Release Notes for SF250, SG250, SF350, SG350/350X/350XG, SF550X, SG550X/ 550XG, SX350X, SX550X Series Switches up to Software Version 2.5.8.12

Introduction

September 2021

Release Notes for SF250, SG250, SF350, SG350/350X/ 350XG, SF550X, SG550X/550XG, SX350X, SX550X Series Switches Software Version 2.5.8.12.

What's New

This section details new features and modifications available on this firmware release.

Last Version to Support SG350XG and SG550XG

Firmware release 2.5.8.12 is the last firmware version to support the SG350XG and SG550XG SKUs (see full list below). The firmware upgrade of these SKUs to future firmware versions of 2.6 or higher will be prohibited and blocked. A stack containing one of these SKUs cannot be upgraded to version 2.6 or higher even if the other units in the stack are of a different type.

If an SG350XG or SG550XG SKU is added to a stack running firmware version 2.6, the unit will shutdown and will not join the stack.

Upgrading the firmware from the previous version 2.5.7.x to version 2.6 or higher is prohibited for ALL SKUs. User must first upgrade the device(s) to version 2.5.8 and only then upgrade to version 2.6 or higher if possible (for SKUs that are not included in the SG350XG and SG550X).

Table 1: Affected SKUs

SKU Name	SKU Description
SG350XG-24F	SG350XG-24F 24-Port 10G SFP+ Stackable Managed Switch
SG350XG-24T	SG350XG-24T 24-Port 10GBase-T Stackable Managed Switch
SG350XG-48T	SG350XG-48T 48-Port 10GBase-T Stackable Managed Switch

SKU Name	SKU Description
SG350XG-2F10	SG350XG-2F10 12-Port 10G Stackable Managed Switch
SG550XG-8F8T	SG550XG-8F8T 16-Port 10G Stackable Managed Switch
SG550XG-24T	SG550XG-24T 24-Port 10GBase-T Stackable Managed Switch
SG550XG-24T	24-Port 10GBase-T Stackable Managed Switch
SG550XG-48T	48-Port 10GBase-T Stackable Managed Switch

Updated Cisco Trusted Core Bundle

Firmware release 2.5.8.12 uses Cisco core bundle dated July 5, 2021.

Downgrade from Version 2.5.7.x and later to Version 2.5.5.x or Earlier

As of version 2.5.7.x, the switch supports an enhanced encryption of AAA user credentials - user credentials are salted and hashed using PBKDF2 based on HMAC-SHA-512 hash. This encryption method is not supported in versions 2.5.5.x (and prior versions), and therefore configuration files containing user credentials cannot be maintained when downgrading to version 2.5.5.x and lower.

Therefore, to preserve switch security – the configuration files are erased when downgrading from version 2.5.7.x and higher to version 2.5.5.x and earlier.

Please make sure to back up the configuration files before a firmware downgrade. Before loading back to device, remove the lines that contained encrypted AAA user credentials. Then downgrade a copy of the config file to the device. Following this procedure, you will be able to login with the default credentials. At this point, update the device with the required credentials and save the configuration.

Downgrade Notes – PoE Chip Version

Boards released from the factory with release 2.4.5.x and further will use an updated PoE chipset - 6920xM version 0x4a02. In addition to this new chipset version, the switches will also support:

- PoE chipsets 6920xM version 0x4b42 (used on boards manufactured using SW version 2.2.8.4 until 2.4.0.x)
- PoE chipset 6920x version 0x4ac2 (used on boards manufactured using SW version 2.1.0.63 to 2.2.7.7).
    - PoE chipset version can be reviewed as part of the “show power inline” command output.
    - Due to the different chipset version support – the following downgrade rules will be applied.
- Non PoE SKUs, and PoE SKUs which use the original PoE chipset (69208 0x4ac2).
    - Will follow the same downgrade rules as the previous versions (basically downgrade is allowed until the first SW versions which are supported by this SKU).
- Sx250 SKUs which support PoE chipset 0x4b42.
    - Downgrade to version 2.2.7 or earlier will be prevented.

- The following Sx250 SKUs - SG250-10P, SG250-26HP/P, SF250-48HP, which supports chipset 0x4a02.
  - Downgrade from 2.4 will be prevented completely.
- The following Sx250 SKUs - SF250-24P, SG250-08HP, SG250-50HP, SG250-50P, SG250X-24P, SG250X-48P, which support chipset 0x4a02.
  - Can downgrade only to version 2.3.5 (the 1st SW version supporting these SKUs).
- Sx350 or Sx550 PoE SKUs supporting chipset 0x4a02 or 0x4b42.
  - Downgrade will be prevented to version 2.2.7 or lower.

