# Release Notes for SF250, SG250, SF350, SG350, SG350X, SG350XG, SF550X, SG550X, and SG550XG Series Switches Software Version 2.3.0.130

**October 16, 2017**

These Release Notes describe the recommended practices and known issues that apply to software version 2.3.0.130 for the products listed in the following table:

| Model | Description | Ports |
|---|---|---|
| **SF250-48** | 48-Port 10/100 Smart Switch | fa1-fa48, gi1-gi4 |
| **SF250-48HP** | 48-Port 10/100 PoE Smart Switch | fa1-fa48, gi1-gi4 |
| **SG250-10P** | 10-Port Gigabit PoE Smart Switch | gi1-gi10 |
| **SG250-26** | 26-Port Gigabit Smart Switch | gi1-gi26 |
| **SG250-26HP** | 26-Port Gigabit PoE Smart Switch | gi1-gi26 |
| **SG250-26P** | 26-Port Gigabit PoE Smart Switch | gi1-gi26 |
| **SF350-48** | 48-Port 10/100 Managed Switch | fa1-fa48, gi1-gi4 |
| **SF350-48MP** | 48-Port 10/100 PoE Managed Switch | fa1-fa48, gi1-gi4 |
| **SF350-48P** | 48-Port 10/100 PoE Managed Switch | fa1-fa48, gi1-gi4 |
| **SG350-10** | 10-Port Gigabit Managed Switch | gi1-gi10 |
| **SG350-10MP** | 10-Port Gigabit PoE Managed Switch | gi1-gi10 |
| **SG350-10P** | 10-Port Gigabit PoE Managed Switch | gi1-gi10 |

| Model | Description | Ports |
|---|---|---|
| **SG350-28** | 28-Port Gigabit Managed Switch | gi1-gi28 |
| **SG350-28MP** | 28-Port Gigabit PoE Managed Switch | gi1-gi28 |
| **SG350-28P** | 28-Port Gigabit PoE Managed Switch | gi1-gi28 |
| **SG350-8PD** | 8-Port 2.5G PoE Managed Switch | gi1-gi6, tw7-tw8, te1-te2 |
| **SG350X-24** | 24-Port Gigabit Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG350X-24MP** | 24-Port Gigabit PoE Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG350X-24P** | 24-Port Gigabit PoE Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG350X-24PD** | 24-Port 2.5G PoE Stackable Managed Switch | gi1-gi10, gi13-gi22, tw11-tw12, tw23-tw24, te1-te2 |
| **SG350X-48** | 8-Port Gigabit Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG350X-48MP** | 48-Port Gigabit PoE Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG350X-48P** | 48-Port Gigabit PoE Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG350X-8PMD** | 8-Port 2.5G PoE Stackable Managed Switch | tw1-tw8, te1-te2 |
| **SF550X-24** | 24-Port 10/100 Stackable Managed Switch | fa1-fa24, te1-te4 |
| **SF550X-24MP** | 24-Port 10/100 PoE Stackable Managed Switch | fa1-fa24, te1-te4 |
| **SF550X-24P** | 24-Port 10/100 PoE Stackable Managed Switch | fa1-fa24, te1-te4 |
| **SF550X-48** | 48-Port 10/100 Stackable Managed Switch | fa1-fa48, te1-te4 |

| Model | Description | Ports |
|---|---|---|
| **SF550X-48MP** | 48-Port 10/100 PoE Stackable Managed Switch | fa1-fa48, te1-te4 |
| **SF550X-48P** | 48-Port 10/100 PoE Stackable Managed Switch | fa1-fa48, te1-te4 |
| **SG550X-24** | 24-Port Gigabit Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG550X-24MP** | 24-Port Gigabit PoE Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG550X-24MPP** | 24-Port Gigabit PoE Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG550X-24P** | 24-Port Gigabit PoE Stackable Managed Switch | gi1-gi24, te1-te4 |
| **SG550X-48** | 48-Port Gigabit Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG550X-48MP** | 48-Port Gigabit PoE Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG550X-48P** | 48-Port Gigabit PoE Stackable Managed Switch | gi1-gi48, te1-te4 |
| **SG350XG-24F** | 24-Port 10G SFP+ Stackable Managed Switch | te1-te24 |
| **SG350XG-24T** | 24-Port 10GBase-T Stackable Managed Switch | te1-te24 |
| **SG350XG-2F10** | 12-Port 10G Stackable Managed Switch | te1-te12 |
| **SG350XG-48T** | 48-Port 10GBase-T Stackable Managed Switch | te1-te48 |
| **SG550XG-24F** | 24-Port 10G SFP+ Stackable Managed Switch | te1-te24 |
| **SG550XG-24T** | 24-Port 10GBase-T Stackable Managed Switch | te1-te24 |

