Release Note for Cisco Catalyst 1200 and 1300 Series Switches Firmware Version 4.0.0.91 - 4.1.9.94

First Published: 2026-04-10

Note Generally, Catalyst 1300 series switches can be downgraded to software versions supported by the bootloader software pre-installed on the switch. From time-to-time, Cisco updates the bootloader software to accommodate chipset driver updates and bootloader software cannot be downgraded.

Downgrading to versions earlier than 4.1.3.36 is blocked for the following SKUs:

Catalyst 1300 Stackable Managed Switch with 10G support on all ports
Catalyst 1300 Series Managed Switch, 4-port 2.5GE, 4-port GE, PoE, 2x10G SFP+
Catalyst 1300 Series Managed Switch, 8-port 2.5GE, 16-port GE, PoE, 4x10G SFP+
Catalyst 1300 Series Managed Switch, 16-port 2.5GE, 32-port GE, PoE, 4x10G SFP+

Release Note for Cisco Catalyst 1200 and 1300 Series Switches Firmware Version 4.0.0.91 - 4.1.9.94

First Published: 2026-04-10

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.9.94

August 2026

This Release Note describes the recommended practices and known issues that apply to software version 4.1.9.94 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New in 4.1.9.94

This section details new features and modifications added to Version 4.1.9.94.

Dot1x re-authentication - Session Termination

For releases up to 4.1.9.85, 802.1X reauthentication was performed without terminating the active client session, allowing traffic to continue uninterrupted while reauthentication was in progress. However, in some posture-related reauthentication scenarios, it may be necessary to terminate the existing session before reauthentication is performed.

Starting with release 4.1.9.94, a new optional capability has been added through the dot1x reauthentication terminate-session command, enabling the switch to explicitly terminate the current 802.1X session during reauthentication and require a new session to be established before traffic is restored. By default, this feature is disabled, preserving the previous behavior.

This setting affects both periodic reauthentication and administrator-initiated reauthentication. Reauthentication triggered by CoA or Disconnect messages continues to follow the same behavior as in previous releases.

Caveats

Caveats Acknowledged in Release 4.1.9.94

Bug ID	Description
CSCwu56253	**Symptom** Switch with AXIS cameras connected having issue function randomly.
CSCww15588	**Symptom** A fatal error occurs when changing the TACACS+ server during a privilege level 1 login session, followed by an 'enable' password authentication.
CSCww15596	**Symptom** If the primary TACACS+ server becomes unreachable during the authentication process, there is a 15-second delay before it fails over to the secondary server.
CSCww15606	**Symptom** C1300-48P-4X: Following an STP state transition, the LAG takes 5 minutes to resume traffic forwarding.
CSCww15633	**Symptom** No warning message is displayed when enabling the 'power inline force-on' option in the GUI.

Caveats Resolved in Release 4.1.9.94

Bug ID	Description
CSCws91182	**Symptom** Fatal Error - BRMN - %SEC-F-PORTMACHASHFAILED.
CSCwu01873	**Symptom** Unexpected reboot with Fatal Error Reporting Task: AAAT, "Invalid TCP id".
CSCwq81084	**Symptom** When running RSTP, rebooting a switch may trigger a convergence failure until ports are shut down. This issue is reproducible only in large-scale topologies consisting of 14 or more switches.
CSCww15642	**Symptom** PnP cloud redirection fails with specific DNS servers.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.9.85

April 2026

This Release Note describes the recommended practices and known issues that apply to software version 4.1.9.85 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New in 4.1.9.85

This section details new features and modifications added to Version 4.1.9.85.

Catalyst 1000 Configuration Conversion Tool

A new IOS Configuration Conversion link has been added to the Other Resources section of the Getting Started GUI page. This link redirects users to a Cisco-hosted tool that assists in converting Catalyst 1000 CLI configuration syntax to the equivalent Catalyst 1200 and Catalyst 1300 CLI syntax. The tool simplifies configuration migration and helps streamline the transition from Catalyst 1000–based networks to Catalyst 1200 and Catalyst 1300 platforms.

MAB Default Authentication Method Change to Radius

As of version 4.1.9.85, the default authentication method for MAC-Based Authentication (MAB) has been changed from EAP to RADIUS (relevant CLI command dot1x mac-auth {eap|radius}).

In the earlier versions, MAB defaulted to EAP (dot1x eap), which caused compatibility issues with Cisco ISE guest authentication and required manual configuration to use RADIUS. Aligning the default behavior with other Catalyst platforms improves interoperability and reduces configuration overhead.

RADIUS Attribute 32 (NAS-Identifier) Support

As of version 4.1.9.85, 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; for version 4.1.9.85, 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.

New ignore-nas-id-attributes Option for RADIUS CoA

In NAT-based deployments, RADIUS Change of Authorization (CoA) requests may be rejected due to a mismatch between the NAS identifier in the CoA packet and the switch IP address or hostname. This can happen since packets sent by the CoA Client are addressed to the NAT gateway address before translation.

As of version 4.1.9.85, an optional ignore-nas-id-attributes setting was added to the client command (under aaa server radius dynamic-author configuration mode) to allow CoA requests to be processed despite a NAS identifier mismatch. When enabled, session identifiers are still validated. By default, this setting is disabled

and the switch continues to enforce both NAS and session identifier validation, in accordance with RFC behavior.

SAN (Subject Alternative Name) Support for HTTPS Certificates

As of version 4.1.9.85, users can configure the Subject Alternative Name (SAN) field when creating HTTPS certificates. The SAN extension allows a single certificate to secure multiple domain names and/or IP addresses, providing greater flexibility than the traditional Common Name (CN) field, which supports only a single identifier. The SAN field is optional and can be specified when generating a self-signed certificate or creating a certificate signing request (CSR). The enabling improved compatibility with modern HTTPS deployments and browser validation requirements.

Syslog over TCP Support (RFC 6587)

As of version 4.1.9.85, 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.

Power Inline Force-On Command

The **power inline force-on** command was introduced in version 4.1.9.85 to resolve field compatability 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.

This issue affected certain powered devices connected to the Catalyst 1200 and 1300 series switches.

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.

Miscellaneous Changes

This section details minor issues introduced to version 4.1.9.85.

“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 4.1.9.85, the supported range has been extended to 1–65535 seconds. This enhancement provides greater flexibility when configuring this parameter.

Extended SNMPv3 Authentication and Privacy Password Length

As of version 4.1.9.85, the maximum supported length for SNMPv3 authentication and privacy passwords has been increased from **32 characters to 64 characters**. This enhancement applies to SNMPv3 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 4.1.9.85, 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.

rlifPresentTable MIB

In version 4.1.9.85 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.

Support Additional Tag Values for RADIUS VLAN Attributes (RAVA/DVA)

In earlier versions, RADIUS attributes used for RAVA/DVA VLAN assignment were ignored if the Tag field was set to a non-zero value, which could prevent VLAN assignment when using default Cisco ISE configurations. As of version 4.1.9.85, the switch now supports Tag values in the range 0x00–0x1F for RADIUS attributes Tunnel-Type (64), Tunnel-Medium-Type (65), and Tunnel-Private-Group-ID (81), in accordance with RFC 2868. This enhancement improves interoperability with Cisco ISE and eliminates the need for additional server-side configuration when using tagged RADIUS VLAN attributes.

CBD Network Probe Version

In Version 4.1.9.85 the CBD Network Probe version was upgraded to version 2.10.1.20250619

Caveats

Caveats Acknowledged in Release 4.1.9.85

Bug ID	Description
CSCwt93407	Syslog cannot set both TCP and UDP for the same Syslog server.

Caveats Resolved in Release 4.1.9.85

Bug ID	Description
CSCwo47792	**Symptom** Dynamic VLAN Allocation is not working in PVST mode.
CSCwt26298	**Symptom** C1300 Intermittent Loss of Console Access.
CSCwq41644	**Symptom** Should accept VLAN radius attribute tag other than 0.
CSCwo81510	**Symptom** Change of Authorization to accept colon in calling station ID.
CSCwq81084	**Symptom** When running RSTP, rebooting the device may trigger a convergence failure until ports are shut down.
CSCwi00366	**Symptom** The switch cannot connect to the CBD Dashboard with a static DNS entry if the DNS SRV is unreachable.
CSCwk42463	**Symptom** Subject Alternative Names cannot be configured for Certificate requests generated on the device.
CSCwp23502	**Symptom** IF-MIB::ifInUcastPkts = Wrong Type (should be Counter32 instead of Counter64).

Bug ID	Description
CSCwo58287	**Symptom** Fails to power up AP-UAP-AC-HD.
CSCws80461	**Symptom** Crash when using LogicMonitor Interactive SSH probe.
CSCwq30432	**Symptom** System crash during show tech at show spanning-tree.
CSCwt08877	**Symptom** When using a space character in the port description, the command fails.
CSCwq71179	**Symptom** SCP Username and Password displayed in log as plaintext.
CSCwp01175	**Symptom** Loggin origin-ID sends incorrect timestamp.
CSCwp39924	**Symptom** C1300-16P-4x/C1300-16P-2G - Fails to power on the last PD when it meets the max nominal power supply with class-base mode.
CSCwe81260	**Symptom** Pre-standard PD cannot exit power denied state caused by PoE budget storage.
CSCwe81261	**Symptom** Sometimes the PoE ports cannot recover from an overload state even after a decrease of the load to normal state.
CSCwf56969	**Symptom** PoE issue with DBS-210.
CSCwi00552	**Symptom** The PVST Interface settings page on the GUI displays an empty inconsistency type when the inconsistency type is Port PVID.