Known Issues V2_5_8

Caveats Acknowledged in Release Version 2.5.8.12

Bug ID	Description
CSCvz45955	**Symptom** If a device contains revoked certificates and is upgraded from version 2.5.5.x to 2.5.7.x, the show running firmware will cause device to reboot. Issue was fixed in 2.5.8 release. **Workaround** When upgrading to version 2.5.8.12 from an earlier version revocation entries will be removed and user will need to re-configure then on new version.

Resolved Issues V2_5_8

Caveats Resolved in Release Version 2.5.8.12

Bug ID	Description
CSCvy74466	**Symptom** Cannot access device privilege exed 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.

Bug ID	Description
CSCvz45993	**Symptom** Device GUI cannot load if any interface description includes the word “form”
CSCvz46007	**Symptom** Device will reboot if clicking on JP or CN OLH general information sub items.
CSCvz46020	**Symptom** Device reloads after setting IPv6 tunnel as route destination.
CSCvz46034	**Symptom** Device front panel on web GUI displays abnormally.

Release Notes for SF250, SG250, SF350, SG350/350X/350XG, SF550X, SG550X/ 550XG, SX350X, SX550X Series Switches up to Software Version 2.5.7.85

March 2021

Release Notes for SF250, SG250, SF350, SG350/350X/ 350XG, SF550X, SG550X/550XG, SX350X, SX550X Series Switches Software Version 2.5.7.85

What's New

When upgrading from previous version complexity will be modified to enabled, if not already set.

1.1 Password Complexity

In previous version user could enable or disable the password complexity settings. As of version 2.5.7, to enhance security, the user does not have the option to disable the password complexity setting. The password complexity is supported with 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.

1.2 SSL Cipher Support

For enhanced security the support for 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

1.3 Cipher Support

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

1.4 Cisco/cisco Default Username and Password

In version 2.5.5 user user was forced to change default credentials upon first login, but could still explicitly configure cisco/cisco credentials. As of version 2.5.7 user can no longer configure cisco/cisco as credentials. These credentials are supported only upon factory default and only until 1st user login.

1.5 Password Encryption

In previous version user credentials were saved to config file and displayed using SHA-1 hash algorithm. In current release user 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

When upgrading from previous version to current version the existing password will be “double hashed” with a salt and new hash method. A user requiring access still uses the same password configured in previous version

When downgrading from current version to previous version (Version 2.5.5. or lower) device configuration will be erased to prevent security issues. User will be prompted to confirm this behavior before device reloads.

1.6 SNMPv3 Enhancements

This version removed support for md5 as authentication method and DES as encryption method and added support for SHA-2 based authentication methods (HMAC-SHA-224-128, HMAC-SHA-256-192, HMAC-SHA-384-256 and HMAC-SHA-512-384) and AES-128 encryption method. In case of upgrade from previous version md5 authentication will be replaced with SHA-1 and DES encryption will be replaced with AES-128.

1.7 Self-Signed Certificate Lifetime

To enhance security, the default and supported validity of device self signed certificate have been changes as follows:

- 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

1.8 Update to Port Security Action

In previous releases only the drop (discard) and trap actions were supported for port security if the violating MAC was registered as a Secure MAC on one of the other interfaces on the switch. This was true even if the “shutdown” option was selected for the interface (“port security discard-shutdown”). As of the 2.5.7 release,

the shutdown action is also supported for this type of violation, meaning that if port security action is set to discard it will be applied even if violating MAC address is a secure MAC address on one of the device other interfaces

1.9 CA Manager - Validity of Certificates and Default System Clock

In previous versions a CA certificate installed on device was confirmed as valid if current system date and time was within certificate duration period. The system did not check the source of the system clock. As of the 2.5.7 release the system checks the source of the system clock and a CA Certificates will be confirmed as valid only if system clock was set by one of the following:

- SNTP
- Manually by user (or web browser)

If system clock was not set by one of the above method (default system clock) the certificate will be considered invalid even if system TOD is within certificate duration period.

1.10 Changes to Voice VLAN and Auto Smartport Default Setting

In previous version the default is setting of Voice VLAN and Auto SmartPort was as follows:

- Voice VLAN default administrative state - auto-triggered
- Auto SmartPort default administrative state – controlled

As of version 2.5.7 the default of these features will be as follows:

- Voice VLAN default administrative state - disabled
- Auto SmartPort default administrative state – disabled

The new default settings are applied to device at factory default. Upon upgrade or downgrade from/to the 2.5.5 release, the device will retain the existing value for both settings. This may require change in configuration file (due to the difference in default settings between version)

1.11 PNP Agent – HTTPS Transport Protocol

The 2.5.7 release supports the configuration of HTTPS as 1st choice" transport protocol. The 2.5.5 release supported only HTTP as 1st choice transport protocol.

1.12 PNP Agent – Built in Bundle Support

In Previous version the PNP agent supported download and installation of a CA certificate bundle (trustpool). Bundle could be downloaded via option 43 "T parameter" or via Cisco PnP Connect from the following URL: http://www.cisco.com/security/pki/trs/ios_core.p7b.

