Release Notes For Cisco Business 250 - 350 Series Switches, Firmware Version, 3.3.0.16

Introduction

May 2023

This Release Note describes the recommended practices and known issues that apply to software version 3.3.0.16 for the Cisco Business 250 and 350 Series Switches.

Warning Please read the Readme note before installing the firmware upgrade. If upgrading from any firmware below 3.2.0.84 to 3.2.0.84 or greater, note that the firmware upgrade process may take approximately 15 minutes to complete. During this time, the switch may not show any activity. As part of the upgrade process, switch may reboot couple of times. Interrupting the upgrade process may result in permanent damage to the switch and make it unusable.

Note Some of the CBS features require the platform to support the ACT2 chip (See section below). The Appendix will also provide information on the platforms that support the ACT2 chip.

Downgrade Restrictions Disclosure

Downgrading is the process of installing a lower firmware version to a device from a higher firmware version. Except as indicated in Device Lists in the Appendix, downgrading a firmware is available to all CBS products from any higher firmware down to a lower version.

Please keep in mind that we recommend that customers should run the most recent firmware unless there is a compelling reason to do otherwise. Even so, we recommend using it only temporarily while working on a problem.

Our latest release as of April 2023 is 3.3.0.16

These restrictions and notes may be amended if circumstances warrant.

General Note – Downgrading to version 3.1.1.7 or Lower Version

When attempting to downgrade from Version 3.2.0.84 (or later) to version 3.1.1.7 or lower, the device startup configuration will be deleted as part of the downgrade operation. User will be alerted to this behavior when attempting to boot from an image lower than Version 3.2.0.84. It is highly recommended to backup device configuration file before performing the downgrade and load the saved configuration file to device after downgrade was completed.

Hardware Dependent Features

This section will detail features introduced in release 3.2.0.84, and that require the device to include the ACT2 chip. The ACT2 is supported only in the platforms listed in the table in the Appendix and according to the Hardware VID indicated in the notes to the table.

What's New in Release 3.3.0.16

This section details new features and modifications in this release compare to previous ones.

CBD Probe Version

Cisco Business Dashboard (CBD) Probe version was upgraded in this release to version 2.6.0.20230314 (upgraded from version 2.4.1.20220225 supported in CBS release 3.2.x.x. This CBD version includes bug fixes and the new functionalities detailed in the next items:

CBD - Organization and Network Name Parameters

Up until CBS release 3.2.x.x (inclusive) the user was required to define the following 2 parameters in order to allow the connection to the Dashboard:

- CBD Organization Name
- CBD Network Name

The above two parameters are no longer required as of CBS version 3.3.x.x and are thus removed from the device CLI and the graphical user interface (GUI).

If the user upgrades from a CBS version 3.2.x.x (or earlier) to version 3.3.x.x (or higher) the above 2 parameters will be removed from the configuration file.

Note This section is relevant both to manual “traditional” connection to Dashboard and connection using the CBD Wizard (See following section).

CBD Wizard

Up until CBS release 3.2.x.x (inclusive) prior to connecting the device to the Dashboard, the user was required to do the following:

- Pre-register the device with the CBD services (including device PID and SN).
- Install a root CA certificate on the switch.
- Configure on the device an Access Key ID and secret.

In CBS release 3.3, the user has an option to manually perform the above, or to use a CBD Wizard to simplify the connection and registration to the CBD server. The CBD Wizard is supported only via GUI.

Connection steps, using the wizard are as follows:

- Navigate to the following page: **Administration > Cisco Business Dashboard Settings**.
- Enable the Dashboard Connection and configure the address (IP/host) and port of the Dashboard.
- Select **Online with Web Browser** to use the Wizard to configure the connection to the Dashboard.

- Once process is completed and approve by the user, the Dashboard updates the switch with the relevant CA root certificate and CBD access key.

Resolved Issues

Table 1: Caveats Resolved in Release V3.3.0.16

Number	Description
CSCwd60295	**Symptom** Incorrect STP output may be visible if STP is disabled and mode is set to PVST or RPVST.
CSCwe64339	**Symptom** Management ACL generates errors for inbuilt Probe.
CSCwe64160	**Symptom** FATAL error when enable MSTP and show spanning-tree detail on a stack.
CSCwd59624	**Symptom** The command "display macro auto ports" needs the line "SmartPort is enabled" removed.
CSCwe32312	**Symptom** Cisco Small Business Series Switches Buffer Overflow Vulnerabilities
CSCwe32313	**Symptom** Cisco Small Business Series Switches Unauthenticated Heap Buffer Overflow
CSCwe32315	**Symptom** Cisco Small Business Series Switches Buffer Overflow Vulnerabilities
CSCwe32318	**Symptom** Cisco Small Business Series Switches Unauthenticated Denial-of-Service
CSCwe32321	**Symptom** Cisco Small Business Series Switches Buffer Overflow Vulnerabilities
CSCwe32323	**Symptom** Cisco Small Business Series Switches Stack Buffer Overflow
CSCwe32326	**Symptom** Cisco Small Business Series Switches Unauthenticated BSS Buffer Overflow
CSCwe32334	**Symptom** Cisco Small Business Series Switches Unauthenticated Stack Buffer Overflow
CSCwe32338	**Symptom** Cisco Small Business Series Switches Unauthenticated Configuration Reading

Known Issues

Table 2: Caveats Acknowledged in Release V3.3.0.16

Bug ID	Description
CSCwe76469	**Symptom** The CBD probe does not respond when the HTTPs port is changed. **Workaround** After changing the HTTPs port, disable and then re-enable the CBD probe, or reset the CBD probe using the CLI command "cbd reset" or the WEB GUI button "Reset Connection."
CSCwe76605	**Symptom** On the CBD settings page, the plaintext input box for the Access Key Secret is grayed out. **Workaround** Click the plaintext box, then move to encrypted, then back to plaintext.
CSCwe87662	**Symptom** Fails to launch the CBD connect wizard on a standalone device with unit ID 2 **Workaround** Configure as unit 1.
CSCwe87686	**Symptom** Sometimes the command “clear ipv6 neighbor binding table” may cause unexpected log messages on the console. **Workaround** None

Firmware 3.2.xx Release

March 2023

This Release Note describes the recommended practices and known issues that apply to software version 3.2.x.x for the Cisco Business 250 and 350 Series Switches.