| Model | Description | Ports |
|---|---|---|
| **SG550XG-48T** | 48-Port 10GBase-T Stackable Managed Switch | te1-te48 |
| **SG550XG-8F8T** | 16-Port 10G Stackable Managed Switch | te1-te16 |

# Contents



# What's New in this Release

- Multigigabit support—Multigigabit ports negotiation is based on 2.5G/5Gbase-T IEEE 802.3bz-2016 and is fully compliant with the NBASE-T final specification (version 2.3).
- Multicast TV VLAN Enhancement—The multicast TV VLAN feature is enhanced to now support the configuration of up to 250 ranges of multicast addresses associated to the multicast VLAN. Each range can include the entire multicast address range except the multicast reserved address range.
- VLAN mapping/VLAN tunneling—An enhancement to the existing QinQ feature, which allowed the addition, per port, of a single Service tag (S-tag). The same S-tag was added to any Customer-tagged (C-tag) frame received on the interface, regardless of the C-tag VLAN-ID.
  - VLAN tunneling adds the ability to replace existing tag (C-tag) with a new tag (S-tag), and supports defining a different S-tag for different C-tag.
  - VLAN mapping adds the ability to add an S-tag based on the C-tag received (which allows different S-tag for different C-tags), and to define a default S-tag for C-tags that are not specifically mapped.
  - VLAN mapping also allows changing or defining the Ethertype of the S-tag with one of the Ethertypes dot1q (default) or dot1ad | 9100 | 9200.
- QoS statistics—This feature is enhanced to automatically provide per-port and per-queue egress statistics for packets and byte count. You no longer need to create the sets of statistics.
- Smart Network Application (SNA)—This feature now supports the following functionality:
  - VLAN membership service for multiple devices + trunk vlan mode

  - Interface management service
  - Adding functionality to device explorer/host name per port
  - Dashboard
  - Device location with LED flashing.

- IPv6 DHCP client—Support for IPv6 (DHCPv6) stateful client. With this feature, the device can receive its IPv6 address allocation from a DHCPv6 server, in addition to stateless information such as the DNS server IPv6 address, the SNTP server IPv6 address, and so on.
- VRRP - accept mode control—VRRP accept mode defines whether the VRRP router acting as the master switch takes ownership of the VRRP virtual IP address even if it not the address owner. If accept mode is set to "accept," the virtual router acting as master switch processes and handles traffic sent to the virtual IP address, even if it is not the owner of this address. If accept mode is set to "drop," the virtual router drops traffic that is sent to the virtual IP address, unless the virtual router is the owner of the addresses.
- SLA object tracking for static routes—The SLA operation provides a mechanism to track the connectivity to a destination network via the next hop specified in the static route. If connectivity to a destination network is lost, the route state is set to down, and, if available, a different static route that is in up state can now be selected for routing traffic.
- 802.1x supplicant—In addition to capacity as an 802.1x authenticator, a port on a switch can be configured as an 802.1x supplicant to seek port access permission from a neighbor switch or other authenticator. The supplicant supports the EAP MD5-Challenge method specified by RFC3748. This method authenticates a client by its name and password.
- 802.1x on individual interfaces in LAG—The authenticator and supplicant can be enabled on individual Ethernet interfaces that are members of a LAG/port-channel. In this case, and in accordance with the 802.1x standard, the 802.1x protocol runs individually on each Ethernet port that is associated to the port channel. 802.1x features can be enabled on all or on some of the interfaces in LAG. Only authorized Ethernet ports can be active members in the port channel.
- 802.1x 2010 based statistics—When displaying statistics by using the **show dot1x statistics interface** command or the web-based user interface, the device displays an extended EAP counters set. The counters that are displayed are based on the 802.1x-2010 standard