Bug ID	Description
CSCwk42479	**Symptom** No monitor capture control-plane command when using optional keywords in or out of control plane is removed completely instead of just removing the specific direction.
CSCwk42490	**Symptom** OPC captured packets from or to the standby/member units are encapsulated into IEEE802a OUI extended ethertype.
CSCwn83021	**Symptom** GUI displays “inactive” for key accept and send life status (security → key management → key settings.
CSCwp84820	**Symptom** "TACACS-W-ABORT" system message is raised when a single TACACS connection is used.
CSCwp84834	**Symptom** The millisecond field in syslog timestamps is always formatted as a two-digit number.
CSCwp84848	**Symptom** The datetime of syslog on the remote log server is incorrect when configuring the timezone with negative offset.
CSCwp85371	**Symptom** Sometimes the auto baud rate causes the console to hang.
CSCwn61510	**Symptom** Tacacs single-connection does not work.
CSCwq15229	**Symptom** MAB authentication issue after switch reboot.
CSCwn61489	**Symptom** The show tacacs status is not connected even when connected.
CSCwp35086	**Symptom** It takes 30 to 40 seconds to converge for RPVST or RSTP on the C1300 when the uplink is in access mode.

Bug ID	Description
CSCwq10393	**Symptom** Issue with multiple authentication methods on interface.
CSCws11612	**Symptom** FATAL ERROR Reporting Task: POLI

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.7.26

January 2026

This Release Note describes the recommended practices and known issues that apply to software version 4.1.7.26 for the Cisco Catalyst 1200 and 1300 Series Switches.

Resolved Issues

Caveats Resolved in Release V4.1.7.26.

Bug ID	Description
CSCws68844	**Symptom** The switch reboots with a fatal error from the DNSC process.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.7.24

October 2025

This Release Note describes the recommended practices and known issues that apply to software version 4.1.7.24 for the Cisco Catalyst 1200 and 1300 Series Switches.

Known Issues

Caveats Acknowledged in Release V4.1.7.24.

Bug ID	Description
CSCwr65287	**Symptom** Applying and subsequently removing a port ACL on a Dot1x authenticated port causes abnormal traffic blocking. **Workaround** Save the configuration, then reboot the device.
CSCws26119	**Symptom** The CLI command "show platform integrity sign nonce 123" and "show platform sudi certificate sign nonce 123" fails. **Workaround** None

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.7.17

June 2025

This Release Note describes the recommended practices and known issues that apply to software version 4.1.7.17 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New in this Release

This section details new features and modifications added to Version 4.1.7.17 compared to previous releases.

TACACS+ Command Authorization and Accounting

Version 4.1.7.17 added support for CLI command authorization and authentication based on the TACACS+ Protocol. The TACACS+ Protocol is only supported on the Cisco C1300 Series switches.

Here is a short explanation for these 2 mechanisms:

- AAA Command Authorization - AAA Command Authorization is a security mechanism to control which users can execute specific commands on the switch. It works by integrating with an AAA (Authentication, Authorization, and Accounting) server (for example TACACS or RADIUS) to enforce policies that restrict command access per each user. For example User A will be allowed to execute all of level 15 commands while User B will be allowed to execute only a subset of level 15 commands.
- AAA Command Accounting - The AAA Command accounting feature tracks and logs the commands executed by users on a network device. This information is sent to a security server (like TACACS+ or RADIUS) for auditing, billing, and network management purposes.

The following CLI commands were added or updated to support these 2 features:

Command Authorization

- aaa authorization commands privilege-level {default | list-name} method [method2...]} – defines the list of protocols that are used for authorizing CLI commands.
- aaa authorization config-commands — defines that CLI configuration mode commands require authorization.
- aaa authorization console — enables command authorization for CLI commands configured on the console management interface.
- authorization commands privilege-level {default| list-name} — enables a commands authorization method list for a management line.
- show authorization methods — displays information about the commands authorization methods.

Command Accounting

- aaa accounting commands privilege-level {default | list-name} method} — defines the list of protocols that are used for commands accounting.
- accounting commands privilege-level {default| list-name} – enables a commands accounting method list for a management line.
- show accounting - displays information as to which type of accounting is enabled on the switch, and if periodic updates are enabled.

This feature is supported on the Cat 1300 and Cat 1300 stacking families.

Disabling SSH Algorithms

The device supports both SSH server and SSH client. Both the server and the client supports the following SSH algorithms:

- Host-key Algorithms - rsa-sha2-512,rsa-sha2-256,ssh-rsa
- Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm, aes256-gcm
- MAC Algorithms: hmac-sha2-256, hmac-sha2-512,hmac-sha1
- Key exchange (KEX) Algorithms: diffie-hellman-group16-sha512, diffie-hellman-group14-sha1

A setting was added to this version which disables one or more of SSH algorithms in the categories listed above. At least 1 algorithm must remain active in each category. The SSH server and client will advertise only algorithms that were not disabled by the user. The settings for the SSH server and SSH client are separated.

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

- ip ssh server algorithm {encryption enc-alg1 [enc-alg-2…]} | {hostkey host-alg1[host-alg2…]} | {kex kex-alg1[kex-alg2…]} | {mac mac-alg1[mac-alg2…]} — enable on the SSH server one or more of the algorithms used for the SSH session encryption.
- ip ssh-client algorithm {encryption enc-alg1 [enc-alg-2…]} | {hostkey host-alg1[host-alg2…]} | {kex kex-alg1[kex-alg2…]} | {mac mac-alg1[mac-alg2…]} — enable on the SSH server one or more of the algorithms used for the SSH session encryption.
- show ip ssh — command output updated to show SSH server algorithm support and setting.
- show ip ssh-client — command output updated to show SSH client algorithm support and setting.

This feature is relevant to all the product families.

SNMPv3– New Encryption Methods

In previous version only AES-128-CFB algorithm was supported for SNMPv3 encryption (or no encryption at all). From version 4.1.7 and on, the device sill support 2 additional encryption methods: AES-292-CFB and AES-256-CFB.

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

- snmp-server user username groupname {v1 | v2c | [remote host] v3[auth { sha | sha224| sha256| sha384| sha512} auth-password [priv {aes-128|aes-192|aes-256} priv-password]]}— {aes-128|aes-192|aes-256} was added as a mandatory parameter when enabling SNMPv3 encryption (priv keyword).
- show snmp users — the command output was modified to display the encryption method configured by the user.

Note When upgrading from a previous version to version 4.1.7 (or higher), SNMP user configuration will be maintained, and the keyword aes-128 will be added to existing snmp-server user commands.

When downgrading from version 4.1.7 (or higher) to a version that supports only aes-128 encryption

- The configuration of the SNMPv3 users that were defined with aes-128 algorithm will be preserved after the downgrade, and the keyword aes-128 will be removed from the existing snmp-server user commands.
- The configuration of SNMPv3 users defined with other algorithms (aes-192 and aes-256) will be removed from the configuration after the downgrade.

This feature is relevant to all the product families.

SNTP New Authentication Key Algorithms

Up to Catalyst C1200/C1300 version 4.1.7, md5 algorithm was the only protocol supported for SNTP key authentication. From Version 4.1.7 and on the following authentication methods will be supported in addition to md5:

- sha1 - Authentication using the SHA1 hash function
  - The key length is 1 to 32 bytes
  - The digest length is 128 bits
- sha2-256 - Authentication using the SHA2 hash function.
  - The key length is 1 to 32 bytes
  - The digest length is 160 bits (the 1st 20 bytes of the digest result).
  - The hash is computed over the key followed by the SNTP packet header and extensions fields (but not the Key Identifier or Message Digest fields). This method is similar to the method defined in RFC5905 (section 7.3).
- hmac-sha2-256 - Authentication using HMAC using the SHA2 hash function.

- The key length is 1 to 32 bytes
- The digest length is 256 bits
- The hash computation uses the key provided in the command for the inner and outer key generation. The actual hash "source" is the SNTP packet header and extensions fields (but not the Key Identifier or Message Digest fields), and does not include the key provided in the CLI command.

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

- sntp authentication-key key-number authentication-algorithms key-value — The authentication-algorithms parameter was updated to include the following algorithms (in addition to md5 which was already supported): sha1, sha2-256 and hmac-sha2-256.
- show sntp configuration — The command output was modified to display the algorithm configured for SNTP authentication.

This feature is relevant to all the product families.

Syslog Message Timestamp Configuration

Up to Catalyst 1200/1300 version 4.1.7 there was a single format for syslog messages timestamp. The format was dd-MMM-yyyy HH:mm:ss. For example 30-Apr-2025 10:46:12.

