Release Note for Catalyst C1300x Switches MR 4.10.3.26

Release Note for Catalyst C1300x Switches MR 4.10.3.26

Contents

- Introduction
- What's New
- Caveats

First Published: October 28, 2026

Introduction

This release note is for Version 4.10.3.26. This software supports the Catalyst 1300x Stackable Managed Switch Series.

Note The full list of the supported SKUs and the minimal supported version per SKU can be found in below.

Supported Platform

The following tables lists the SKUs that are supported in the Catalyst 1300x series. Each table lists one of the Catalyst 1300x Series and provides information on each SKU description, OID and minimum supported version. Boards not listed in the following table are not supported by Catalyst C1300x release.

sysOID branch: iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cisco (9) . ciscoProducts (1) (OID field below begins from cisco (9) . ciscoProducts (1))

Table 1. Catalyst 1300x Stackable Managed Switches

Device PID	Description	OID	Minimum Supported Version
C1300X-10NU-2X	Catalyst 1300X Series Managed Switch, 10*5G+2SFP28 (C1300X-10NU-2X)	9.1.3410	4.10.0.85

C1300X-24MU-4X	Catalyst 1300X Series Managed Switch, 24*2.5G+4SFP28 (C1300X-24MU-4X)	9.1.3311	4.10.0.85
C1300X-24NGU-4X	Catalyst 1300X Series Managed Switch, 16GE+8*5G+4SFP28 (C1300X-24NGU-4X)	9.1.3412	4.10.0.85
C1300X-24P-4X	Catalyst 1300X Series Managed Switch, 24GE+4SFP28,PoE (C1300X-24P-4X)	9.1.3413	4.10.0.82
C1300X-24T-4X	Catalyst 1300X Series Managed Switch, 24GE+4SFP28 (C1300X-24T-4X)	9.1.3414	4.10.0.82
C1300X-48NGU-4X	Catalyst 1300X Series Managed Switch, 40GE+8*5G+4SFP28 (C1300X-48NGU-4X)	9.1.34.15	4.10.0.85
C1300X-48P-4X	Catalyst 1300X Series Managed Switch, 48GE+4SFP28, PoE (C1300X-48P-4X)	9.1.3416	4.10.0.82
C1300X-48T-4X	Catalyst 1300X Series Managed Switch, 48GE+4SFP28 (C1300X-48T-4X)	9.1.3417	4.10.0.82

What's New

This section details new features and modifications added to Version 4.10.3.26 compared to previous releases.

Power Inline Force-On Command

The **power inline force-on** command was introduced in version 4.10.3.26 to resolve field compatibility issues where certain powered devices could not be detected or powered up. Some devices fail the switch's normal power-on validation process due to class overcurrent conditions, preventing them from receiving

power even though they would function properly once powered.

The **power inline force-on {enable | disable}** command provides administrators with manual override capability to force power delivery to connected devices that fail the switch's standard detection and classification process. When enabled, the command bypasses the normal detection and classification phases, allowing the switch to deliver power directly to devices that would otherwise be rejected. Administrators should enable this feature selectively and only when normal power delivery fails, as bypassing standard safety checks may pose risks to non-compliant devices.

The command includes a safety warning prompting administrators to confirm their action: “Force delivering power to the connected device may damage it. Are you sure? (Y/N)[N]”

“dot1x timeout tx-period” Range Change

In earlier versions, the supported range for the seconds parameter in the **dot1x timeout tx-period seconds** command was 30–65535 seconds. As of version 4.10.3.26, the supported range has been extended to 1–65535 seconds. This enhancement provides greater flexibility when configuring this parameter.

802.1x Unauthorized Ports – Unidirectional Traffic Blocking

In earlier C1300X versions, both ingress traffic (traffic from the supplicant to the switch interface) and egress traffic (traffic from the switch interface towards the supplicant) are blocked for an IEEE 802.1X unauthorized port. This provides a high security level - until a supplicant successfully authenticates, no traffic is allowed in either direction, preventing unauthorized access or data leakage.

However, in some cases it is required to block only ingress traffic and allow egress traffic even if the interface is not authorized. An example of a protocol that requires only ingress traffic blocking is Wake-on-LAN (WoL). WoL requires that a “magic packet” be sent to the sleeping client to wake it up – even if the client is not authenticated. If the port blocks egress traffic (from the network to the supplicant), the WoL packet cannot reach the device, preventing it from waking up. Allowing egress traffic on an unauthorized port also allows IT administrators to send configuration or management traffic to endpoints before authentication.