- Security—SSL enhancements:
  - Disabled support for TLS v1.1
  - Disables support for the following weak SSL ciphers: cipher suites offering no authentication, cipher suites offering no encryption, weak-ciphers below 64 bit, cipher suites using DES, cipher suites using 3DES, cipher suites using RC2, cipher suites using RC4, and cipher suites using MD5
- Security—SSH enhancements:
  - Removed support for following weak ciphers: aes256-cbc, arcfour, aes128-cbc, 3des-cbc, and aes192-cbc
  - Added support for the following ciphers: aes128-ctr, aes192-ctr, aes256-ctr
  - Removed the hmac-md5 message authentication code (MAC)
- Downgrade prevention—In some cases, previous software releases cannot support certain newer unit hardware revisions. Downloading and running the older version on a newer platform may result in device not functioning or the device running in an endless reboot cycle.

  In such cases, the download of an older software version to a newer device revision is prevented. In a stack configuration, the download is prevented to the master and all units if the stack master or any of the units are of the new HW revision. Adding a unit to an existing stack succeeds only if both active and non-active images of stack support the hardware revision of the additional unit.
- Device location—Device location allows a system administrator to easily locate a specific device (single or stack) among all devices in a network environment. When the feature is activated, all network port LEDs on the specified device flash for the duration that you specify (the default duration is 1 minute). When you activate this feature, you can specify whether a specific device in the stack or all devices in the stack flash their network port LEDs.
- Configuration migration—The configuration migration service facilitates the process of replacing Sx200/300/500 series devices with new Sx250/350/550 series devices while maintaining the functionality of a device. This service is hosted on the Cisco website, and not part of the 2.3.0.130 image features. After you navigate to the service in a web browser, you are prompted to load the configuration file from a Sx200/300/500 series device. Then the system analyzes the configuration and alter commands

that were changed between the products to make sure the configuration file can be loaded to a Sx250/350/550 series device.

- PoE enhancements:
  - LLDP and CDP interoperability—Support for full interoperability of CDP and LLDP L2 PoE power level negotiation. CDP has precedence. If CDP information is not received within 10 seconds, LLDP information is used. The protocol that is not chosen (CDP or LLDP) advertises power information based on the negotiation of the active protocol
  - CDP/LLDP “expired” state—After CDP or LLDP is selected as the active protocol for power negotiation, it remains as the active protocol until a link status change occurs or PoE is disabled then enabled on the interface. If the power supply device or the powered device does not receive PoE information from the active protocol (for example, if a neighbor timeout occurs) a port moves to “expired” negotiation state. The power level that was set via negotiation is maintained until a link change or PoE enable change occurs.
  - Disable class error detection—A control to disable class error detection had been added. (Class error detection is enabled by default.) Class error is a situation in which the powered device classification current is higher than 44 mA. The control was added to support powered devices that may not be standard compliant.
- MAC Address table (FDB) max aging time—The MAC Address table max aging time has been changed from 500 seconds to 400 seconds for Sx250 and Sx350 switches. If in previous versions this time on these devices was set to a value higher than 400 seconds, device will uses default aging value of 300 seconds when it is updated to 2.3.0.130 software. You then can configure a value up to 400 seconds.

# Known Issues

## Open Bugs in Software Version 2.3.0.130

This section lists that bugs that are acknowledged in software version 2.3.0.130.