In some cases, a more flexible time-stamp format is required to allow more accurate timing of the message and to support event logging for devices across multiple time zones. To support this flexibility in version 4.1.7, the following time stamp functionalities were added:

- Adding Milliseconds to the timestamp.
- Adding time zone abbreviation to the timestamp.
- Defining that the timestamp will reflect local time (the current behavior and the default) or UTC.

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

- service timestamps log datetime {[utc| localtime] [msec] [show-timezone]} — defines the format of the timestamps that are included in syslog messages

This feature is relevant to all the product families.

Note This feature does not support a dedicated show command. The configuration can be viewed via the show running-config command.

The Catalyst 1000 default time-zone is UTC. The Catalyst 1200 and Catalyst 1300 default time-zone display is the local time, as this was the default time-zone in the previous version.

This feature changes the format of the timestamp in syslog messages. This means that the format of the log entry in this version is different from the one in the previous versions. Consequently, the flash log is erased upgrading/downgrading to/from a version supporting/ not supporting the time stamp configuration.

802.1x Unauthorized Ports– Unidirectional Traffic Blocking

Unidirectional Traffic Blocking – Introduction

In the version before release 4.1.7, 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 should be allowed in either direction to prevent unauthorized access or data leakage.

However, in some cases it is required to block only ingress traffic (traffic from the supplicant to the switch interface) 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 client is not authenticated. If the port is blocking 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.

Unidirectional Traffic Blocking – Functional Description

To address the WoL (and other) scenarios, new setting was added to release 4.1.7 which defines whether both ingress and egress traffic will be blocked on 802.1x unauthorized interface, of if just ingress traffic will be blocked. The default behavior is to block traffic in both direction 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 will continue to block traffic on both directions even if this 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 un-authorized interface.
- show dot1x – the output of the command was modified to display control direction setting.

Erratum

There was an error on the datasheet on the size and dimensions of the C1200-8T-D switches.

Info in Datasheet for the C1200-8T-D are dimensions are 160 x 128 x 30 mm (6.3 x 5.04 x 1.18 in) weight: is 0.54 kg (1.19 lb)

The correct dimensions for the C1200-8T-D are 177*141.5*30mm (6.96*5.57*1.18 in) weight is 0.58kg (1.28 lb).

Known Issues

Caveats Acknowledged in Release V4.1.7.17.

Bug ID	Description
CSCwp84681	**Symptom** There is no response for the Net-SNMP v3 query when using specific authentication and privacy options. **Workaround** Use SHA/AES-192-C, SHA/AES-256-C or SHA-224/AES-256-C instead.

Bug ID	Description
CSCwp84809	**Symptom** When commands are authorized via TACACS, the command interface GigabitEthernet (with a space) 1/0/1 and interface GigabitEthernet1/0/1 are matched to different ISE command sets. **Workaround** None.
CSCwp84820	**Symptom** TACACS-W-ABORT system message is raised when a single TACACS connection is used. **Workaround** To enable single connection mode, select the Legacy Cisco Device option.
CSCwp84834	**Symptom** The milliseconds field in syslog timestamps is always formatted as a two-digit number. **Workaround** None
CSCwp84848	**Symptom** The datetime of syslog on the remote log server is incorrect when configuring the timezone with negative offset. **Workaround** None
CSCwp84863	**Symptom** When redirect ACL and filter-id are configured on ISE, the device WEB GUI fails to display the redirect URL on the dot1x session details page. **Workaround** None
CSCwp84865	**Symptom** Show detail dot1x session always displays the first interface entry if the user is identical. **Workaround** None
CSCwp84876	**Symptom** The Telnet/SSH login and authorization configurations cannot be combined under the line telnet/ssh section. **Workaround** None

Bug ID	Description
CSCwp85371	**Symptom** Sometimes auto baud rate cause console hang **Workaround** Disable auto baud rate on the console.
CSCwp85600	**Symptom** Show clock always display last synchronized 00:00:00 ago when using broadcast SNTP. **Workaround** None.
CSCwp85610	**Symptom** The service timestamps log datetime command is not supported on the GUI. **Workaround** Configure via the CLI
CSCwp85687	**Symptom** The timestamps for logging do not work on the Flash memory page of the Web GUI. **Workaround** Check the log in the CLI.
CSCwn65293	**Symptom** C1300 FATAL ERROR Reporting task: PNPA **Workaround** Avoid using special characters.

Resolved Issues

Bug	Description
CSCwn60736	**Symptom** It takes 30-40 seconds to converge for RPVST or RSTP on the C1300.
CSCwo04461	**Symptom** C1300-48T-4X: received traffic which failed to send out to the inter-link LAG.
CSCwn52331	**Symptom** C1200/C1300 enhancement request: support for RADIUS attribute 8 (Framed-IP-Address)

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.6.54

March 2025

This Release Note describes the recommended practices and known issues that apply to software version 4.1.6.54 for the Cisco Catalyst 1200 and 1300 Series Switches.

Resolved Caveats

Caveats Resolved in Release V4.1.6.54.

Bug ID	Description
CSCwm08426	**Symptom** SFP-10G-T-X with ACWxxxx serial number does not work.
CSCwk42474	Link up may fail on some SKUs when inserting SFP-10G-T-X and set speed to 1G speed. **Note** SKUs affected include all of the C1300 stacking 10G SKUs.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.6.53

February 2025

This Release Note describes the recommended practices and known issues that apply to software version 4.1.6.53 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications added to Version 4.1.6.53 compared to previous releases.

On-board Packet Capture - GUI Support

On-board Packet Capture (OPC) support was added in release 4.1.3.x (see section 4.2.4 below). It is supported on all product families. In Version 4.1.3.x the feature control was available only via the CLI. Version 4.1.6.x added GUI controls for this feature.

IPv6 Host Certification

Version 4.1.6.53 was updated to pass the IPv6 forum (https://www.ipv6forum.com/) IPv6 Ready IPv6 Host conformance tests, except for tests that require support for RFC7217 (Method for Generating Semantically Opaque Interface Identifiers with IPv6 stateless address auto configuration (SLAAC)).

Changes to the RADIUS Client Behavior

The changes to RADIUS client functionality that is described in this section were done to address the MD5 vulnerability reported in CVE-2024-3596. This section provides information on this vulnerability and the changes that are made to the device behavior in order to address the vulnerability.

CVE-2024-3596 Vulnerability

The attack that is detailed in CVE-2024-3596 exploits the inherent weakness of the MD5 algorithm that is used by the RADIUS protocol (Based on RFC 2865).

The successful execution of this attack may result in a compromise of the RADIUS packet exchange between the switch acting as a RADIUS client, and the RADIUS server. At the extreme exploitation of this vulnerability, the attacker gains the ability to authenticate or authorize any user.

Currently, the attack is not possible if all the messages (RADIUS requests and RADIUS responses) exchanged between the switch and the RADIUS server include the Message-Authenticator attribute (type 80).



Note In order to exploit the attack, the attacker must use a high CPU power computer and physical access to the user network.

Device Vulnerability – Pre Version 4.1.6.x

RFC 2869 defines that the Message-Authenticator attribute is mandatory for RADIUS exchanges that contain an EAP Message attribute (type 79). On the Catalyst 1200/1300 switches, the following applications do not contain an EAP Message attribute, and are therefore vulnerable to this attack:

- AAA authentication based on RADIUS
- 8021.x MAC-based authentication (MAB) using the RADIUS authentication method (command dot1x mac-auth RADIUS)

802.1x authentication and MAC-based authentication (MAB) using the EAP method (command dot1x mac-auth EAP – which is the default configuration), are not vulnerable to this attack. The RADIUS requests that in these applications contain the EAP Message attribute, and the device also verifies that the RADIUS responses include this attribute and that it is valid.

Changes to the Device Behavior

To prevent the exploitation of vulnerabilities the following changes were implemented in the Catalyst 1200/1300 4.1.5 release. Their purpose is to ensure that the Message-Authenticator attribute is included in all RADIUS packets:

- The Message-Authenticator attribute is included in all RADIUS request packets – including AAA authentication and 8021.x MAC-based authentication (MAB) using the RADIUS authentication method.
- The Message-Authenticator attribute is included as the 1st attribute in the RADIUS request packet. This is also implemented for 802.1x authentication and MAC-based authentication (MAB) using the EAP method.
- A new setting was added to this release - The user can define that the Message-Authenticator is mandatory for all RADIUS responses and not only for RADIUS responses that contain the EAP Message attribute. RADIUS responses that do not include this attribute (or that the authenticator is not valid) will be dropped.

By default the Message-Authenticator is mandatory only for RADIUS responses that contain the EAP Message attribute.

Note The reason this setting is optional and disabled by default, is to allow compatibility with existing RADIUS server behavior.

According to RFC 2869 the Message-Authenticator is not mandatory in RADIUS responses that do not contain the EAP-Message attribute. Therefore, unless the RADIUS request contains the EAP-Message attribute, many RADIUS servers will not include a Message-Authenticator attribute in the response even if the RADIUS request included the Message-Authenticator.

In the future, when RADIUS server behavior will be modified to include the Message-Authenticator attribute in all responses (to address this vulnerability), this behavior may be enabled by default or even mandatory.

