr due to Classification Objects
CSCwt79827	IOS-XE not parsing transform payload with unknown attributes
CSCwt94337	cpp_cp_svr crashes with SIGSEGV while printing packet trace data
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwv73701	Packet reordering observed when application performance-monitor service policy enabled

Identifier	Headline
CSCwt97049	Buffer Overflow in Domain Name Pattern Handling Causes Pointer Corruption and System Crash
CSCwt44596	Cat8300 router fails to bring up BFD over IPSEC Tunnel when underlay path is using switching module instead of on-board interface.
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.
CSCwt56693	L2TP: Seeing "protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCwu02842	Unexpected reload on ASR1K due to race condition in QoS service group configuration
CSCwu35982	Router unexpectedly reloads after IKEv2 operations
CSCwv42272	NULL Dereference in NHRP MIB
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router
CSCwv60786	Intermittent issue with RRI being lost on the Flex Hub
CSCwt17412	Sessions appear as two unidirectional records instead of one bidirectional flow

Open Bugs in Cisco IOS XE 26.2.1

Table 5: Open bugs in Cisco IOS XE 26.2.1

Identifier	Headline
CSCww20413	Update outdated GeoDB in 17.18.x
CSCwv86632	IOSd crash in "Open DNS Dev-Reg" process on 17.12.6 despite CSCwp09231 fix (Umbrella device-registration UAF during config churn)
CSCwv80846	IOSd crash in router_init due to stale PDB pname during routing process creation
CSCww05599	Unexpected reload due to NAT pool exhaustion

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.