**Table 1 Open Bugs in Software Version 2.3.0.130**

| Bug ID | Description |
|---|---|
| CSCve55065 | **Symptom:** 6to4 tunnel traffic is not forwarded in line rate when the tunnel outgoing port is trunk or general tagged.<br><br>**Workaround:** Configure tunnel outgoing port as access or no switch port. |
| CSCve55069 | **Symptom:** Some functions in the web GUI not response when using the Apple Safari browser: reboot button, logout, Stop button of Locate Device.<br><br>**Workaround:** Use the Google Chrome, Mozilla Firefox, or Microsoft Edge browser. |
| CSCve55070 | **Symptom:** When a PoE port is connected to a neighbor that is not a PD, the invalid signature counter keeps increasing.<br><br>**Workaround:** This behavior is expected behavior due to the detection process when a non-PD devices is connected to a port. |
| CSCve55072 | **Symptom:** When defining a time range for a PoE operation and the time range does not include the hour 00:00 as the active time, the PoE consumption values for hours, days and weeks show 0 even if there is a consumption during the displayed period (minutes display correct values).<br><br>**Workaround:** There is no workaround. |
| CSCve55074 | **Symptom:** In some cases, If the unit-ID setting of a unit in a stack is changed from set ID to auto unit ID, the device does not join the stack after reload.<br><br>**Workaround:** Do not change unit ID settings on a unit already in a stack. If the issue happens, disconnect and then reconnect the “stuck” unit from the power source to re-add it to the stack. |
| CSCve55078 | **Symptom:** Egress traffic shaping on XG device uplink interfaces limits traffic to 80 Kbps, even if you configured a lower rate.<br><br>**Workaround:** Use an egress shaping value higher than 80 Kbps. |

**Table 1 Open Bugs in Software Version 2.3.0.130 (Continued)**

| Bug ID | Description |
|---|---|
| CSCve55081/ CSCve55217 | **Symptom:** On some devices and on certain ports when no cable is connected or cable length is very short, running Cable test via the "test cable-diagnostics tdr" command may provide unpredictable results.<br>**Workaround:** There is no workaround |
| CSCve55082 | **Symptom:** If a Cisco 28/29xx terminal server is connected to slave units and "exec" is configured on line, when issuing a reboot command (from master) slave unit reboot may be suspended.<br>**Workaround:** To prevent this issue, configure "no exec" on line of terminal server before rebooting the stack. |
| CSCve55087 | **Symptom:** After a unit switchover from backup to master, the USB interface does not recognize an inserted flash stick (disk on key)<br>**Workaround:** Reload the unit. |
| CSCve55090 | **Symptom:** SNA—when configuring duplex and speed settings for multiple interfaces at the same time, the web page needs to be refreshed to view updated setting.<br>**Workaround:** Refresh web page |
| CSCve55094 | **Symptom:** Queue statistics: packet size is calculated based on the packet size on ingress, although statistics are egress statistics.<br>**Workaround:** There is no workaround. |
| CSCve55102 | **Symptom:** PoE: In rare cases, the voltage display for ports connected to PD, is lower than actual voltage.<br>**Workaround:** There is no workaround. |

**Table 1 Open Bugs in Software Version 2.3.0.130 (Continued)**

| Bug ID | Description |
|---|---|
| CSCve55112 | **Symptom:** Config migration: when converting a configuration file from a Sx200/Sx300/Sx500 PoE device to a Sx250/Sx350/Sx550 non-PoE device, the following command includes PoE parameter and loading of the file to the destination device fails: "lldp med enable network-policy poe-pse inventory."<br><br>**Workaround:** Manually remove the items related to PoE. |
| CSCve55117 | **Symptom:** Config migration tool: When converting large files (more than 10,000 lines), the browser may respond slowly or crash.<br><br>**Workaround:** There is no workaround. |
| CSCve55188 | **Symptom:** Web browser can hang due to lack of RAM because SNA does not release RAM correctly when left open for a long time, such as overnight.<br><br>**Workaround:** There is no workaround. |
| CSCve55203 | **Symptom:** SNA: When selecting multiple devices on which to upgrade firmware and choosing the reboot devices after download option, success indication is provided before the operation completes on all devices.<br><br>**Workaround:** There is no workaround. |
| CSCve55206 | **Symptom:** On XG devices with less than 48 ports, queue statistics from the "show queue statistics" command may show wrong information regarding the number of packets and bytes.<br><br>**Workaround:** There is no workaround. |
| CSCve60999 | **Symptom:** In some cases, a unit may not rejoin a stack after a master switchover (from original master to backup) or when the unit is disconnected and then reconnected to stack.<br><br>**Workaround:** Disconnect and then reconnect the "stuck" unit from the power source to re-add it to the stack |

## Resolved Bugs in Software Version 2.3.0.130

This section lists that bugs that are resolved in software version 2.3.0.130.