New CLI Commands

- The following CLI command was added to the device to enable/disable mandatory Message-Authenticator attribute in all RADIUS responses: “RADIUS-server force-message-authenticator host {ip-address | hostname}”. The default is disabled.
- The “show RADIUS-servers” command was updated to display whether the setting is enabled or disabled.

Cisco Identity Services Engine (ISE)

Cisco Identity Service Engine (ISE) is a leading, identity-based network access control and policy-enforcement system. It is a common policy engine for controlling endpoint access and network device administration for enterprises. ISE allows an administrator to centrally control access policies for wired, wireless, and VPN endpoints in a network.

Catalyst 1200/1300 version 4.1.6 added support for the Guest Access Control ISE network applications which is based on the following network functionalities.

- Dynamic ACL – automatically applying ACLs per user
- URL redirection – redirecting user browser to a predefined web-based authentication server

In order to support the guest access control the following features were added in Catalyst 1200/1300 version 4.1.4:

- Dynamic ACL based on RADIUS standard Filter-id (type 11) attribute
- Dynamic ACL based on Cisco VSA attribute ACS: Cisco Secure-Defined-ACL (a.k.a downloadable ACLs)
- URL redirection based on Cisco VSA attributes URL-redirect-ACL and URL-redirect.
- IPDT
- Interim accounting updates
- 2 new CoA commands

Note The default MAB authentication mode is EAP. For proper interaction with ISE guest control access the MAC-based authentication methods must be set to RADIUS (command “dot1x mac-auth RADIUS”).

IP Device Tracking

The IP Device Tracking (IPDT) feature is responsible for maintaining an IP to MAC-mapping database of hosts that are connected to the switch. IPDT relies on ARP snooping and DHCP snooping to detect host and map the host MAC to the host IP address. IPDT maintains a database of these mappings. The information in this database is used by other applications – for example for applying the supplicant IP address as part of the dynamic ACL IPDT is active on an interface if 802.1x is enabled on it. There is also a way to manually enable IPDT on an interface.

This feature is supported only on the Catalyst 1300 and Catalyst 1300 stacking families.

RADIUS Accounting Interim Updates

Up to version 4.1.6.x the Catalyst 1200/1300 switches supported only 2 types of accounting packets – Start (Acct-Status-Type = 1) and Stop (Acct-Status-Type = 2). From version 4.1.6 and on the device also supports the Interim-Update packet type (Acct-Status-Type = 3)

Interim-Update accounting packets are sent in the following events:

- Following an 802.1X reauthentication event - Examples for reauthentication scenarios – the expiration of reauthentication period on the interface, or following a “reauthenticate” CoA command
- Following an update to the 802.1x supplicant IP address – the changes of a supplicant IP addressed are tracked via the IPDT table.

Periodic accounting updates are enabled –Periodic accounting updates is enabled on the device via the (new) aaa accounting update periodic number command. In this case, an accounting Interim-Update packet will be sent for each 802.1x or AAA session at every interval as set by the user.

This feature is supported only on the Catalyst 1300 and Catalyst 1300 stacking families.

New CoA Commands

The following 2 CoA commands were added in version 4.1.6:

- reauthenticate-type=rerun
- reauthenticate-type=last

These 2 commands may appear in the same CoA request that includes the reauthenticate (host) command.

This feature is supported only on the Catalyst 1300 and Catalyst 1300 stacking switches.

FIPS 140–2 Compliance

What is FIPS

FIPS stands for Federal Information Processing Standards. FIPS 140 is a specific series within the FIPS standards that focus on the security requirements for cryptographic modules. These modules are hardware or

software components that are used to encrypt and decrypt data. The FIPS 140 series ensures that these cryptographic modules meet stringent security standards to protect sensitive information.

Catalyst 1200/1300 FIPS Compliance

Catalyst 1200/1300 version 4.1.6.x is compliant with FIPS 140–2 which was published in 2001. The compliance is in relation to the following management channels, which mean they use only FIPS-approved encryption/decryption, hashing and authentication algorithm:

- HTTPS server and client (TLSv2 and V3)
- SSHv2 server and client
- SNMPv3

FIPS Compliance Mode

Version 4.1.6 supports 2 operational modes:

- FIPS-compliant mode – supports only FIPS-approved encryption/decryption, hashing, and authentication algorithm.
- FIPS non-compliant mode – may support encryption/decryption, hashing, and authentication algorithm that are not FIPS-approved.

By default, the switch operates in the FIPS non-compliant mode. Switching between modes requires device reboot and will remove the SSH key and the SSL key and certificate configuration. The operational FIPS mode is displayed at device bootup and also in the output of the “show fips status” CLI command

In Version 4.1.6 the main difference between FIPS-compliant mode and FIPS non-compliant mode is: that FIPS-compliant mode does not support the following:

- DSA keys (SSH client and server) are not supported in FIPS-compliant mode.
- The chacha20-poly1305@openssh SSH Server Cipher (SSH client and server) is not supported in FIPS-compliant mode.
- The TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) cipher is not supported in FIPs compliant mode.
- OpenSSL version:
  - FIPs compliant mode supports 2 OpenSSL versions – based provider version 3.0.14 and FIPS provider version 3.0.9.
  - FIPS non-compliant mode supports only the based provider version 3.0.14.

Known Issues

Caveats Acknowledged in Release V4.1.6.53.

Bug ID	Description
CSCwm90485	**Symptom** 2SWMACTBL-N-PORTMACHASHFAILED: Port x,MAC xx:xx:xx:xx:xx:xx: Cannot be added to the FDB (Hash Table Collision) syslog messages may displayed on the screen. **Workaround** This is an expected behavior due to mac address table updates. It will occur only if mac learning causes hash collisions. Entry with collisions will not be learned until the collision is resolved.
CSCwn83021 **Note** Relevant only for the C1300 model.	**Symptom** GUI displays "inactive" for key accept and send life status (security > key management > key settings. **Workaround** This is a display issue in the GUI. The keys are actually active.
CSCwn83022 **Note** Relevant only for the C1300 model.	**Symptom** The 1st rule of downloadable ACLs is not displayed in the output of the “show ip access-lists interface” command. **Workaround** This is just a display issue and the rule is actually active. To view the ACL with all rules use the “show access-lists” command.
CSCwk77710	**Symptom** The switch may reboot if all ports are configured to SmartPort enable or disable via CBD. Error message format: %CDB-F-NONOWN: CDBG_releaseAccess **Workaround** Enabled or disable Smartports in smaller blocks (not all ports on the device).
CSCwn83025	**Symptom** When the switch acts as a telnet client its CPU increases once the session to the telnet server (remote switch) is timed out. **Workaround** Press enter on switch console.

Bug ID	Description
CSCwn83030	**Symptom** The SNMP add community screen in basic mode does not display checkbox for the “View Name” field. It also allows to check the “Advanced” field and it should not. **Workaround** None.
CSCwn83036	**Symptom** In rare cases the wrong auto voice VLAN ID may be selected. This behavior will occur only if UC5xx device location is changed and also voice VLAN ID is changed. **Workaround** None
CSCwn83037	**Symptom** When a switch is connected to CBD and a HW error occurs – the LED on the member units front panel changes to blinking yellow (expected behavior) but the LED in GUI remains blue. **Workaround** This issue occurs only on the member units in a stack (does not occur on active unit or on standalone devices). Check the LED on device front panel to detect HW failure.
CSCwn83038	**Symptom** Dot1x violation trap setting will change if the host authentication mode is changed via the GUI while the port Administrative Port Control is not in Force Authorized. **Workaround** Don’t change dot1x setting via GUI while the port is not in forced authorized mode.
CSCwn83040	**Symptom** Configuring Private VLAN settings via GUI may fail if the upper limit of primary VLANs has been reached. **Workaround** Issue does not happen when configuring via CLI.

Bug ID	Description
CSCwn83041 Relevant only for the C1200 model.	**Symptom** The Clear Interface Counters button does not clear RMON statistics (Status and Statistics > RMON > Statistics). **Workaround** Use the Clear Interface Counters button from the “View All Interfaces Statistics” screen.
CSCwo04949 **Note** Relevant only for the C1300 model.	**Symptom** Fails to display the downloadable ACL applied for the dot1x supplicants other than the first one. **Workaround** This is just a display issue and the downloadable ACL works fine.
CSCwo08732	**Symptom** Cannot reach the maximum QoS and ACL HW resource. **Workaround** It is a display issue. Once the VLAN ACL is applied, the system will reserve (use) the four rules. However, these four rules are not displayed.

Resolved Issues

Caveats Resolved in Release V4.1.6.53.

Bug ID	Description
CSCwi91143	**Symptom** C1300- dot1x MAB issue with PVST.
CSCwn17952	**Symptom** C1300/1200 - interoperability issue with Cisco DECT 110.
CSCwk42458	**Symptom** An error message “Login banner too long” is displayed in GUI when entering a banner with more than 519 characters.
CSCwk42481	**Symptom** The Syslog Notifications Pop-Up in GUI stops working if the log table is has more than 1000 items.
CSCwe81238	**Symptom** Auto surveillance VLAN (ASV) will not be active on general mode port if STP mode is set to PVST/RPST.