As of version 4.10.3.26, a new setting defines whether both ingress and egress traffic are blocked on an 802.1X unauthorized interface, or only ingress traffic. The default behavior is to block traffic in both directions for an unauthorized interface. The configuration is applied only to interfaces that are in the 802.1X multi-session mode. Interfaces that are in the multi-host or single-host mode continue to block traffic in both directions even if the command was configured on the interface.

The following CLI commands were added or updated to support this feature:

- **dot1x control-direction {both | in}** – defines the direction of traffic that is blocked on an unauthorized interface
- **show dot1x** – the output of the command was modified to display the control direction setting

RADIUS Attribute 32 (NAS-Identifier) Support

As of version 4.10.3.26, support was added for including RADIUS Attribute 32 (NAS-Identifier) in RADIUS Access-Request and Accounting packets. By default, the device does not send this attribute. Users can explicitly enable transmission of Attribute 32 using the **radius-server attribute 32 include-in-access-req** and/or **radius-server attribute 32 include-in-accounting-req** commands. When enabled, the NAS-Identifier is sent using the device hostname by default. An optional **format** parameter allows users to configure a custom NAS-Identifier string; in this version, support is limited to a user-defined string format.

This feature is configured through the CLI only and is not supported by the GUI management interface. GUI support is planned for a future release.

Extended SNMPv3 Authentication and Privacy Password Length

As of version 4.10.3.26, the maximum supported length for SNMPv3 authentication and privacy passwords has been increased from 32 characters to 64 characters. This enhancement applies to SNMP users configured using the **snmp-server user** command and supports both authentication and privacy credentials.

Extending the supported password length provides greater flexibility when aligning SNMPv3 configurations with modern security policies and external authentication standards that mandate longer credentials. This improvement enables stronger password selection without impacting existing configurations, as previously supported password lengths remain valid.

RFC 2863 Counter32 and Counter64 Interface Packet Counters

As of version 4.10.3.26, all unicast, multicast, and broadcast input and output packet counters defined in RFC 2863 were updated to align with the standard definitions for Counter32 and Counter64 types. In previous versions, counters such as **ifInUcastPkts** in the ifTable MIB were incorrectly reported as Counter64, which did not comply with RFC 2863 requirements.

With this update, **ifInUcastPkts** and similar RFC 2863 counters are now reported as Counter32, while the corresponding high-capacity (HC) counters (for example, **ifHCInUcastPkts**) provide Counter64 statistics. This follows the RFC requirement that 32-bit counters must remain available even when 64-bit counters are supported.

This change improves standards compliance and interoperability with SNMP management and monitoring systems that expect strict RFC 2863 behavior, while still supporting high-traffic interfaces through HC counters for accurate long-term statistics.

Syslog over TCP Support (RFC 6587)

As of version 4.10.3.26, support was added for syslog transmission over TCP in accordance with RFC 6587, in addition to the existing syslog over UDP support. To support this new behavior, the **logging host** command was enhanced with the **[transport {udp|tcp}] [port <port-number>]** parameter, allowing users to explicitly configure the transport protocol and destination port for each syslog server.

Supporting syslog over TCP provides increased reliability for log delivery, ensuring that critical system events are not lost due to packet drops, which can occur with UDP-based transport. This added flexibility allows users to align syslog behavior with network policies, firewall requirements, and log-collection infrastructures that mandate TCP-based logging, while maintaining backward compatibility with existing UDP configurations.

Syslog – Username Added to Logging Enable/Disable Messages

As of version 4.10.3.26, the username and management information are added to the syslog message generated when logging is enabled or disabled (command **logging on/ no logging on**). This is a logging related security feature (tractility).

Changes to the MAC Table Hash Collision SYSLOG Message

The switch stores learned MAC addresses in a hardware Forwarding Database (FDB) using a hash function to map each (VLAN, MAC) pair to a storage location. When too many MAC addresses happen to map to the

same location – a hash collision – the switch cannot store the new entry and generates the %2SWMACTBL-PORTMACHASHFAILED syslog message (for example %2SWMACTBL-N-PORTMACHASHFAILED: Port gi9 ,MAC 72:8d:77:6f:a3:09 : Cannot be added to the FDB (Hash Table Collision)). This is expected behavior inherent to hash-based hardware tables and is not a bug; it may occur in networks with a large number of active MAC addresses.

