Release Notes for Cisco 1100 Terminal Services Gateway, Cisco IOS XE 26.1.x

First Published: 2026-04-24

Full Cisco Trademarks with Software License

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

Table 2: New Hardware Features

Feature	Description
Cisco 1100 Terminal Services Gateway	The Cisco 1100 Terminal Services Gateway are based on Cisco IOS XE Amsterdam 17.2 release, multi-core data plane and 4 core CPU. The Cisco 1100 Terminal Services Gateway are in two platform series. The base model has a 32 async ports with 2 GB memory, the plus model has 32 ports, 24 L2 switch and 4GB or 8GB memory to support programmability features. A 16 port async ports daughter card is available to extend onboard async ports to 48 for both these platforms.

New and Changed Software Features

Table 3: New software features for Cisco 1000 Series Integrated Services Routers, Release 26.1.1

Product impact	Feature	Description
Software Reliability	Resilient Infrastructure	

Product impact	Feature	Description
		As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all

Product impact	Feature	Description
		insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption. For more information, refer this document Routing-SD-WAN Resilient Infrastructure

New and Changed Software Features in Cisco IOS XE 26.1.1

Table 4: New Software Features

Product Impact	Feature	Description
Ease of Use	BGP Advertisement Startup Delay	When a Border Gateway Protocol (BGP) process initializes during a router reload or when BGP routing sessions are reset by using the **clear ip bgp*** command, it could result in a temporary period of traffic loss. The BGP Advertisement Startup Delay feature addresses this issue by introducing a configurable delay before BGP begins advertising routes to its neighbors. This delay allows sufficient time for routes to be installed in the hardware, ensuring traffic forwarding is ready before new routes are announced.

Resolved and Open Bugs

Resolved Bugs in Cisco IOS XE 26.1.1

Table 5: Resolved Bugs in Cisco IOS XE 26.1.1

Identifier	Headline
CSCws40263	uCode failure due to a stuck thread during the NAT session database walk.
CSCws89172	Failure at cft_engine_handle_vrf_associate_if_needed on the router with IPv6 traffic.
CSCwq77458	FMAN failure after FNF configuration changes on the device.
CSCwr00088	Add a CLI command to change the per-MPLS label CEF statistics query interval on the FMAN FP on the device.

Identifier	Headline
CSCwr06399	Certificate verification fails and the identity certificate is not installed after a device reload for certificates with an EC key of 521.
CSCwr08462	The NAT router is not responding to ARP requests.
CSCws62501	IOSd failure with **match authen-status unauthenticated** configured on the device.
CSCwq98154	Multicast traffic is not forwarded over the P2P DMVPN phase 1 tunnel on the device.

Open Bugs in Cisco IOS XE 26.1.1

Table 6: Open Bugs in Cisco IOS XE 26.1.1

Identifier	Headline
CSCwt22873	High QFP utilization is caused by the "all-host" limit in Carrier Grade NAT mode on the device.
CSCws99246	Clarification regarding the operation that enables communication from outside the NAT.
CSCwt18839	A segmentation fault occurs in the cpp_cp_svr process while printing FIA trace data on the device.
CSCwq00263	IPv6 IPsec packets are being dropped in SVTI AH in transport mode, causing ping failures for packets of a specific size.

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.