Bug ID	Description
CSCwk42476	**Symptom** RIP – routes are redistributed even if redistributing is not enabled.
CSCwi00748	**Symptom** “show lldp local tlvs-overloading” command output - the field “Left” (bytes for TLV) displays the number of overloaded bytes instead of the bytes still available for local TLVs.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.4.1

September 2024

This Release Note describes the recommended practices and known issues that apply to software version 4.1.4.1 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications added to Version 4.1.4.1 compared to previous releases.

Password Complexity - Keyboard Pattern Prevention

- A new password complexity setting called Keyboard pattern prevention was added in this version.
- When enabled, the password configured by the user can’t include more than three consecutive letters or numbers keys on the QWERTY keyboard.
- This feature can be enabled or disabled using the “passwords complexity keyboard-pattern” CLI command. By default, this feature is disabled. In the current version there isn’t GUI control for this setting.
- The feature applies to the passwords configured via one of the following commands “username” (Global Configuration mode command) “enable password” (Global Configuration mode command) and “password” (Line Configuration mode command).

Masked Secret

- From this version and on the user has the option to type in a password as a masked secret, instead of a cleartext password. The masked secret is provided by the user following a prompt displayed on the screen. The masked password needs to be confirmed by the user, as follows:

```
switch(config)#username example privilege 15 masked-secret
Enter secret: ********
secret: ******** Confirm secret: ********
```

- This ability was added to the following commands “username” (Global Configuration mode command) and “enable password” (Global Configuration mode command).

- The command including the password is saved to the configuration in the same format as a command entered in cleartext.

Security Syslog

Security-related messages were enhanced to include the following:

- The syslog messages which indicate firmware upgrade success or failure, includes the following information:
  - The management interface from which the firmware operation was initiated (Console, telnet, SSH, HTTP, or HTTPS).
  - The username of the management session that initiated the firmware operation.
  - The IP address of the management session that initiated the firmware operation.
- A syslog message, which includes the information detailed in the previous item, is generated when one of the following management interfaces are enabled or disabled: SSH; Telnet; HTTP/HTTPS or SNMP.

Log File Exceed Threshold

- In this version the user can configure an alarm threshold for the logging file (file messages stored to the flash).
- Once this threshold is exceeded a syslog message is generated indicating the threshold has been crossed.
- The command to set this threshold is “logging file threshold percent” where percent is a number 1–99. By default, a threshold isn’t defined - which means the syslog message won’t be generated.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.3.36

June 2024

This Release Note describes the recommended practices and known issues that apply to software version 4.1.3.36 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications added to Version 4.1.3.36 compared to previous releases.

Radius Change of Authorization (CoA)

Supported on the C1300 standalone and C1300 stack families.

Radius Change of Authorization (CoA) is an extension to the RADIUS protocol, allowing dynamic changes to an AAA or dot1x user session. This includes support for disconnecting users and changing authorizations applicable to a user session. The device acts as a CoA server receiving Change of Authorization (CoA) and Packet of Disconnection requests from a CoA client. CoA is supported for 802.1x sessions. the following CoA commands are supported

- “disable host port” command - included in a Cisco VSA “Cisco:Avpair=“subscriber:command=disable-host-port”
- “Bounce host port” command - included in a Cisco VSA “subscriber:command=bounce-host-port”
- “Reauthenticate host” Command - included in a Cisco VSA “Cisco:Avpair=“subscriber:command=reauthenticate”

Audit-Session-ID

Supported on the C1300 standalone and the C1300 stack families.

The Cisco Vendor Specific Audit-Session-ID RADIUS attribute is used to uniquely identify a user session. The device will include this attribute in all messages sent to the RADIUS server. The same Audit-Session-ID will be used for all authentication, authorization and accounting messages until the session is terminated.

HTTPS Server Certificate Chain/ Intermediate Certificate

Supported on all product families.

During the SSL/TLS handshake between the Switch (HTTPS server) and a browser (HTTPS client), the Switch presents its signed certificate. The browser, having the CA certificate in its trusted store, uses the CA's public key to verify the signature on the server certificate. This process establishes the authenticity of the server's identity. Once verified, the server and browser proceed to exchange cryptographic parameters, enabling the encryption of data in transit between them, ensuring a secure and authenticated connection for data transmission over HTTPS.

While server certificates can be directly signed by the root CA certificate, the use of intermediate certificates introduces a hierarchical structure that enhances the signing process. Intermediate certificates act as intermediaries between the server certificate and the root CA, offering benefits such as increased security through isolation of key compromises, flexibility in certificate management, and the ability to delegate signing authority. This hierarchical approach provides improved scalability, eases certificate renewal processes, and allows for more granular control over revocation. In essence, employing intermediate certificates enriches the signing process by providing enhanced security, flexibility, and streamlined certificate management.

The C1300 supports the following functionalities related to intermediate certificate and HTTPS server certificate chain:

- Installation of one or more intermediate certificates.
- Including the intermediate certificate(s) in the TLS handshake with the HTTPS client
- Display of intermediate certificate
- Display of the certificate chain of the device’s HTTPS server certificates

On-board Packet Capture

Supported on all product families.

The Onboard Packet Capture (OPC) provides the ability to capture packets received and sent on device interface and by CPU. The packet captures can then be displayed locally, saved to local storage, or exported for offline analysis. The OPC feature enhances troubleshooting capabilities on the device.

OPC on the C1300 supports the following:

- Creating up to 4 capture points – which are session for capturing packets. Packet capture is supported for the control plane (CPU) interface
- Define the following capture point attributes:
  - Define the capture direction (in, out or both)
  - Define the buffer mode and buffer size
- Starting or stopping a capture session (only 1 capture point can be active)
- Displaying capture buffer statistics
- Exporting the capture file to a *.pcap file on local flash or the USB.

GUI Management interface is not supported in this version.

"show diff-config" – New CLI Command

Supported on all product families.

Version 4.1.3.36 supports a new CLI command “show diff-config”. This command compares and displays the differences between the running and startup configuration file. This command is useful in cases where the user reboots the device and is prompted to save the running configuration.

CBD Connection System LED Indication

Supported on all product families.

The System LED will provide a tri color (Green, Yellow, Blue) indication. The new color (blue) will provided CBD connection info, as follows:

- Green LED (the default LED color (once the software is fully loaded)), provides the following indications:
  - No errors detected
  - The device is not connected to the CBD Dashboard
  - Supports LED flashing to indicate specific information (e.g. stack unit ID indication, reset button push duration etc) – the definition for the system LED flashing is detailed in other specifications
- Blue LED, provides the following indications:
  - No errors detected
  - New indication - The CBD agent on the device is connected to the Dashboard (Dashboard status == connected in the “show cbd” command output)
  - Supports LED flashing to indicate specific information (e.g. stack unit ID indication, reset button push duration etc) – the definition for the system LED flashing is detailed in other specifications
- Amber LED provides the following indications: error conditions exist on the device (e.g. detect HW failed, firmware failure or/and configuration file error)

The connection to the Dashboard is polled every 5 seconds. If the status of the connection changes, then the LED color will change accordingly.

If an error condition occurs, the system LED shall change from green or blue (depending on the state when error occurred) to amber. Once the error condition stops the LED will return to either green or blue color based on the latest poll indication.

CBD - add CBD Probe Mode Information

Supported on all product families.

Added CBD probe mode information to CLI Operational status field (show cbd command) and Probe Status GUI field. The probe mode is relevant only when the probe is active. The following probe modes are displayed:

- Probe Managed - The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard
- Direct Managed - Direct managed devices will discover other devices in the broader network and connect those devices to the Dashboard automatically then those devices become manageable.

SSL Updates

Effects all product families.

- OpenSSL version upgraded to version 3.0.11 (19 Sep 2023)
- Support for the following ciphers was removed in version 4.1.3.36:
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
  - TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072)
  - TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072)
  - TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 3072)

SSH Updates

Effects all product families.

Support for the following ciphers was added:

- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

Support for the following SSH Key Exchange methods (KEX) was removed in version 4.1.3.36:

- diffie-hellman-group1-sha1

Changed to GUI

Effects all product families.

- Added "Virtual Assistant" and CBD links to the Getting Started page
- Added to GUI mast an CBD icon which provides a link to the CBD product web page.

Known Issues

Caveats Acknowledged in Release V4.1.3.36.

Bug ID	Description
CSCwk42456	**Symptom** The SFP+ Port LEDs alternately flash green and amber when transmitting jumbo frame and jumbo frame support is disabled. This is a display issue. Jumbo frame handling is correct. **Workaround** None
CSCwk42458	**Symptom** An error message “Login banner too long” is displayed in GUI when entering a banner with more than 519 characters. **Workaround** None
CSCwk42463	**Symptom** Subject Alternative Names cannot be configured for Certificate requests generated on the device (command “crypto certificate request”). This generates an error message on browser when connecting via HTTPS. **Workaround** Generate a certificate request using an external tool.
CSCwk42465	**Symptom** When executing "show diff-config context-lines 0", the context-line count is empty instead of 1. **Workaround** None
CSCwk42467	**Symptom** The route time for RIP entries continues to increment and do not reset every 30 seconds. **Workaround** None
CSCwk42470	**Symptom** Revocation of intermediate certificate fails and secure access is provided based on this certificate **Workaround** Copy running to startup and reload the switch.