The 2.5.7 release added support to a built in bundle, which is included as part of the PNP agent. Built-in certificates are intended to be used as backup in case connection to PNP Connect server is not active. It is always preferable to rely on bundle downloaded from PNP connect as they are more up to date.

1.13 PNP Agent - Certificate CN/SAN Validation Support

In the 2.5.7 release, in addition to validating server certificates using CA certificates, the device will also validate certificates by comparing Server IP address/hostname to the information included in the Certificate's

CN (Common Name) and SAN (Subject Alternative Name) fields. If the CN/SAN validation fails the connection to the PNP server is terminated and the a warning level syslog message and trap is generated.

1.14 Stack Unit Naming

In this release naming convention for stack unit has been changed in CLI, GUI and documentation as follows:

- Stack master unit = Stack Active unit
- Stack Backup unit = Stack Standby unit
- Stack Slave unit = Stack Member unit

1.15 CBD Version Support

The 2.5.7 release supports Cisco Network Probe version 2.2.1.x

1.16 Downgrade Notes – PoE Chip Version

Boards released from the factory with release 2.4.5.x and on will use an updated PoE chipset - 6920xM version 0x4a02. In addition to this new chipset version – devices in the field also support:

- PoE chipsets 6920xM version 0x4b42 (used on boards manufactured using SW version 2.2.8.4 until 2.4.0.x);
- PoE chipset 6920x version 0x4ac2 (used on boards manufactured using SW version 2.1.0.63 to 2.2.7.7).
  - PoE chipset version can be reviewed as part of the “show power inline” command output.
  - Due to the different chipset version support – the following downgrade rules will be applied:
- Non PoE SKUs, and PoE SKUs which use the original PoE chipset (69208 0x4ac2)
  - Will follow the same downgrade rules as previous versions (basically downgrade is allowed until 1st SW versions which supported this SKU)
- Sx250 SKUs which support PoE chipset 0x4b42
  - Downgrade to version 2.2.7 or earlier will be prevented
- The following Sx250 SKUs - SG250-10P, SG250-26HP/P, SF250-48HP, which support chipset 0x4a02
  - Downgrade from 2.4 will be prevented completely
- The following Sx250 SKUs - SF250-24P, SG250-08HP, SG250-50HP, SG250-50P, SG250X-24P, SG250X-48P, which support chipset 0x4a02
  - Can downgrade only to version 2.3.5 (the 1st SW version supporting these SKUs)
- Sx350 or Sx550 PoE SKUs supporting chipset 0x4a02 or 0x4b42
  - Downgrade will be prevented to version 2.2.7 or lower

Known Issues

Caveats Acknowledged in Release Version 2.5.7.85

Bug ID	Description
CSCvx52167	**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.
CSCvx52220	**Symptom** Alert Icon continues to blink even though it was disabled by user. **Workaround** None.
CSCvx52223	**Symptom** On certain devices Egress traffic shaping with value less that CIR = 18M on XG uplink. **Workaround** None

Resolved Issues

Caveats Resolved in Release Version 2.5.7.85

Bug ID	Description
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).

Release Notes for SF250, SG250, SF350, SG350/350X/350XG, SF550X, SG550X/ 550XG, SX350X, SX550X Series Switches up to Software Version 2.5.5.47

May 2020

These Release Notes describe the recommended practices and known issues that apply to software version 2.5.5.47 for the products listed in the following table:

Model	Description	Ports
SF250-24	24-Port 10/100 Smart Switch	fa1-fa24, gi1-gi4
SF250-24P	24-Port Gigabit PoE Smart Switch	fa1-fa48, gi1-gi4
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
SG250-08	8-port Gigabit Smart Switch	gi1-gi8
SG250-08HP	8-port Gigabit PoE Smart Switch	gi1-gi8
SG250-10P	10-Port Gigabit PoE Smart Switch	gi1-gi10
SG250-18	18-port Gigabit Smart Switch	gi1-gi18
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
SG250-50	50-port Gigabit Smart Switch	gi1-gi50
SG250-50HP	50-port Gigabit PoE Smart Switch	gi1-gi50
SG250-50HP	50-Port Gigabit PoE Smart Switch	gi1-gi50
SG250X-24	24-port Gigabit Smart Switch with 10G Uplinks	gi1-gi24, te1-te4
SG250X-24P	24-port Gigabit PoE Smart Switch with 10G Uplinks	gi1-gi24, te1-te4
SG250X-48	48-port Gigabit Smart Switch with 10G Uplinks	gi1-gi48, te1-te4
SG250X-48P	48-port Gigabit PoE Smart Switch with 10G Uplinks	gi1-gi48, te1-te4
SF350-08	8-Port 10/100 Managed Switch	fa1-fa8
SF350-24	24-Port 10/100 Managed Switch	fa1-fa24, gi1-gi4
SF350-24MP	24-Port 10/100 PoE Managed Switch	fa1-fa24, gi1-gi4
SF350-24P	24-Port 10/100 PoE Managed Switch	fa1-fa24, gi1-gi4
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