Warning Please read the Readme note before installing the firmware upgrade. Note that the firmware upgrade process may take approximately 15 minutes to complete. During this time, the switch may not show any activity. As part of the upgrade process, switch may reboot couple of times. Interrupting the upgrade process may result in permanent damage to the switch and make it unusable.

Resolved Issues

Table 3: Caveats Resolved in Release V3.2.1.1

Number	Description
CSCwe52939	**Symptom** Sometimes a specific SFP（GLC-SX-MM-RGD can cause I2C bus read issue, therefore it can damage the device during boot up. This issue impacts the 24 ports Gigabits CBS250/350 switches with HW version 03 or 05.

Resolved Issues

Table 4: Caveats Resolved in Release V3.2.0.89

Number	Description
CSCwd29685	**Symptom** Display specific startup configure file causes fatal error - %SYSLOG-F-OSFATAL: caught segmentation fault exception at address 0xfffe947e9000
CSCwc68648	**Symptom** ARP issue in Rapid PVST mode.
CSCwc31999	**Symptom** CBS350-48P-4X-EU - SSH session will not time out
CSCwc32010	**Symptom** Failed to manage device via console, SSH and GUI after a while.
CSCwa69564	**Symptom** On the CBS350, the access control list entries (ACEs) created in GUI cannot be removed via CLI.

Resolved Issues

Table 5: Caveats Resolved in Release V3.2.0.84

Number	Description
CSCvx89372	**Symptom** Help text was “"Destination/Source MAC Wildcard Mask" which did not provide info on the field format. The help text was changed to “See Online Help for format”.
CSCwc39418	**Symptom** Alert Icon continues to blink even though it was disabled by user.

Number	Description
CSCvw65642	**Symptom** In some cases when setting a session timeout via GUI it is not saved to startup configuration and is not applied after reboot.
CSCwa91538	**Symptom** In some cases when removing and then re-applying ACL to VLAN interface, operation may fail with message related to hardware resources, and backup unit may reboot.
CSCvz42028	**Symptom** In some cases, in PVST mode the output from command "show spanning-tree active vlan <#>" may show access ports that do not belong to the specified VLAN.
CSCwc39424	**Symptom** After about 2 hours SNTP stops polling SNTP servers which were configured by hostname.
CSCwc39428	**Symptom** Wrong LDP MAC-PHY TLV value for 2.5 and 10G interfaces.
CSCwc39431	**Symptom** Following a stack switchover to a Standby unit, the Probe does not automatically reconnect to CBD Dashboard.
CSCvu81808	**Symptom** In some cases, an ACE will be deleted if edited via GUI.
CSCwc39432	**Symptom** Auto negotiation of MAC/PHY configuration/Status TLV indicates disable although interface is set to auto- negotiation
CSCwc39434	**Symptom** After importing a CA certificate with "tab" characters through the GUI, the "signer" CA will be displayed twice.
CSCwc39437	**Symptom** PoE settings and statistics page display on the GUI is very slow.
CSCwc39514	**Symptom** When switching a DHCPv6 client from a VLAN interface to a physical interface, the device may crash in some cases.
CSCwc39515	**Symptom** Command renew dhcp oob fails if previously the OOB interface declined an address due to conflict with default IP on VLAN 1.

Number	Description
CSCwc39531	**Symptom** Login via CBD mobile app fails if device credentials are added/changed via GUI.
CSCwb57285	**Symptom** A Class0-4 PoE PD with low priority and no LLDP negotiated may reboot when a Class4 PD is plugged in.
CSCvz97713	**Symptom** CBS250-8P-E-2G - The link flaps and "denied counter" increments in PoE .

Known Issues

Table 6: Caveats Acknowledged in Release V3.2.0.84

Bug ID	Description
CSCwc39517	**Symptom** After a brief power outage, the switch may occasionally fail to respond. CBS350-24XTS is the only SKU with this symptom. **Workaround** None
CSCwc39527	**Symptom** On some platforms legacy PoE PDs are detected as 802.3AT instead of 802.3AF. **Workaround** None
CSCwc39529	**Symptom** Sometimes I2C related messages are generated when inserting SFP GLC-BX, GLC-BX-D or MGBLX1-V2-1G transceivers. **Workaround** There are no functionality issue, SFP will be initialized in few seconds.
CSCwc44155	**Symptom** Backup Dashboard data to USB before enabling CBD, as "File operations" on the web page become invalid. **Workaround** The functionality of the WEB page "File operations" cannot be restored, however the relevant CLI capabilities continue to function.

Bug ID	Description
CSCwc39519	**Symptom** Login Attack prevention- the failed login attempt count, time period and quite mode are reset when an active unit switchover occurs. **Workaround** None.
CSCwc39521	**Symptom** When setting VLAN1 to static IP address 192.168.1.254 and quickly pinging other device the ping fails **Workaround** Manually configure IP address instead of copying paste the IP configure commands.
CSCwc39522	Unable to access device GUI management if device software is downgraded from 3.2.0.x to 3.1.1.7 or lower version – unless user removes browser cookies. **Workaround** Remove browser cookies before connecting to a device.
CSCwc39527	**Symptom** On some platforms legacy PoE PDs are detected as 802.3AT instead of 802.3AF **Workaround** None.
CSCwc39529	**Symptom** I2C related messages are generated when inserting SFP GLC-BX, GLC-BX-D or MGBLX1-V2-1G transceivers. **Workaround** There are no functionality issue, However it is suggested to check the transceiver status using the show inventory and show interface status commands.
CSCwc39530	**Symptom** Certificate revocation configuration is missing from configuration file after upgrading from an earlier version to version 3.1.1.7 **Workaround** None

Firmware 3.1.1.7 Release

September 2021

This Release Note describes the recommended practices and known issues that apply to software version 3.1.1.7 for the Cisco Business 250 and 350 Series Switches.