Bug ID	Description
CSCwk42473	**Symptom** On some SKUs the sflow flow-sample does not work on a port that is a member of a port-channel **Workaround** None
CSCwk42474	**Symptom** Link up may fail on some SKUs when inserting SFP-10G-T-X and set speed to 1G speed. **Workaround** None
CSCwk42476	**Symptom** RIP – routes are redistributed even if redistributing is not enabled. **Workaround** None
CSCwk42479	**Symptom** “No monitor capture control-plane” command – when using optional keywords in or out control plane is removed completely instead of just removing the specific direction. **Workaround** Remove control-plane and then re-add the required direction.
CSCwk42481	**Symptom** The Syslog Notifications Pop-Up in GUI stops working if the log table is has more than 1000 items. **Workaround** None
CSCwk42484	**Symptom** The display of time source in the GUI is "from browser" even though the time was set manually. **Workaround** Use CLI command "show clock detailed" to view correct clock source.
CSCwk42485	**Symptom** CLI command "no monitor capture match" in CLI guide is not supported. **Workaround** None.

Bug ID	Description
CSCwk42490	**Symptom** OPC captured packets from or to the standby/member units are encapsulated into IEEE802a OUI extended ethertype. **Workaround** None
CSCwk42492	**Symptom** On C1300 10G SKUs monitor session cannot capture the packets dropped by configured ACL. **Workaround** None
CSCwm50839	**Symptom** C1200/1300 - UDLD Exchange Fails with Nexus. **Workaround** None

Resolved Issues

Caveats Resolved in Release V4.1.3.36.

Bug ID	Description
CSCwi56166	**Symptom** SSH to device fails when using RSA-SHA2-512 and RSA-SHA2-256 host key algorithm in Key exchange.
CSCwk42496	**Symptom** The 'PVST Interface settings' page on the GUI displays inconsistency type “PVID” even though the actual inconsistency type is “Port Type”.
CSCwk42499	**Symptom** Loopback detection fails when STP mode is PVST and STP is disabled.
CSCwi00760	**Symptom** Device console and GUI will not respond for about 3 minutes in the following scenario: • One or more DNS servers configured on device are not reachable. • In this state the user deletes and then adds the default SNTP servers.

Bug ID	Description
CSCwe81254	**Symptom** An error message will appear on console if the DHCP pool name includes special chars (for example single quote, double quote, backslash) and user presses the “details” button in IPv4 Configuration→ DHCP Server → Network Pools GUI page.
CSCwj13150	**Symptom** In some cases address count are not decremented on a port that is configured to port security Dynamic Lock mode. This may prevent other MACs to be learned.
CSCwj75101	**Symptom** DHCP server does not respond to Discover packet from client if the discover packet includes an option 55 (Parameter request list) with value 0.
CSCwi00359	**Symptom** In some cases stack interface LED may not light up when disconnecting then reconnecting stacking cable.

Resolved Issues 4.1.0.76

Table 1: Caveats Resolved in Release V4.1.0.76.

Bug ID	Description
CSCwi77502	**Symptom** In rare case there is slight packet loss on C1300-24XT when forwarding traffic in line rate and using long Cat6A cables.

Known Issues 4.1.0.75

Table 2: Caveats Acknowledged in Release V4.1.0.75

Bug ID	Description
CSCwi56166	**Symptom** SSH to device fails when using the RSA-SHA2-512 and RSA-SHA2-256 host key algorithm in a key exchange. **Workaround** None

Resolved Issues 4.1.0.75

Table 3: Caveats Resolved in Release V4.1.0.75.

Bug ID	Description
CSCwi54956	**Symptom** C1300-24MGP-4X port 17 cannot forward a packet at a speed of 2.5G.
CSCwi54958	**Symptom** MAC address relearning fails when a similar entry exists in the MAC forwarding table.
CSCwi54959	**Symptom** In rare cases, the Ports 45,46,47, and 48 of the C1300-48MGP-4X cannot link up after a reboot.

What's New

This section details the new features and modifications introduced in firmware version 4.1.0.72.

- Support for the new hardware platforms:
  - New PIDs are being introduced in this release and are listed in the table below:

Device PID	Description
C1300-8MGP-2X	Catalyst 1300 Series Managed Switch, 4-port 2.5GE, 4-port GE, PoE, 2x10G SFP+
C1300-24MGP-4X	Catalyst 1300 Series Managed Switch, 8-port 2.5GE, 16-port GE, PoE, 4x10G SFP+
C1300-48MGP-4X	Catalyst 1300 Series Managed Switch, 16-port 2.5GE, 32-port GE, PoE, 4x10G SFP+
C1300-12XT-2X	Catalyst 1300 Series Managed Switch, 12-port 10GE, 2x10G SFP+
C1300-12XS	Catalyst 1300 Series Managed Switch, 12-port SFP+, 2x10GE Shared
C1300-24XT	Catalyst 1300 Series Managed Switch, 24-port 10GE, 4x10G SFP+ Shared
C1300-24XS	Catalyst 1300 Series Managed Switch, 24-port SFP+, 4x10GE Shared
C1300-16XTS	Catalyst 1300 Series Managed Switch, 8-port 10GE, 8-port SFP+
C1300-24XTS	Catalyst 1300 Series Managed Switch, 12-port 10GE, 12-port SFP+

- New software features as detailed below:
- Feature updates to existing feature as detailed below:

New Software Features

Support of 1300 stackable devices supporting 10G on all Ports

This version added supports a new subtype of the Catalyst 1300 Stackable Managed Switch Series – devices supporting10G interfaces on all ports (on top of the existing Catalyst 1300 stackable devices supporting 10G uplink ports sub-type). Device of each sub-type cannot be stacked in the same stack with devices of the other sub-type. If they are stacked together, the units of one of the sub-types will be shutdown.

Feature set of the 2 sub-types is identical besides the following items:

- The following features/abilities are supported only on the devices supporting 10G interfaces on all ports subtype:
  - Physical OOB port for management – supporting IPv4
  - IPv6 Manual Tunnel
  - Automatic 6-to-4 tunnel
  - ISATAP Routing for IPv6
- The 2 sub-types have different table sizes - mainly for features which rely on hardware resources.
- Stacking interfaces
  - On the devices supporting 10G interfaces – Up to 8 stacking interfaces are supported. Any interface can be defined as a stacking interface.
  - On the devices supporting 10G uplink ports – up to 4 stacking interfaces are supported. Only the 10G uplink interfaces can be defined as a stacking interface.

PNP Agent Support

The Plug-n-Play (PNP) Agent on switch communicates with a PNP server, which allows centralized installation of configuration and image files to the switch. This allows customer to execute Zero Touch Installs of the switch in various deployment scenarios and deployment locations. PNP operation reduces customer costs associated with deployment/installation of network devices, increases the speed and reduce the complexity of deployments without compromising the security.

Cisco Business Dashboard (CBD) Support

Cisco Business Dashboard (CBD) helps you monitor and manage your Cisco network with the use of the Cisco Business Dashboard Manager. The Cisco Business Dashboard Manager is an add-on that automatically discovers your network and allows you to configure and monitor all supported Cisco devices such as Cisco switches, routers, and wireless access points.

Cisco Business Dashboard Manager is a distributed application which is comprised of two separate components or applications: one or more Probes referred to as Cisco Business Dashboard Probe and a single Manager called Cisco Business Dashboard Manager. An instance of Cisco Business Dashboard Probe is installed at each site in the network, performs network discovery and communicates directly with each Cisco device.

Certificate Authority (CA) Certificate Manager

The Cisco Business Dashboard Probe (CBD) and Plug-n-Play (PNP) features require CA certificates to establish HTTPS communication with the CBD or PNP servers. The CA Certificate Manager feature allows these applications and device managers to do the following:

- Install trusted CA certificates and to remove certificates that are no longer wanted

- Statically add certificates to device configuration file
- Manage a revocation list of untrusted certificates

HTTPS Redirection

As part of the tightening of the system security of the switch, users accessing the management GUI should use HTTPS whenever it is supported. In order to ensure the use of HTTPS, All HTTP requests will be redirected to HTTPS if HTTPS is enabled on the device.

Port Locate (beacon)

In some cases there is a need to physically identify a single or multiple interfaces on a device, using the port LED as a physical and external (device front panel) indicator. An example for such a situation is where system administrator is in a remote location and needs to guide the onsite installer or support engineer. The Port Locate/Beacon feature addresses this issue by allowing the system administrator to activate the interface LED of one or more specified interfaces (either physical interfaces or LAGs).

This feature is only supported via the CLI.

Interface LED flashing as in indication for err-disable State

When an interface moves to the err-disable state the interface LED will flash amber to provide an indication to this state.

Support of Additional Transceivers

Support for the following SFP/SFP+ Transceivers was added in this version:

- GLC-EX-SMD
- GLC-ZX-SMD
- CWDM-SFP-1470
- CWDM-SFP-1530
- CWDM-SFP-1610
- SFP-H10GB-ACU7M
- SFP-10G-AOC2M

Changes to Existing Features

This section details important changes to features which were already supported on previous versions.