**Table 2 Resolved Bugs in Software Version 2.3.0.130**

| Bug ID | Description |
|---|---|
| CSCux89585 | **Symptom:** If CDP and LLDP are both enabled on a port, disabling one of them may cause the remaining protocol PoE negotiation to fail. |
| CSCuz88563 | **Symptom:** When connecting an Sx250x, Sx350x, or Sx550 PoE switch to a 3750 PoE switch, the Sx250x, Sx350x, or Sx550 provides power to the 3750 through PoE. |
| CSCva97565 | **Symptom:** The command “delete sna storage file-name” is missing from the system management chapter of the CLI guide.This command allows the deletion of SNA settings that are saved for a specific user (specified in “file-name” parameter).<br><br>**Workaround:** There is no workaround. |
| CSCva97583 | **Symptom:** SNA—In some cases, if a device is preconfigured (via CLI or web) with 802.1x/RADIUS configurations, display/ configuration via DAC may fail |
| CSCva97588 | **Symptom:** SNA—When logging in to a device with an IPv6 address using Win10 Edge, cannot view network topology. |
| CSCvc73697 | **Symptom:** Learned voice VLAN greater than 1024 flush existing VLAN. |
| CSCve55193 | **Symptom:** POE switch provides power when connect to a Cisco Catalyst switch. |

## Open Bugs in Software Version 2.2.8.04

This section lists that bugs that are acknowledged in software version 2.2.8.04.

**Table 3 Open Bugs in Software Version 2.2.8.04**

| Bug ID | Description |
|---|---|
| CSCvc73697 | **Symptom:** Learned voice VLAN greater than 1024 flush existing VLAN.<br>**Workaround:** There is no workaround.<br>This bug is resolved in software version 2.3.0.130. |

## Open Bugs in Software Version 2.2.7.07

There are no new open bugs in software version 2.2.7.07.

## Open Bugs in Software Version 2.2.5.68

This section lists that bugs that are acknowledged in software version 2.2.5.68.

**Table 4 Open Bugs in Software Version 2.2.5.68**

| Bug ID | Description |
|---|---|
| CSCva97565 | **Symptom:** The command “delete sna storage file-name” is missing from the system management chapter of the CLI guide.This command allows the deletion of SNA settings that are saved for a specific user (specified in “file-name” parameter).<br>**Workaround:** There is no workaround.<br>This bug is resolved in software version 2.2.5.68. |
| CSCva97578 | **Symptom:** SNA—In rare situations if SNA display is not touched for many hours, the SNA topology display is out of sync.<br>**Workaround:** Refresh the SNA display. |

**Table 4 Open Bugs in Software Version 2.2.5.68 (Continued)**

| Bug ID | Description |
|---|---|
| CSCva97583 | **Symptom:** SNA—In some cases, if a device is preconfigured (via CLI or web) with 802.1x/RADIUS configurations, display/configuration via DAC may fail.<br><br>**Workaround:** Remove all manual DAC related settings (802.1x/RADIUS) from the device before using the DAC feature.<br><br>This bug is resolved in software version 2.3.0.130. |
| CSCva97586 | **Symptom:** RSPAN—If traffic is simultaneously forwarded to a destination port due to a mirror operation and another operation (such as regular forwarding), not all traffic is mirrored to the RSPAN destination port<br><br>**Workaround:** There is no workaround. |
| CSCva97588 | **Symptom:** SNA—When logging in to a device with an IPv6 address using Win10 Edge, cannot view network topology.<br><br>**Workaround:** Use an IPv4 address or other browsers to connect.<br><br>This bug is resolved in software version 2.3.0.130. |
| CSCva97591 | **Symptom:** SNA—If devices have different times, selecting any statistics in "Connection Explorer" with interfaces selected for devices with different clock times shows incorrect graphs.<br><br>**Workaround:** Make sure that all devices have synchronized clocks (for example, via SNTP). |
| CSCva97601 | **Symptom:** Cannot upgrade firmware and configuration file from an SNA device to devices with version V2.1 or lower.<br><br>**Workaround:** Download of firmware to versions earlier than 2.2 is not supported. |
| CSCva97603 | **Symptom:** If the last physical interface in a VLAN is set to L3 mode and then back to L2 mode, the VLAN status stays down.<br><br>**Workaround:** Perform a shutdown/no shutdown on the physical interface. |

**Table 4 Open Bugs in Software Version 2.2.5.68 (Continued)**

| Bug ID | Description |
|---|---|
| CSCva97605 | **Symptom:** Upgrading boards running version 2.2.0.x to version 2.2.5.x is not possible via XMODEM.<br><br>**Workaround:** Use TFTP for upgrading from version 2.2.0.x to version 2.2.5.x. |

## Open Bugs in Software Version 2.2.0.63

This section lists that bugs that are acknowledged in software version 2.2.0.63.