What is New in Release 3.1.1.7

This section details new features and modifications in this release compare to previous one.

1.1 Default IP Settings on Devices that Support OOB

On previous versions, the default management interface, on devices that support OOB in native mode, was applied to the OOB port and not on the default VLAN. In Hybrid mode default IP management interface is applied to VLAN 1 and OOB is disabled. From this version and on, the default management interface is applied to VLAN 1, even on devices in native mode that support OOB. The OOB interface, in new behavior, will be DCHP enabled by default in native mode, and will not support the default IP settings. In Hybrid mode OOB will be disabled, as in previous version.

The following table summarizes VLAN 1 and OOB default IP setting before and after the change applied in version 3.1.1.7

	Cisco Business firmware up to version 3.1		**Cisco Business firmware version 3.1.1.7**	
	OOB interface	VLAN 1 interface	OOB interface	VLAN 1 interface
IP settinngs	Default IP + DHCP		DHCP enable	Default IP + DHCP
Interface CLI configuration	None	None	"IP address dhcp"	None
Other	Bonjour enabled	None	None	Bonjour enabled

Note When upgrading or downgrading between previous and current version the intention is to keep existing configuration unless device is set to factory default. Please note configuration before and after upgrade/downgrade operation and verify configuration.

Note Refrain from changing stacking mode when upgrading to new version. The new settings may be different then expected. If a change of mode is needed, first change the mode and then upgrade the stack.

1.2 Updated Cisco Trusted Core Bundle

The 3.1.1.7 firmware uses the Cisco core bundle.

1.3 New PoE Driver

New PoE driver version 0.2.0.17.

Resolved Issues

Table 7: Caveats Resolved in Release V3.1.1.7

Number	Description
CSCvy74466	**Symptom** Cannot access device privilege exec mode using enable password.
CSCvw29853	**Symptom** Device may reboot if connected Polycom phones send LLDP info.
CSCvw28120	**Symptom** Device may reboot if connected NEC DT800 phones send LLDP info.
CSCvy66085	**Symptom** Ongoing syslog messages related to FDB hash collision flood interfere with console usage.
CSCvz45993	**Symptom** Device GUI cannot load if any interface description includes the word “form”.
CSCvz46007	**Symptom** Device will reboot if clicking on OLH general information sub items.
CSCvz59935	**Symptom** Fiber link between SG350X-48MP and CBS350-48XT-4 flaps and then suspended
CSCvw84846	**Symptom** After awhile, the PoE will stop the power supply on some interfaces.
CSCvw86418	**Symptom** CBD Probe cannot connect if the name of the CA certificate configured on devices includes a space in the certificate name (for example “my cert”).
CSCvz46020	**Symptom** Device reloads after setting IPv6 tunnel as route destination.

Known Issues

Table 8: Caveats Acknowledged in Release V3.1.1.7

Bug ID	Description
CSCvz58788	**Symptom** Certificate revocation configuration is missing from configuration file after upgrading from an earlier version to version 3.1.1.7. **Workaround** None.
CSCvz62516	CBD probe and mobile app fail to connect device with updated password after modify user password via device web gui. If modify user password via CLI or CBD probe, there is no problem. **Workaround** Log out the device web gui then log in with new password.
CSCvz64701	CBS350-48P-4G: Port may power cycle when both wireless access point and phone are connected. **Workaround** None.
CSCvz67634	CBS350-24P-4X: PoE not resetting properly and leading to PD devices losing power and flap) **Workaround** None.

Release Notes for Cisco Business 250 and 350 Series Switches - Software Version 3.1.0.57

February 2021

This Release Note describes the recommended practices and known issues that apply to software version 3.1.0.57 for the Cisco Business 250 and 350 Series Switches.

Whats New in Release 3.1.0.57

1.1 Enhancements

The following list introduces the changes and enhancements featured in this release.

- RIPv2 support on CBS350 SKUs
- CA certificates are valid only if system clock was set by user, RTC or SNTP.

- Hybrid stack support was added to CBS350 stacking SKUs
- Naming of stacking unit roles was changed to Active Unit, Standby Unit and Member Unit
- CBD Probe version 2.2.1.x

Resolved Issues

Table 9: Caveats Resolved in Release V3.1.0.57

Number	Description
CSCvs26294	**Symptom** Port security supporting shutdown action for MACs that are secured on other interfaces.
CSCvx48537	**Symptom** SNMPv3 security improved by deprecating md5 authentication method and DES encryption method and replacing them with SHA-2 authentication and AES-128 as encryption method.
CSCvx48588	**Symptom** Changed default settings of voice VLAN and autosmart port to disable.
CSCvx48591	**Symptom** Added Built-in Bundle support for PNP agent.
CSCvx48594	**Symptom** Added PNP server Certificate CN/SAN validation to enhance security.
CSCuu65557	**Symptom** If the management session is using the device's IPv6 address, and this is asecure session (HTTPS), the device cannot be managed using the Safari browser.
CSCvu81809	**Symptom** Apply/Remove acl to/from port-channel and its member port cause traffic interrupt.
CSCvu81810	**Symptom** Fail to associate time-range with mac acl via GUI.
CSCvu81807	**Symptom** After set permit ip source 10.10.10.1 service telnet gi1, Show management access-list Telnet_Only then it will not display port.

Known Issues

Table 10: Caveats Acknowledged in Release V3.1.0.57

Number	Description
CSCvx44260	**Symptom** Connection to PNP server fails if PNP server address is configured as IPv6 Link Local address. **Workaround** Use Global IPv6 address or IPv4 address.
CSCvx44267	**Symptom** 100Mbps Half duplex cannot be configured on OOB port. **Workaround** Use different speed settings to connect to OOB.
CSCvx44269	**Symptom** On some Mgig interfaces when no cable is connected, or cable length is very short (shorter than 3 meters), running Cable test (VCT) may provide unpredictable results. **Workaround** None.
CSCvx44271	**Symptom** Alert Icon continues to blink even though alert Icon Blinking was disabled by user. **Workaround** None.
CSCvx44276	**Symptom** On XG uplink interfaces of certain devices Egress traffic shaping(CIR) with a value less than 18M, may shape traffic to less than set value. **Workaround** None.