Auto Surveillance VLAN (ASV)

The following 2 changes were introduced to ASV in this version:

- When changing the ID of the ASV VLAN (CLI command “surveillance-vlan vlan-id”) a confirmation message will be displayed. User will need to confirm the change is required.
- When enabling ASV the global bridge multicast filtering setting will be automatically enabled (in addition to IGMP snooping and IGMP snooping querier which were automatically enabled in previous versions).
- On some of the SKUs ASV entries will consume TCAM entries also on ports in access mode (TCAM entries utilization can be viewed using command “show system tcam utilization”. In the previous versions ASV entries consumed entries only if the interface was in general mode.

- The CoS action for ASV classified traffic was changed to “remark”, meaning that the VPT field value in the packet will be modified to the value defined in CLI command “surveillance-vlan cos” (in previous versions the CoS action was “assign” meaning the packet is assigned to the defined CoS queue but VPT field value was not modified.



Note The remark action consumes TCAM entries. These entries are in addition to TCAM entries displayed using the command **show system tcam utilization**.

Half Duplex Support

We do not support half duplex mode on any of the ports that are 10Gig on the switches listed in the table above.

Password Complexity

A more lenient interpretation is implemented for the following requirements:

- More than 2 sequential chars or numbers are not allowed.
- Prevent Usage of Known passwords in new passwords – in this release (4.1.0.72) only the beginning of the new password is compared to the known passwords, the middle will NOT be checked, In addition, the comparison doesn’t include reverse order or replacing character as follows: "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e".

Chip Protection

Added the observed and imprinted DB hash values to the output of the “show platform hardware integrity” command.

Boot-up Time Change

Bootup time in this release (4.1.0.72) increased by about 27 seconds compared to previous release (4.0.0.94). The increase in the bootup time is due to adding support to CBD feature.

Known Issues

Caveats Acknowledged in Release V4.1.0.72.

Bug ID	Description
CSCwi00331	**Symptom** The “show dying-gasp packets” command does not display the information related to the IPv6 syslog and the SNMP servers. **Workaround** None

Bug ID	Description
CSCwi00359	**Symptom** In some cases, the stack interface LED may not light up when disconnecting and then reconnecting the stacking cable. **Workaround** None
CSCwi00366	**Symptom** The switch cannot connect to the CBD Dashboard with a static DNS entry if the DNS server configured on the device is not reachable by existing host. **Workaround** Make sure that the DNS servers are reachable or remove the DNS server configuration if static DNS entries are being used.
CSCwi00368	**Symptom** In some cases, the 1G fiber interface will fail to link up if the fiber cable is disconnected and then reconnected quickly. **Workaround** Shutdown / no shutdown on the interface or Disconnect the fiber cable together with the SFP and then re-insert.
CSCwi00373	**Symptom** Loopback detection fails when STP mode is PVST and STP is disabled. **Workaround** Change the STP mode to RSTP, and then change it back to PVST/RPVST.
CSCwi00382	**Symptom** The 'PVST Interface Settings' page on the GUI displays an inconsistency type “PVID” even though the actual inconsistency type is “Port Type” . **Workaround** The inconsistency type is displayed correctly in the "PVST Inconsistent Ports" GUI page.
CSCwi00552	**Symptom** The 'PVST Interface settings' page on the GUI displays an empty inconsistency type when the inconsistency type is “Port PVID” **Workaround** The inconsistency type is displayed correctly in the "PVST Inconsistent Ports" GUI page.

Bug ID	Description
CSCwi00728	**Symptom** The CPU utilization rate does not refresh automatically (GUI page Status and Statistics > CPU Utilization). **Workaround** Refresh the page manually.
CSCwi00748	**Symptom** “show lldp local tlvs-overloading” command output - the field “Left” (bytes for TLV) displays the number of overloaded bytes instead of the bytes still available for local TLVs. **Workaround** Calculate the number of bytes available for TLV by subtracting the value displayed in the "total” field from MTU value (1500).
CSCwi00760	**Symptom** Device console and GUI will not respond for about 3 minutes in the following scenario: • One or more DNS servers configured on device are not reachable. • In this state, the user deletes and then adds the default SNTP servers. **Workaround** Disable IPv6 on all interfaces.
CSCwi00762	**Symptom** The 1G Combo interface port LED does not flash amber when the port is in err-disable state. **Workaround** The LED on these ports will be off when interface moves to the down state. In this case, use the CLI or GUI display to check if this port is in err-disable (or is down due to disconnection or manual configuration).
CSCwi00765	**Symptom** In some cases, the “Invalid perpetual restart detected, restarting board” syslog message will appear when the board is rebooted. **Workaround** There is no effect on the device functionality – board reboot and perpetual PoE support are not effected.

Bug ID	Description
CSCwi00769	**Symptom** On a stack of 6 or more members with ring topology, some of members may always reboot if using auto unit ID and stack link is a mix of Te1-2 and Te3-4. When this issue happens, by simply rebooting the whole stack can recover it and it will not happen again in next reboot. **Workaround** Connect a stack neighbor using TE1-2 or TE3-4, but don't mix them. Or do one of the following: • use a fixed unit ID • a chain topology • reboot the stack one more time
CSCwi00776	**Symptom** The ports that are not in the VLAN of "MST instance VLAN mapping" shouldn't participate in the MST calculation for this instance **Workaround** None

Resolved Issues

Caveats Resolved in Release V4.1.0.72.

Bug ID	Description
CSCwf56969	**Symptom** C1200 C1300 - PoE issue with DBS-210.
CSCwh21119/CSCwh06683	**Symptom** 802.1x MAC based authentication fails if STP mode is set to PVST/RPVST.
CSCwh58899	**Symptom** Switches running firmware 4.0.0.93 may fail to boot up after performing "load golden image to factory reset" option on the Uboot "Basic Menu" (pressing CTRL+Shift+6 key > Basic Menu > 1. load golden image to factory reset.”
CSCwe81251	**Symptom** Welcome Banner (configured via GUI) will be erased if the user configures via the CLI, a login banner with more than 512 characters in a single line.

Bug ID	Description
CSCwe81247	**Symptom** PoE Class display in GUI (page Port Management > PoE > Setting) is wrong for a class 0 PD.
CSCwe81236	Error message is displayed when configuring the command “"no ipv6 nd hop-limit " – and configuration is not accepted.
CSCwi00805	snmp "ipNetToMediaIfIndex" ifindex value not exist in IfTable->ifEntry->ifindex.

Introduction

Release 4.0.0.93 supports the following product series:

- Catalyst 1200 Smart Switch Series
- Catalyst 1300 Managed Switch Series
- Catalyst 1300 Stackable Managed Switch Series

This release (4.0.0.93) is a maintenance release fixing bugs found in version 4.0.0.91. It does not add any new additional features to release 4.0.0.91.

This version includes an important fix. Therefore, it is highly recommend to upgrade a device running an earlier version to version 4.0.0.93.

Downgrade from version 4.0.0.93 to previous versions is blocked.

Due to the downgrade prevention implemented in version 4.0.0.93, both active and inactive images are upgraded when upgrading from a prior version.

Caution Due to downgrade prevention applied to version 4.0.0.93 - adding a unit running version 4.0.0.93 to a stack running an earlier version will cause the new unit to shutdown due to version incompatibility.

To resolve this issue, disconnect the unit running 4.0.0.93 from the stack and reload it. Next, upgrade the existing stack to version 4.0.0.93, and then add the new unit to the stack.

Therefore, before adding a new unit, it is advised to upgrade the current stack to version 4.0.0.93 in order to prevent this behavior.

What's New in this Release

This section details new features and modifications in this release.

Release 4.0.0.93 does not support any additional features or functionalities above release 4.0.0.91 in any capacity.

Known Issues

Caveats Acknowledged in Release V4.0.0.93.

Bug ID	Description
CSCwh21119	**Symptom** MAC authentication fails when PVST command is added. **Workaround** Use STP mode other than PVST/RPVST.
CSCwh58899	**Symptom** C1200/1300 switches running firmware 4.0.0.93 may fail to boot up after performing "load golden image to factory reset" option on the Uboot "Basic Menu" (pressing **CTRL+Shift+6 key > Basic Menu > 1. load golden image to factory reset**). **Note** The issue has little impact on users as the “Load golden image to factory reset” option is rarely used. To reset switch configuration to factory default, it can be set using the reset button or CLI or GUI or start up menu. Will be fixed in 4.1.0.x **Workaround** Contact Cisco support for assistance if the switch reaches this state after using “Load golden image to factory reset” option to reset the switch. **Recommended Action:** Avoid using the “Load golden image to factory reset” option to factory reset the switch while the switch is on firmware version 4.0.0.93.

Resolved Issues

Caveats Resolved in Release V4.0.0.93.

Bug ID	Description
CSCwh02042	**Symptom** With an extremely low probability (1/4096) the boot process may hang and the error message “hw error” will be printed to the console.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.0.0.91

August 2023

This Release Note describes the recommended practices and known issues that apply to software version 4.0.0.91 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications in this release.