**Table 5 Open Bugs in Software Version 2.2.0.63**

| Bug ID | Description |
|---|---|
| CSCuy97777 | **Symptom:** After reload, the actual spanning tree cost of port-channel is different with running-config.<br><br>**Workaround:** There is no workaround.<br><br>This bug is resolved in software version 2.2.5. |
| CSCuy97791 | **Symptom:** When STP cost path is equal, Port channel is always selected as root port even if it has a higher priority value.<br><br>**Workaround:** STP still functions properly and no loops are created. If needed, use cost setting to change the root port.<br><br>This bug is resolved in software version 2.2.5. |
| CSCuy97837 | **Symptom:** On dashboard, the port rx Traffic Error indication shows in red even though the interface counter and rmon statistics of proper ports were cleared.<br><br>**Workaround:** There is no workaround.<br><br>This bug is resolved in software version 2.2.5. |

**Table 5 Open Bugs in Software Version 2.2.0.63 (Continued)**

| Bug ID | Description |
|---|---|
| CSCuz01765 | **Symptom:** Some revisions of the Cisco IP Phone 7960 cannot be powered up on switch 60W ports.<br><br>**Workaround:** This issue occurs due to a short between phone pins. Connect phone to af/at ports or use Cat 3 cable (2 pairs) to connect a phone to a 60W port. |
| CSCuy97915 | **Symptom:** Cannot change XG port setting to “disable negotiation” and set speed at the same time via the GUI.<br><br>**Workaround:** First disable negotiation and click **Apply**, then change speed and click **Apply**. |
| CSCuy97943 | **Symptom:** In some cases, master unit reloads if stack unit type is changed from fixed to auto.<br><br>**Workaround:** Occurs only if stack units are reloaded twice. Stack stabilizes following master reload.<br><br>This bug is resolved in software version 2.2.5. |
| CSCuy97946 | **Symptom:** DHCPv6 relay does not work if destination is set to tunnel interface.<br><br>**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 is sent DHCP release.<br><br>**Workaround:** Wait until the IP address expires after full lease expiration. |
| CSCuz45730 | **Symptom:** When negotiating 60W PoE with Cisco PD switches, Cisco PoE-PSE switches sometimes are not able to provide 60W and provide 30W only.<br><br>**Workaround:** Connect PD switch to PSE switch before PSE switch boot up. Or disconnect then connect PD switch when issue happens. Or use static 60 watt.<br><br>This bug is resolved in software version 2.2.5. |

## Open Bugs in Software Version 2.1.0

This section lists that bugs that are acknowledged in software version 2.3.0.130.

**Table 6 Open Bugs in Software Version 2.1.0**

| Bug ID | Description |
|---|---|
| CSCux77649 | **Symptom:** When connecting a switch to a Cisco Catalyst compact UPOE PD device, LLDP may not negotiate power on AT / AF ports.<br><br>**Workaround:** Use CDP to negotiate.<br><br>This bug is resolved in software version 2.2.0. |
| CSCux77651 | **Symptom:** When applying policer on ingress interface and sending traffic with multiple priority may result in dropping of higher priority traffic on lower speed egress ports.<br><br>**Workaround:** There is no workaround. |
| CSCux77654 | **Symptom:** Egress ACL cannot be applied to and interface if ACE includes TCP/UDP port range as a parameter.<br><br>**Symptom:** Apply required TCP/UDP ports as individual ports in ACL, or apply a range as ingress ACL on relevant interfaces.<br><br>This bug is resolved in software version 2.2.5. |
| CSCux77675 | **Symptom:** Aggregate policer QoS statistic always display a value of 0 for both in and out of profile counters.<br><br>**Workaround:** There is no workaround.<br><br>This bug is resolved in software version 2.2.5. |
| CSCux89410 | **Symptom:** PVID is enabled on an interface when membership type is set to forbidden via the GUI. Interface functionality is not affected. The port still blocks traffic for the relevant VLAN.<br><br>**Workaround:** There is no workaround.<br><br>This bug is resolved in software version 2.2.0. |