Release Notes for Cisco Business 250 and 350 Series Switches - Software Version 3.0.0.69

September 2020

This Release Note describes the recommended practices and known issues that apply to software version 3.0.0.69 for the Cisco Business 250 and 350 Series Switches that include the following models:

Model	Product Label
CBS250-8T-E-2G	8-Port Gigabit Smart Switch
CBS250-8PP-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-8P-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-8FP-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-16T-2G	16-Port Gigabit Smart Switch
CBS250-16P-2G	16-Port Gigabit PoE Smart Switch
CBS250-24T-4G	24-Port Gigabit Smart Switch
CBS250-24PP-4G	24-Port Gigabit PoE Smart Switch
CBS250-24P-4G	24-Port Gigabit PoE Smart Switch
CBS250-24FP-4G	24-Port Gigabit PoE Smart Switch
CBS250-48T-4G	48-Port Gigabit Smart Switch
CBS250-48PP-4G	48-Port Gigabit PoE Smart Switch
CBS250-48P-4G	48-Port Gigabit PoE Smart Switch
CBS250-24T-4X	24-Port Gigabit Smart Switch with 10G Uplinks
CBS250-24P-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS250-24FP-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS250-48T-4X	48-Port Gigabit Smart Switch with 10G Uplinks
CBS250-48P-4X	48-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS350-8T-E-2G	8-Port Gigabit Managed Switch
CBS350-8P-2G	8-Port Gigabit PoE Managed Switch
CBS350-8P-E-2G	8-Port Gigabit PoE Managed Switch
CBS350-8FP-2G	8-Port Gigabit PoE Managed Switch
CBS350-8FP-E-2G	8-Port Gigabit PoE Managed Switch
CBS350-16T-2G	16-Port Gigabit Managed Switch
CBS350-16T-E-2G	16-Port Gigabit Managed Switch
CBS350-16P-2G	16-Port Gigabit PoE Managed Switch
CBS350-16P-E-2G	16-Port Gigabit PoE Managed Switch
CBS350-16FP-2G	16-Port Gigabit PoE Managed Switch

Model	Product Label
CBS350-24T-4G	24-Port Gigabit PoE Managed Switch
CBS350-24P-4G	24-Port Gigabit PoE Managed Switch
CBS350-24FP-4G	24-Port Gigabit PoE Managed Switch
CBS350-48T-4G	48-Port Gigabit Managed Switch
CBS350-48P-4G	48-Port Gigabit PoE Managed Switch
CBS350-48FP-4G	48-Port Gigabit PoE Managed Switch
CBS350-24T-4X	24-Port Gigabit Stackable Managed Switch with 10G Uplinks
CBS350-24P-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-24FP-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-48T-4X	48-Port Gigabit Stackable Managed Switch with 10G Uplinks
CBS350-48P-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-48FP-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks

What's New in This Release

1.1 Browser and OS Support

The device web UI supports the following browsers and OS system:

- Supported OS – MS Windows 7 (32 & 64 bit), MS Windows 10 (32 & 64 bit), MAC OS (not supported: MS Windows 8, 8.1, XP and Vista; Linux)
- Supported Browsers – Chrome, Firefox and Microsoft Edge (Microsoft Internet Explorer not supported) – both for Windows and for MAC OS; Safari – MAC OS only .

1.2 Web GUI Style

The CBS 3.0 uses a new GUI style which is the PISA compliant.

1.3 Password Complexity

For enhanced security, the user does not have the option to disable the password complexity setting. The password complexity is supported with the following default and ranges:

- Min-length – range 8-64, default = 8
- Min-class – range 1-4, default = 3
- No-repeat – range 1-16, default = 3
- Not-current/not-username/not manufacturer = are always enabled

1.4 SSL Cipher Support

For enhanced security, support for the following Ciphers was removed:

- RSA_WITH_AES_128_CBC_SHA256;
- RSA_WITH_AES_128_GCM_SHA256;
- RSA_WITH_AES_128_CCM_8;
- RSA_WITH_AES_256_CCM_8

1.5 SSL Cipher Support

OpenSSL version upgraded from 1.1.0b to 1.1.0l (Lower case L).

1.6 Console Support

Both RJ45 and mini-USB console are supported on CBS350 and CBS250 switch models listed in this release note. The mini-USB has precedence.

1.7 Password Encryption

In the previous version, the user's credentials were saved to the config file and displayed using SHA-1 hash algorithm. In the current release, the user's credentials are salted and hashed using PBKDF2 based on HMAC-SHA-512 hash. This adds additional security to the credentials and protects them from various attacks.

Relevant credentials:

- Local database password
- Enable password
- Line password

1.8 Self-Signed Certificate Lifetime

To enhance security, the default and supported validity of the device self signed certificate are changed:

- Validity Range: 30 days to 1095 days (i.e. 3 years); was 30 days to 10 years
- Default = 730 days (i.e 2 years); was 1 year

1.9 Real Time Clock

SKUs in this release support have an internal self-sufficient Real Time Clock (RTC) component that keeps time even when the device is shut down and not connected to a power source. This internal clock is initialized during manufacturing and can be updated by the time features of the device when the software clock is set (for example manually or via SNTP).

In a stack configuration – all units will sync with the master unit RTC. For more details on stack behavior see functional spec. Note: future releases of CBS may contain SKUs that do not support RTC – in this case a different unit (not the master) will be used as the system time source.

RTC is considered "reliable" for features that require a "reliable" time source: Time range settings; updating IP DHCP Snooping Database and scheduled reboot.

1.10 PNP Agent Enhancements

CBS 3.0 supports the configuration of HTTPS as 1st choice" transport protocol. Tesla 2.5.5 supported only HTTP as 1st choice transport protocol.