Changes to Hardware Components

Reset Button Functionality

The reset button function has been updated as follows:

- System LED provides different flash indication for regular device reload and reset to factory default:
  - Regular device reload (the reset button is pressed and then released within 6-10 seconds) – the system LED will provide an indication of a slow flash.
  - Resetting device to factory default (the reset button is pressed and then released within 16-20 seconds) – the system LED will provide an indication of a rapid flash.
- Pressing the system LED and releasing within 1-2 seconds on SKUs that support PoE will provide the following indication:
  - On ports that are delivering power to connected PDs – the port LED will provide a solid amber indication for 5 seconds.
  - On ports that are not delivering power to connected PDs – the port LED will not provide any indication for 5 seconds (LED will be off).

Type-C USB Interface

The device supports a type-C USB Interface located on device front panel. This provides an additional console interface besides the RJ45 interface. The type-C USB based console has the following characteristics:

- The console is active only from OS init stage and on.
- When active, the Type C USB consoled had priority over the RJ45 console.
- The type-C USB console is agnostic to baud rate setting.

Trusted Platform Module (TPM) Support

All SKUs support a TPM component. The TPM provides hardware level protection and operation for security related features such as Chip guard and Boot Integrity Visibility. The device support TPM 2.0 specification.

Bluetooth Management Interface

The current version added support for a Bluetooth Management Interface – providing IP connectivity over Bluetooth. This device management over Bluetooth via telnet, SSH or HTTP/HTTPS GUI interface.

Support of Bluetooth is achieved by connecting a Bluetooth (BT) dongle, to the device USB port. The device will automatically detect the insertion of a supported BT dongle into device's USB port and provide Bluetooth host support. The device supports the following Bluetooth Dongles.

1. BTD-400 Bluetooth 4.0 Adapter by Kinivo
2. Bluetooth 4.0 USB Adapter by Asus

3. Bluetooth 4.0 USB Adapter by Insignia
4. Philips 4.0 Bluetooth adapter
5. Lenovo LX1815 Bluetooth 5.0 USB adapter
6. Lenovo LX1812 Bluetooth 4.0 USB adapter

Persistent PoE

The Persistent PoE feature (also referred to as Always-On PoE) minimizes the dependency of the PoE operation on the switch's status. Before the introduction of this feature, any disruption in the switch operation such as a software related reboot, would also cause a disruption in the PoE operation until the device finished coming back up. With the persistent PoE feature warm reboots such as the ones performed by the reload command will not disrupt the operation of the PoE in it's current state, allowing PDs connected to the switch to continue and operate.

Auto Surveillance VLAN (ASV)

Network communication between surveillance devices such as cameras and monitoring equipment should often be given higher priority and it is important that the various devices that comprise the surveillance infrastructure in the organization are reachable for each-other.

Normally, it falls to the network administrator to ensure that all surveillance devices are connected to the same VLAN and to setup this VLAN and the interfaces on it to allow for this high priority traffic.

The Auto Surveillance VLAN (ASV) feature automates aspects of this setup by detecting surveillance devices on the network, assigning them to a VLAN and setting their traffic priority.

MSTP Enhancements

The following MSTP related enhancements were added to this release:

- Catalyst 1300 product line supports 16 instances.
- MSTP instance ID can be in the range of 0-4094.

To allow support the range of 0-4094 for MSTP instance ID the user is required to create an MSTP instance– and assign it an instance ID. Once Instance ID is created the user can map VLANs to the created instances (in previous releases there was no need to create the instance prior to mapping VLANs to the instance.

Password Aging Enhancements

Password aging allows the administrator to force a change of a password after a predefined period. The current version added the following enhancements:

- Only a level 15 user can change passwords. A Level 1 user is presented with notice on (expected) password expiration but does not have the privilege to change the password.
- Expiration period (10 days prior to password expiration) – Upon login the (level 15) user will be presented with the option to change the password. The user can refuse the option – in which case login will be provide, or accept suggestion, in which case they will be able to change the password immediately (in previous version user would need to log in and then enter relevant configuration mode).

Attestation Certificate and Key-pair (AIK) Support

The certificate and key pair are used to validate various device information as well as signing the output of commands displaying security related information (for example Chip Guard and Boot integrity Visibility).

The current version added support for an additional certificate and key pair. This is the Attestation certificate and key pair (also known as AIK - Attestation Identity Key). The attestation certificate and keys are considered more secure than the SUDI certificate and keys, as operation using the AIK certificate is confined within the TPM. this provides a higher confidence in the validity of signed information.

Boot Integrity Visibility (BIV)

Boot integrity Visibility (BIV) feature allows a platform's software integrity information to be visible and actionable. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted and is running a trusted code. BIV on the Catalyst 1200 and 1300 product line utilizes the functionalities of the TPM component.

During the boot process, the software creates a hash record of the different images involved in the boot stages. To ensure integrity of the measurements, the measurements are stored in a hardware protected component called TPM and extended into PCRs (Platform Configuration Register). The user can then retrieve these records (via CLI commands) and compare it with Known Good Values (KGV) records maintained by Cisco. If the values do not match, the device may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

The CLI commands allow to display the hash measurements and PCR quote for the bootloader and entire image. Optionally this information can also be signed using SUDI or attestation Keys.



Note The BIV feature works without user intervention or accepting any changes out of the box, but if end-user requires confirmation of this, an option will be provided soon to help users.

Chip Guard Enhancements

The current version added the following enhancements:

- Support of CLI command to display Chip guard information.
- Support of attestation certificate and keys for signing command output.

Random Token for Debug Access

- Certain debug interfaces (for example Linux shell) are sensitive or may cause disruption to device operation, and therefore require elevated access control and verification.
- The current version supports the enhanced requirement by generating a random challenge upon each attempt to access such debug interfaces, followed by a prompt to provide a password based on the challenge.
- In order to access the interface the challenge needs to be signed by a dedicated key managed by Cisco.

Dying Gasp

The Dying Gasp feature provides a mechanism to alert monitoring systems that a device is experiencing an unexpected loss of power due to HW failure (disconnection or disruption of power source).

When a loss of power event occurs, a hardware capacitor will delay the device shutting down for a short time. During this time, the device will send Dying Gasp messages. The messages can be sent to SNMP servers (as notification) or to syslog servers.

This feature is supported only on the 1300 product lines (standalone and stacking). It is not supported on the 1200 product line.

Golden Image Support

- The current version added Golden Image support.
- The Golden Image is a production level image, and as such underwent extensive testing cycles.
- In case the current software is corrupted and will not load – the device will automatically load the Golden Image as a fallback image. This may prevent the need to RMA such a unit. Loading the golden image may result in erase of device configuration.
- The Golden Image is burned to device flash as part of the manufacturing process. The user does not have an option update the Golden Image version. In some cases (for example secure boot key revocation) the Golden Image will be updated as part of the regular image update.

CLI Command to Reset Device to Factory Defaults

CLI commands provide the ability to not only reboot the switch but to also reset the switch back to factory defaults. For more information, please refer to the CLI Guide for detailed commends in the standalone and stackable switches.

SSL and SSH Support

The following changes were introduced in the current release:

- TLS 1.2 secure client-initiated renegotiation is disabled.
- Supported OpenSSL version – 1.1.1q
- Supported OpenSSH version - Version 7.3p1 (no change to previous version)

Known Issues

Caveats Acknowledged in Release V4.0.0.91.

Bug ID	Description
CSCwe81236	**Symptom** Error message is displayed when configuring command “"no ipv6 nd hop-limit " – and configuration is not accepted. **Workaround** Disabled IPv6 on interface.
CSCwe81238	**Symptom** Auto surveillance vlan (ASV) will not be active on general mode port if STP mode is set to PVST/RPVST. **Workaround** To activate ASV on the interface either disable and then re-enable the ASV VLAN or change STP mode to STP/RSTP and then change back to PVST/RPVST.

Bug ID	Description
CSCwe81247	**Symptom** When a port is set to class mode, the PoE Class display in the GUI (**Port Management > PoE > Setting**) is wrong for a class 0 PD. **Workaround** Check class info via the CLI.
CSCwe81251	**Symptom** Welcome Banner (configured via the GUI) will be erased if the user configures via the CLI with a login banner with more than 512 characters in a single line **Workaround** None
CSCwe81253	**Symptom** When the authentication or login default method list is updated, the Syslog messages are duplicated. **Workaround** None
CSCwe81254	**Symptom** An error message will appear on the console if the DHCP pool name includes special characters (for example single quote, double quote, backslash) and the user clicks the "**Details**" button in **IPv4 Configuration> DHCP Server>Network Pools** GUI page. **Workaround** There is no functionality effect and workaround.
CSCwe84307	**Symptom** C1200/C1300 - PoE port fault status when non PoE device connected **Workaround** Disable the port PoE by applying **power inline never** command to the PoE interface.
CSCwf56969	**Symptom** C1200 C1300 - PoE issue with DBS-210 **Workaround** No workaround
CSCwe81260	**Symptom** Pre-standard PD cannot exit power denied state caused by POE budget shortage. **Workaround** Disable then enable the POE on the problem port.

Bug ID	Description
CSCwe81261	**Symptom** Sometimes the POE ports cannot recover from overload state even after a decrease of the load to normal. **Workaround** Disable then enable the POE on the problem port.

© 2026 Cisco Systems, Inc. All rights reserved.