**Table 6 Open Bugs in Software Version 2.1.0 (Continued)**

| Bug ID | Description |
|---|---|
| CSCux89413 | **Symptom:** Auto SmartMacro—In some cases, the interface is set to BPDU guard erri-disable state after replacing the device connected to the interface from a phone/desktop to switch.<br><br>**Workaround:** Either disable persistent setting on the interface, or, after the issue occurs, remove the desktop/phone macro from the interface, reactivate the port, and then connect the switch to the interface. |
| CSCux89418 | **Symptom:** When connecting Sx350P as PD to Sx300P/ Sx500P as PSE, Sx350P reboots when disconnecting AC power. After rebooting, Sx350P powers up and functions as expected.<br><br>**Workaround:** There is no workaround. |
| CSCux89582 | **Symptom:** Interface is suspended (down) when connecting a copper SFP (MGBT1/GLC-T SFP) with no cable. This issue happens when inserting uplink GE ports (for example, gi3 or gi4) of Sx350/Sx250 or to XG network ports.<br><br>**Workaround:** To prevent interface suspension, insert the cable to SFP before inserting SFP to port. If port is already in suspended state, insert the cable into SFP and then activate the suspended port, and the port moves to up state. |
| CSCux89585 | **Symptom:** If CDP and LLDP are both enabled on a port, disabling one of them may cause the remaining protocol PoE negotiation to fail.<br><br>**Workaround:** Do not enable both CDP and LLDP power negotiation at the same time. If the issue occurs, disconnect and then reconnect cable to PD.<br><br>This bug is resolved in software version 2.3.0.130. |
| CSCux89597 | **Symptom:** In port limit mode, the default admin power limit value for all types of ports (AF, AT, and 60W PoE) is 30 watts.<br><br>**Workaround:** Manually set a limit of 60 watts if needed. |

**Table 6 Open Bugs in Software Version 2.1.0 (Continued)**

| Bug ID | Description |
|---|---|
| CSCux89611 | **Symptom:** Power negotiation for 60W PoE via LLDP may take up to 1 minute to complete.<br><br>**Symptom:** There is no workaround. |
| CSCux89626 | **Symptom:** When connecting 60W PD to switch, in some cases power indication on switch is higher than 60W. This bug is a display issue. Actual PD consumption is 60W<br><br>**Workaround:** There is no workaround. |

## Open Bugs in Software Version 2.0.0

This section lists that bugs that are acknowledged in software version 2.0.0.

**Table 7 Open Bugs in Software Version 2.0.0**

| Bug ID | Description |
|---|---|
| CSCuq03628 | **Symptom:** An ISATAP client sends RS packets only when the tunnel interface is disabled and then enabled.<br><br>**Workaround:** As long as the tunnel endpoints are both SG350XG/ SG550XG, the tunnel works. In mixed devices applications, manually disable and enable the tunnel interface. |
| CSCur86883 | **Symptom:** When using the web-based configuration interface to set up queue scheduling, you may have a lengthy response time if the system includes a stack of four or more units.<br><br>**Workaround:** After about one minute, the web-based configuration interface becomes responsive again, and the setting takes effect. Use the command line interface (CLI) commands for a quicker response time |