1.11 Stack Unit ID Indication

The stacking SKUs in this release do not support dedicated stacking LED(s). Therefore the system LED is used on these units to indicate stack unit ID, as follows:

- Active unit – system LED will remain solid green (unless device is in bootup phase, or there is a HW fault or device is not connected to the power)
- For member units - following completion of bootup phase and connection to the master unit, every 20 seconds the System LED will blink green according to unit ID of the member unit:
  - Unit 1 (if not active) – system LED will blink 1 time;
  - Unit 2 (if not active) – system LED will blink 2 times;
- Unit 3 – system LED will blink 3 times;
- Unit 4 – system LED will blink 4 times;

Note Note: SKUs added in following releases may support dedicated stacking LEDs.

1.12 Online Help (OLH) and Language File

Version 3.0.0.69 includes multiple fixes to OLH files. It also supports Chinese and Japanese language files.

1.13 CBD Probe Version 2.2.0.20200801

In version 3.0.0.69 the CBD Probe was upgraded to version 2.2.0.20200801.

Resolved Issues

Table 11: Caveats Resolved in Release V3.0.0.69

Number	Description
CSCvv70507	**Symptom** In some rare cases, device active image is corrupted after reboot and will not load properly.

Release Notes for Cisco Business 250 and 350 Series Switches - Software Version 3.0.0.61

August 2020

This Release Note describes the recommended practices and known issues that apply to software version 3.0.0.61 for the Cisco Business 250 and 350 Series Switches that include the following models:

Model	Product Label
CBS250-8T-E-2G	8-Port Gigabit Smart Switch
CBS250-8PP-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-8P-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-8FP-E-2G	8-Port Gigabit PoE Smart Switch
CBS250-16T-2G	16-Port Gigabit Smart Switch
CBS250-16P-2G	16-Port Gigabit PoE Smart Switch
CBS250-24T-4G	24-Port Gigabit Smart Switch
CBS250-24PP-4G	24-Port Gigabit PoE Smart Switch
CBS250-24P-4G	24-Port Gigabit PoE Smart Switch
CBS250-24FP-4G	24-Port Gigabit PoE Smart Switch
CBS250-48T-4G	48-Port Gigabit Smart Switch
CBS250-48PP-4G	48-Port Gigabit PoE Smart Switch
CBS250-48P-4G	48-Port Gigabit PoE Smart Switch
CBS250-24T-4X	24-Port Gigabit Smart Switch with 10G Uplinks
CBS250-24P-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS250-24FP-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS250-48T-4X	48-Port Gigabit Smart Switch with 10G Uplinks
CBS250-48P-4X	48-Port Gigabit PoE Smart Switch with 10G Uplinks
CBS350-8T-E-2G	8-Port Gigabit Managed Switch
CBS350-8P-2G	8-Port Gigabit PoE Managed Switch
CBS350-8P-E-2G	8-Port Gigabit PoE Managed Switch
CBS350-8FP-2G	8-Port Gigabit PoE Managed Switch
CBS350-8FP-E-2G	8-Port Gigabit PoE Managed Switch
CBS350-16T-2G	16-Port Gigabit Managed Switch
CBS350-16T-E-2G	16-Port Gigabit Managed Switch
CBS350-16P-2G	16-Port Gigabit PoE Managed Switch

Model	Product Label
CBS350-16P-E-2G	16-Port Gigabit PoE Managed Switch
CBS350-16FP-2G	16-Port Gigabit PoE Managed Switch
CBS350-24T-4G	24-Port Gigabit PoE Managed Switch
CBS350-24P-4G	24-Port Gigabit PoE Managed Switch
CBS350-24FP-4G	24-Port Gigabit PoE Managed Switch
CBS350-48T-4G	48-Port Gigabit Managed Switch
CBS350-48P-4G	48-Port Gigabit PoE Managed Switch
CBS350-48FP-4G	48-Port Gigabit PoE Managed Switch
CBS350-24T-4X	24-Port Gigabit Stackable Managed Switch with 10G Uplinks
CBS350-24P-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-24FP-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-48T-4X	48-Port Gigabit Stackable Managed Switch with 10G Uplinks
CBS350-48P-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks
CBS350-48FP-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks

What's New in This Release

1.1 Browser and OS Support

The device web UI supports the following browsers and OS system:

- Supported OS – MS Windows 7 (32 & 64 bit), MS Windows 10 (32 & 64 bit), MAC OS (not supported: MS Windows 8, 8.1, XP and Vista; Linux)
- Supported Browsers – Chrome, Firefox and Microsoft Edge (Microsoft Internet Explorer not supported) – both for Windows and for MAC OS; Safari – MAC OS only.

1.2 Web GUI Style

The CBS 3.0 uses a new GUI style which is the PISA compliant.

1.3 Password Complexity

For enhanced security, the user does not have the option to disable the password complexity setting. The password complexity is supported with the following default and ranges:

- Min-length – range 8-64, default = 8
- Min-class – range 1-4, default = 3

- No-repeat – range 1-16, default = 3
- Not-current/not-username/not manufacturer = are always enabled

1.4 SSL Cipher Support

For enhanced security, support for the following Ciphers was removed:

- RSA_WITH_AES_128_CBC_SHA256;
- RSA_WITH_AES_128_GCM_SHA256;
- RSA_WITH_AES_128_CCM_8;
- RSA_WITH_AES_256_CCM_8

1.5 SSL Cipher Support

OpenSSL version upgraded from 1.1.0b to 1.1.0l (Lower case L).

1.6 Console Support

The following changes were introduced to the console support:.

- SKUs in this release support both the RJ45 and mini USB console – mini USB has precedence.
- CBS250 SKUs support console interface (In Tesla Product line the 250 SKUs did not support a console interface).

Note Console support relates only to the SKUs in this release. SKUs in following releases support a single RJ45 interface, and the 250 product line SKUs do not support console.