However, in case of multiple collisions the message may create unnecessary alarm and clutter operational logs. In addition, the message was missing the VLAN ID of the entry, which is an important part of the hash and the FDB entry. To address these issues, as of version 4.10.3.26 the message severity was lowered to debug and the VLAN ID of the entry was added to the message. The new message format (example only) is as follows:

%2SWMACTBL-D-PORTMACHASHFAILED: Port gi9, VLAN 613, MAC 72:8d:77:6f:a3:09 : Cannot be added to the FDB (Hash Table Collision)

No functionality changes were added beyond this change.

rlifPresentTable MIB

In version 4.10.3.26 a new MIB table, **rlifPresentTable**, was added to report only interfaces that are physically present in the stack. Unlike the standard ifTable, which also includes non-existent interfaces (for example, units not currently part of the stack), this table allows management applications to query only interfaces that actually exist. This simplifies monitoring and polling in stacked deployments where users need to operate solely on active stack members.

CBD Network Probe Version

In Version 4.10.3.26 the CBD Network Probe version was upgraded to version 2.12.1.20260608.

New and Updated GUI Pages

This section lists GUI pages and settings that were added or updated in this version and are not reflected in the features listed above – for example, GUI support that was added for features introduced in earlier versions without GUI support.

Table 2. New and updated GUI pages in Version 4.10.3.26

GUI Feature	GUI Page and Details
GUI support for SNMPv3 privacy encryption types (aes-128 | aes-192 | aes-256)	**SNMP > Users** – the “Privacy Method” setting was updated.
GUI support for logging timestamps	**Administration > System Log > Log Settings** – added the “Log Timestamp Timezone”, “Include Milliseconds” and “Show Timezone” settings.
GUI support for disabling SSH server algorithms	**Security > SSH Server > SSH Server Algorithm** – added the SSH Encryption Algorithm, SSH Host Key Algorithm, SSH Key-Exchange Algorithm and SSH Host Mac Algorithm fields.

GUI support for disabling SSH client algorithms	**Security > SSH Client > SSH Client Algorithm** – added the SSH Encryption Algorithm, SSH Host Key Algorithm, SSH Key-Exchange Algorithm and SSH Host Mac Algorithm fields.
GUI support for the logging file (flash) threshold	**Administration > System Log > Log Settings** – added the “Flash Memory Logging Threshold” setting.
GUI support for SNTP SHA-based authentication	**Administration > Time Settings > SNTP Authentication**– added support for the “Authentication Method” setting.
GUI support for the SAN (Subject Alternative Name) field of HTTPS certificates	**Security > SSL Server > SSL Server Authentication Settings**– added the “Subject Alternative Name (SAN)” field when creating HTTPS certificates.

Caveats

Caveats Acknowledged in Release 4.10.3.26.

Bug ID	Description
CSCwx37834	Symptom In the PoE port limit mode, the default "Admin power limit" of the 60w PoE port should be 60w instead of 30w. Workaround Manually configure the "Admin power limit" of this port to 60w through the command " power inline limit 60000".
CSCwx37854	Symptom Console error occurs upon downgrade to pre-4.10.3 releases due to unsupported "dot1x control-direction in" CLI command.The unsupported command should be removed from the running configuration after downgrading. Workaround None

Caveats Resolved in Relase 4.10.3.26

Bug ID	Description
CSCwu07969	Symptom Configuring a negative timezone offset results in an incorrect certificate validity period. Workaround None
CSCwu13951	Symptom Changing the SNMPv3 auth and priv passwords does not take effect. Workaround Reconfigure the settings, or save the current configuration and reload the device.
CSCwu13959	Symptom Incorrect display of C1300X OSPFv3 Neighbor Role/Local Interface. Workaround Verify the information using the CLI.
CSCwr76565	Symptom The no redistribute ospf [process-id] command cannot be executed without optional parameters. Workaround Provide an optional parameter with the required settings.
CSCwr76708	Symptom In some cases, a ‘Bad Packet’ Message” will be displayed, when connecting the devices after OSPFV2 configuration was applied.This is a display issue. OSPF neighbor process is completed successfully. Workaround None
CSCwr86720	Symptom Privacy methods AES256 and AES192 in SNMPv3 cannot be configured in Web GUI. Workaround Use CLI to configure.

Bug ID	Description
CSCwx37890	Symptom When running RSTP, rebooting a switch may trigger a convergence failure until ports are shut down. Workaround None

Copyright © 2026, Cisco Systems, Inc. All rights reserved.