**Table 7 Open Bugs in Software Version 2.0.0 (Continued)**

| Bug ID | Description |
|---|---|
| CSCuu60952 | **Symptom:** When changing an ACE action using the configuration interface, (for example, from deny to shutdown) ACE may be removed from the ACL.<br><br>**Workaround:** Reconfigure the ACE, or use the CLI to remove the ACE and then configure it with the new action. |
| CSCuu60958 | **Symptom:** When configuring a MAC ACE using the web-based configuration interface, creation of new ACE may fail with an error message of "Entry Already Exists," even though it does not exist.<br><br>**Workaround:** Configure the ACE again and it will be accepted, or use the CLI to configure the ACE. |
| CSCuu60983 | **Symptom:** If VRRP is enabled on a device, DCHP relay using Option 82 fails.<br><br>**Workaround:** If VRRP is enabled on device, use DHCP relay without activating Option 82. |
| CSCuu60986 | **Symptom:** When enabling flow control on the LAG using the user interface, the port LEDs will not light even if link is up.<br><br>**Workaround:** This bug is a LED display issue. The functions work as expected. If needed, enable flow control using the command line interface.<br><br>This bug is resolved in software version 2.2.0. |
| CSCuu60989<br>CSCuu61046 | **Symptom:** Enabling an 802.1X guest VLAN or a Voice VLAN on a port is forbidden, if the port is a static member of the VLAN and it is in switchport mode (including inactive modes).<br><br>**Workaround:** Change the port VLAN membership that use switchport modes so that the port is not a static member in the desired VLAN.<br><br>**NOTE** In switchport mode Trunk, the port is a member of all the VLANs by default. Remove the membership in the desired VLANs, or in all VLANs, prior to configuring the 802.1X guest VLAN or the Voice VLAN.<br><br>This bug is resolved in software version 2.2.5. |

**Table 7 Open Bugs in Software Version 2.0.0 (Continued)**

| Bug ID | Description |
|---|---|
| CSCuu61008 | **Symptom:** Agreed Auto Voice VLAN cannot be defined as a primary VLAN, even after the voice VLAN is disabled.<br><br>**Workaround:** There is no workaround. |
| CSCuu61061 | **Symptom:** If short reach is enabled on a port, the cable length test using a Cat6a cable fails.<br><br>**Workaround:** Disable short reach when running the cable length test on an interface.<br><br>This bug is resolved in software version 2.2.5. |
| CSCuu61080 | **Symptom:** DHCP router option (Option 3) is sent by the switch DHCP server, even if the option is not configured for this pool.<br><br>**Workaround:** There is no workaround.<br><br>This bug is resolved in software version 2.2.0. |
| CSCuu61084 | **Symptom:** IPv6 Routes always display a metric value of “0.<br><br>**Workaround:** This bug is a display issue. The correct metric is used for IPv6 L3 forwarding decisions.<br><br>This bug is resolved in software version 2.2.5. |
| CSCuu61088 | **Symptom:** The **show qos interface** command displays info for interfaces that are not present.<br><br>**Workaround:** This bug is a display issue only. |
| CSCuu61100 | **Symptom:** Link partner shows that the link is up, even if the device interface is administratively shut down.<br><br>**Workaround:** This bug is a display issue. The link is actually down and does not forward traffic. |
| CSCuu61125 | **Symptom:** The **show** VLAN command, for VLAN 1, shows non-present interfaces (port and stack units).<br><br>**Workaround:** This bug is a display issue only. |

**Table 7 Open Bugs in Software Version 2.0.0 (Continued)**

| Bug ID | Description |
|---|---|
| CSCuu65516 | **Symptom:** If a language file fails to download (for example, due to a network problem), your Internet browser may display "incomplete/error information."<br><br>**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.<br><br>**Workaround:** Either use a different browser (such as Internet Explorer) or set up an insecure session (HTTP). |
| CSCuu65577 | **Symptom:** When using the web-based configuration interface to set a new keychain for RIP, include an accept-lifetime. If you don't include an accept-lifetime, the configuration doesn't take effect.<br><br>**Workaround:** Use a CLI to enter the keychain, or on the user interface, enter both an accept lifetime and a send lifetime. |
| CSCuu65593 | **Symptom:** On fiber-only ports, negotiation is always enabled; however, the show command displays negotiation as disabled. If the link partner's negotiation is disabled, the link might not come up.<br><br>**Workaround:** Verify that the link partner's negotiation is enabled. |
| CSCuu65595 | **Symptom:** MLD Snooping mode on IP v6 inter faces is always (*, G), even if you set the mode to (S, G).<br><br>**Workaround:** There is no workaround |

# Where to Find Support

For current support information, visit the following URLs:

www.cisco.com/c/en/us/support/switches/550x-series-stackable-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/350x-series-stackable-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/350-series-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/250-series-smart-switches/tsd-products-support-series-home.html

www.cisco.com/go/smallbizsupport