1.7 Password Encryption

In the previous version, the user's credentials were saved to the config file and displayed using SHA-1 hash algorithm. In the current release, the user's credentials are salted and hashed using PBKDF2 based on HMAC-SHA-512 hash. This adds additional security to the credentials and protects them from various attacks.

Relevant credentials:

- Local database password
- Enable password
- Line password

1.8 Self-Signed Certificate Lifetime

To enhance security, the default and supported validity of the device self signed certificate are changed:

- Validity Range: 30 days to 1095 days (i.e. 3 years); was 30 days to 10 years.
- Default = 730 days (i.e 2 years); was 1 year.

1.9 Real Time Clock

SKUs in this release support have an internal self-sufficient Real Time Clock (RTC) component that keeps time even when the device is shut down and not connected to a power source. This internal clock is initialized during manufacturing and can be updated by the time features of the device when the software clock is set (for example manually or via SNTP).

In a stack configuration – all units will sync with the master unit RTC. For more details on stack behavior see functional spec. Note: future releases of CBS may contain SKUs that do not support RTC – in this case a different unit (not the master) will be used as the system time source.

RTC is considered “reliable” for features that require a “reliable” time source: Time range settings; updating IP DHCP Snooping Database and scheduled reboot.

1.10 PNP Agent Enhancements

CBS 3.0 supports the configuration of HTTPS as 1st choice” transport protocol. Tesla 2.5.5 supported only HTTP as 1st choice transport protocol.

1.11 Stack Unit ID Indication

The stacking SKUs in this release do not support dedicated stacking LED(s). Therefore the system LED is used on these units to indicate stack unit ID, as follows:

- Active unit – system LED will remain solid green (unless device is in bootup phase, or there is a HW fault or device is not connected to the power).
- For member units - following completion of bootup phase and connection to the master unit, every 20 seconds the System LED will blink green according to unit ID of the member unit:
  - Unit 1 (if not active) – system LED will blink 1 time;
  - Unit 2 (if not active) – system LED will blink 2 times;
- Unit 3 – system LED will blink 3 times;
- Unit 4 – system LED will blink 4 times;

Note Note: SKUs added in following releases may support dedicated stacking LEDs.

Known Issues

Table 12: Caveats Acknowledged in Release V3.0.0.61

Number	Description
CSCvu81820	**Symptom** Fan status is showing OK even after disconnecting Fan from the SKU SG252X-4. **Workaround** None.

Number	Description
CSCvu81812	**Symptom** 100M SFP is not support on non-combo ports. **Workaround** None.
CSCvu81814	**Symptom** When a non-PD connects to a switch PoE port, PoE short counter increases and status show fault. **Workaround** Disable PoE at port level.
CSCvu81816	**Symptom** Loopback detection shouldn't be triggered when pvst/rpvst is enable. **Workaround** None.
CSCvu81808	**Symptom** Edit ace several times via GUI cause the ace is deleted wrongly. **Workaround** None.
CSCvu81809	**Symptom** Apply/Remove ACL to/from port-channel and its member port cause traffic interrupt. **Workaround** None.
CSCvu81810	**Symptom** Fail to associate time-range with mac acl via GUI. **Workaround** None.
CSCvu81811	**Symptom** GUI: DUT take 45 seconds to configure spanning tree as PVST. **Workaround** None.

Number	Description
CSCvu81807	**Symptom** After I set permit ip source 10.10.10.1 service telnet gi1, Show management access-list Telnet. Only then it will not display port. **Workaround** None.
CSCvu81818	**Symptom** Fan RPM in CBS250-48T-4X is always showing 4075 after FAN disconnect. **Workaround** None.
CSCuu65516	**Symptom** If a language file fails to download (for example, due to a network problem), your Internet browser may display “incomplete/error information.” **Workaround** Delete your browser cookies and try again. The device can still be managed using Telnet.
CSCuu65557	**Symptom** If the management session is using the device’s IPv6 address, and this is a secure session (HTTPS), the device cannot be managed using the Safari browser. **Workaround** Either use a different browser (such as Internet Explorer) or set up an insecure session (HTTP).
CSCuq03628	**Symptom** An ISATAP client sends RS packets only when the tunnel interface is disabled, and then enabled. **Workaround** In mixed devices applications, manually disable and enable the tunnel interface.
CSCuu61125	**Symptom** The show VLAN command, for VLAN 1, shows non-present interfaces (port and stack units). **Workaround** This is a display issue only.

Number	Description
CSCuu61008	**Symptom** The show VLAN command, for VLAN 1, shows non-present interfaces (port and stack units). **Workaround** None.
CSCuy97946	**Symptom** DHCPv6 relay doesn't work if set destination to tunnel interface. **Workaround** Use IPv6 Global destination address as DHCPv6 destination.
CSCuy97999	**Symptom** When using web based authentication and device DHCP server –unauthenticated station IP address is not expired after station sent DHCP release. **Workaround** Wait till IP address expires after full lease expiration.
CSCva97586	**Symptom** RSPAN - if traffic is duplicated to destination port due to mirror operation and another operation (for example regular forwarding) is performed at the exact same time – not all of the traffic is mirrored to RSPAN destination port. **Workaround** None.
CSCve55081/ CSCve55217	**Symptom** On specified devices, on certain ports – when no cable is connected, or cable length is very short, running Cable test via command “test cable-diagnostics tdr” may provide unpredictable results. **Workaround** None.
CSCve55094	**Symptom** Queue statistics. Packet size is calculated based on the packet size on ingress, although statistics themselves are egress statistics. **Workaround** None.

Number	Description
CSCvj32418	**Symptom** In rare scenario (adding 700 certain IPv6 routes) Hardware routing will be disabled – even though resource table is not full. **Workaround** Configure less or different IPv6 routes. if issue occurs – reduce some routes that are not needed and reactivate HW based routing.
CSCvp40302	**Symptom** Loopback detection is triggered when pvst/rpvst is enable, even though it shouldn't. **Workaround** Do not enable Loopback detection together with PVST/RVPST.
CSCvp40311	**Symptom** Cable-diagnostics tdr will always display "short cable" on 10G ports. **Workaround** None.
CSCvp40317	**Symptom** PSE port connected to pacific NICs (not PD device) will display status of "Short" condition. **Workaround** None.
CSCvq63060	**Symptom** Secure SSH file copy (from switch to SSH/SCP server) is not supported over SSH connection (where switch is the SSH server). **Workaround** Use console, telnet or web connection to perform secure SSH file copy from switch to SCP server.
CSCvu16282	**Symptom** Cisco Business Dashboard Probe cannot connect to manager automatically after the primary stack switchover. **Workaround** Reload the stack.
CSCvu16298	**Symptom** PoE LED still light up after save "disable port LEDs" with reboot. **Workaround** None.

Number	Description
CSCvu24619	**Symptom** Backup unit in stack might reboot if Cisco Business Dashboard probe state is toggled between disable and enable within a few seconds. **Workaround** Wait more than 10 seconds before toggling the Cisco Business Dashboard probe state.

Cisco Business Online Support

For current support information, visit the pages given below:

Cisco Business	
Cisco Business Home	http://www.cisco.com/go/ciscobusiness
Support	
CBS250 Product Page	http://www.cisco.com/c/en/us/products/switches/business-250-series-smart-switches/index.html
CBS350 Product Page	https://www.cisco.com/c/en/us/products/switches/business-350-series-managed-switches/index.html
Cisco Business Support Community	http://www.cisco.com/go/cbcommunity
Cisco Business Support and Resources	http://www.cisco.com/go/smallbizhelp
Cisco Business Phone Support	http://www.cisco.com/go/cbphone
Cisco Business Chat Support	http://www.cisco.com/go/cbchat
Cisco Business Firmware Downloads	http://www.cisco.com/go/smallbizfirmware Select a link to download the firmware for your Cisco product. No login is required.
Cisco Business Open Source Requests	If you wish to receive a copy of the source code to which you are entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please send your request to: external-opensource-requests@cisco.com. In your request, please include the Cisco product name, version, and the 18 digit reference number (for example: 7XEEX17D99-3X49X08 1) found in the product open source documentation.

Appendix

Note Please note that Cisco suggests running the latest firmware on these switches to take advantage of the bug fixes and security updates that were included in the latest release.

This section describes the various product IDs found in the CBS series switches, as well as the corresponding hardware revisions, and the minimum software version supported.

Hardware revision 03 and above for Americas (05 and above for rest of the world) support ACT2 chipset, which offers enhanced security features for the switches and as such, cannot support software version below 3.2.0.84. Earlier Hardware revisions (02 and below for Americas, 04 and below for Rest of the world) can be downgraded to software version below 3.2.0.84.

Should you want to downgrade the firmware on the device, compare the TAN value on the device sticker to the TAN number in the list below. If you can't find yours, it implies the firmware can be downgraded without limitation; otherwise, the restrictions listed in the table apply. The minimal firmware you can downgrade to for the devices in the table where the TAN value is not reported is 3.1.0.57, as indicated.

Base SKU	Product Description	Regions	Hardware Version	TAN	Minimum Software
CBS250-8T-E-2G	8-Port Gigabit Smart Switch	Americas	V03	74-123398-03	3.2.0.84
		Rest of the World	V05	74-123399-05	3.2.0.84
CBS250-8PP-E-2G	8-Port Gigabit PoE Smart Switch	Americas	V03	74-123412-03	3.2.0.84
		Rest of the World	V05	74-123413-05	3.2.0.84
CBS250-8P-E-2G	8-Port Gigabit PoE Smart Switch	Americas	V03	74-123414-03	3.2.0.84
		Rest of the World	V05	74-123415-05	3.2.0.84
CBS250-8FP-E-2G	8-Port Gigabit PoE Smart Switch	Americas	V03	74-123416-03	3.2.0.84
		Rest of the World	V05	74-123417-05	3.2.0.84
CBS250-16T-2G	16-Port Gigabit Smart Switch	Americas	V03	74-123418-03	3.2.0.84
		Rest of the World	V05	74-123419-05	3.2.0.84
CBS250-16P-2G	16-Port Gigabit PoE Smart Switch	Americas	V03	74-123420-03	3.2.0.84
		Rest of the World	V05	74-123421-05	3.2.0.84
CBS250-24T-4G	24-Port Gigabit Smart Switch	Americas	V03	74-123422-03	3.2.0.84
		Rest of the World	V05	74-123423-05	3.2.0.84

CBS250-24PP-4G	24-Port Gigabit PoE Smart Switch	Americas	V03	74-123424-03	3.2.0.84
		Rest of the World	V05	74-123425-05	3.2.0.84
CBS250-24P-4G	24-Port Gigabit PoE Smart Switch	Americas	V03	74-123426-03	3.2.0.84
		Rest of the World	V05	74-123427-05	3.2.0.84
CBS250-24FP-4G	24-Port Gigabit PoE Smart Switch	Americas	V03	74-123428-03	3.2.0.84
		Rest of the World	V05	74-123429-05	3.2.0.84
CBS250-48T-4G	48-Port Gigabit Smart Switch	Americas	V03	74-123430-03	3.2.0.84
		Rest of the World	V05	74-123431-05	3.2.0.84
CBS250-48PP-4G	48-Port Gigabit PoE Smart Switch	Americas	V03	74-123432-03	3.2.0.84
		Rest of the World	V05	74-123433-05	3.2.0.84
CBS250-48P-4G	48-Port Gigabit PoE Smart Switch	Americas	V03	74-123434-03	3.2.0.84
		Rest of the World	V05	74-123435-05	3.2.0.84
CBS250-24T-4X	24-Port Gigabit Smart Switch with 10G Uplinks	Americas	V03	74-123436-03	3.2.0.84
		Rest of the World	V05	74-123437-05	3.2.0.84
CBS250-24P-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks	Americas	V03	74-123438-03	3.2.0.84
		Rest of the World	V05	74-123439-05	3.2.0.84
CBS250-24FP-4X	24-Port Gigabit PoE Smart Switch with 10G Uplinks	Americas	V03	74-123440-03	3.2.0.84
		Rest of the World	V05	74-123441-05	3.2.0.84
CBS250-48T-4X	48-Port Gigabit Smart Switch with 10G Uplinks	Americas	V03	74-123442-03	3.2.0.84
		Rest of the World	V05	74-123443-05	3.2.0.84
CBS250-48P-4X	48-Port Gigabit PoE Smart Switch with 10G Uplinks	Americas	V03	74-123444-03	3.2.0.84
		Rest of the World	V05	74-123445-05	3.2.0.84
CBS350-8T-E-2G	8-Port Gigabit Managed Switch	Americas	V03	74-123446-03	3.2.0.84
		Rest of the World	V05	74-123447-05	3.2.0.84

CBS350-8P-2G	8-Port Gigabit PoE Managed Switch	Americas	V03	74-123448-03	3.2.0.84
		Rest of the World	V05	74-123449-05	3.2.0.84
CBS350-8P-E-2G	8-Port Gigabit PoE Managed Switch	Americas	V03	74-123450-03	3.2.0.84
		Rest of the World	V05	74-123451-05	3.2.0.84
CBS350-8FP-2G	8-Port Gigabit PoE Managed Switch	Americas	V03	74-123452-03	3.2.0.84
		Rest of the World	V05	74-123453-05	3.2.0.84
CBS350-8FP-E-2G	8-Port Gigabit PoE Managed Switch	Americas	V03	74-123454-03	3.2.0.84
		Rest of the World	V05	74-123455-05	3.2.0.84
CBS350-16T-2G	16-Port Gigabit Managed Switch	Americas	V03	74-123456-03	3.2.0.84
		Rest of the World	V05	74-123457-05	3.2.0.84
CBS350-16T-E-2G	16-Port Gigabit Managed Switch	Americas	V03	74-123458-03	3.2.0.84
		Rest of the World	V05	74-123459-05	3.2.0.84
CBS350-16P-2G	16-Port Gigabit PoE Managed Switch	Americas	V03	74-123460-03	3.2.0.84
		Rest of the World	V05	74-123461-05	3.2.0.84
CBS350-16P-E-2G	16-Port Gigabit PoE Managed Switch	Americas	V03	74-123462-03	3.2.0.84
		Rest of the World	V05	74-123463-05	3.2.0.84
CBS350-16FP-2G	16-Port Gigabit PoE Managed Switch	Americas	V03	74-123464-03	3.2.0.84
		Rest of the World	V05	74-123465-05	3.2.0.84
CBS350-24T-4G	24-Port Gigabit Managed Switch	Americas	V03	74-123466-03	3.2.0.84
		Rest of the World	V05	74-123467-05	3.2.0.84
CBS350-24P-4G	24-Port Gigabit PoE Managed Switch	Americas	V03	74-123468-03	3.2.0.84
		Rest of the World	V05	74-123469-05	3.2.0.84
CBS350-24FP-4G	24-Port Gigabit PoE Managed Switch	Americas	V03	74-123470-03	3.2.0.84
		Rest of the World	V05	74-123471-05	3.2.0.84

CBS350-48T-4G	48-Port Gigabit Managed Switch	Americas	V03	74-123472-03	3.2.0.84
		Rest of the World	V05	74-123473-05	3.2.0.84
CBS350-48P-4G	48-Port Gigabit PoE Managed Switch	Americas	V03	74-123474-03	3.2.0.84
		Rest of the World	V05	74-123475-05	3.2.0.84
CBS350-48FP-4G	48-Port Gigabit PoE Managed Switch	Americas	V03	74-123476-03	3.2.0.84
		Rest of the World	V05	74-123477-05	3.2.0.84
CBS350-24T-4X	24-Port Gigabit Stackable Managed Switch with 10G Uplinks	Americas	V03	74-123478-03	3.2.0.84
		Rest of the World	V05	74-123479-05	3.2.0.84
CBS350-24P-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	Americas	V03	74-123480-03	3.2.0.84
		Rest of the World	V05	74-123481-05	3.2.0.84
CBS350-24FP-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	Americas	V03	74-123482-03	3.2.0.84
		Rest of the World	V05	74-123483-05	3.2.0.84
CBS350-48T-4X	48-Port Gigabit Stackable Managed Switch with 10G Uplinks	Americas	V03	74-123484-03	3.2.0.84
		Rest of the World	V05	74-123485-05	3.2.0.84
CBS350-48P-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	Americas	V03	74-123486-03	3.2.0.84
		Rest of the World	V05	74-123487-05	3.2.0.84
CBS350-48FP-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	Rest of the World	V05	74-123489-05	3.2.0.84
CBS250-8T-D	8-Port Gigabit Smart Switch	All	All	All	3.1.0.57
CBS250-8PP-D	8-Port Gigabit PoE Smart Switch	All	All	All	3.1.0.57
CBS350-8S-E-2G	8-Port Gigabit SFP Managed Switch	All	All	All	3.1.0.57
CBS350-24S-4G	24-Port Gigabit SFP Managed Switch	All	All	All	3.1.0.57
CBS350-8MGP-2X	8-Port 2.5G PoE Managed Switch	All	All	All	3.1.0.57
CBS350-8XT	8-Port 10G Stackable Managed Switch	All	All	All	3.1.0.57

CBS350-12XT	12 Port 10G Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-24XS	24-Port 10G SFP+ Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-12XS	12-Port 10G SFP+ Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-16XTS	16-Port 10G Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-24XTS	24-Port 10G Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-24XT	24-Port 10G Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-48XT-4X	48-Port 10G Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-8MP-2X	8-Port 2.5G PoE Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-24MGP-4X	24-Port 2.5G PoE Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-12NP-4X	12-Port 5G PoE Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-24NGP-4X	24-Port 5G PoE Stackable Managed Switch	All	All	All	3.1.0.57
CBS350-48NGP-4X	48-Port 5G PoE Stackable Managed Switch	All	All	All	3.1.0.57