Model	Description	Ports
SF350-48P	48-Port 10/100 PoE Managed Switch	fa1-fa48, gi1-gi4
SF352-08	8-Port 10/100 Managed Switch	fa1-fa8, gi1-gi2
SF352-08MP	8-Port 10/100 PoE Managed Switch	fa1-fa8, gi1-gi2
SF352-08P	8-Port 10/100 PoE Managed Switch	fa1-fa8, gi1-gi2
SG350-10	10-Port Gigabit Managed Switch	gi1-gi10
SG350-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-10FP	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-20	20-Port Gigabit Managed Switch	gi1-gi10
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
SG350-28SFP	28-Port Gigabit Managed SFP Switch	gi1-gi28
SG350-52	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350-52MP	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350-52P	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350X-12PMV	12-port 5G POE Stackable Managed Switch	fi1-fi12, xg1-xg4
SG350X-24	24-Port Gigabit Stackable Managed Switch	gi1-gi24, te1-te4
SG350X-24PV	24-port 5G POE Stackable Managed Switch	gi1-gi8, gi13-gi20, fi9-fi12, fi21-fi24, xg1-xg4
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

Model	Description	Ports
SG350X-24PD	24-Port 2.5G PoE Stackable Managed Switch	gi1-gi10, gi13-gi22, tw11-tw12, tw23-tw24, te1-te4
SG350X-48	48-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-48PV	48-port 5G POE Stackable Managed Switch	gi1-gi20, gi25- gi44, fi21-fi24, fi45-fi48, xg1-xg4
SG350X-8PMD	8-Port 2.5G PoE Stackable Managed Switch	tw1-tw8, te1-te2
SX350X-08	8-Port 10GBase-T Stackable Managed Switch	te1-te8
SX350X-12	12-Port 10GBase-T Stackable Managed Switch	te1-te12
SX350X-24	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SX350X-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SX350X-52	52-Port 10GBase-T Stackable Managed Switch	te1-te52
SG355-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
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
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

Model	Description	Ports
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-24MMP	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
SX550X-12F	12-Port 10G SFP+ Stackable Managed Switch	te1-te12
SX550X-16FT	16-Port 10G Stackable Managed Switch	te1-te16
SX550X-24	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SX550X-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SX550X-24FT	24-Port 10G Stackable Managed Switch	te1-te24
SX550X-52	52-Port 10GBase-T Stackable Managed Switch	te1-te52
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

Model	Description	Ports
SG550XG-24T	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SG550XG-48T	48-Port 10GBase-T Stackable Managed Switch	te1-te48
SG550XG-8F8T	16-Port 10G Stackable Managed Switch	te1-te16

What's New

Release 2.5.5.47 includes these updates:

FindIT Probe Enhancement

- In previous version, the only setting available to the user was to enable or disable the FindIT probe. The switch that had the probe enabled would have a separate web user interface for the probe functionality. In the current version, additional settings were added to allow the probe on the switch to connect to a remote FindIT Manager. These settings include the Manager address and transport port, the FindIT Organization and the network name, Manager key-ID and secret.

Note The FindIT probe on the switch no longer has its own web user interface. All FindIT management should be done through the web user interface of the FindIT Network Manager.

CA Certificate Manager

- The FindIT and PNP features require CA certificates to establish HTTPS communication with the FindIT or PNP servers. The CA Certificate Management feature allows these applications and the 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. The validity of the certificates is based on the system clock.

Note The validity of the certificates is based on the system clock.

SNTP server for PNP based on DHCP Option 43

- In previous version PNP connection over HTTPS which was based on option 43 would succeed only if system clock was synchronized by the SNTP server specified in DHCP option 43. In current such PNP connection will succeed if system clock was synchronized by any SNTP server or manually set by switch admin.

Downgrade Notes

Boards that are released with the release 2.4.5.x and later use an updated PoE chipset: 6920xM version 0x4a02. In addition to this new chipset version, devices support the following:

- PoE chipset 6920xM version 0x4b42 (used on boards manufactured using software version 2.2.8.4 through 2.4.0.x)
- PoE chipset 6920x version 0x4ac2 (used on boards manufactured using software version 2.1.0.63 through 2.2.7.7)

The PoE chipset version displays as part of the show power inline command output. Due to the different chipset version support, the following downgrade rules apply:

- Non-PoE devices, and PoE devices that use the original PoE chipset (69208 0x4ac2), follow the same downgrade rules as previous versions: downgrade is supported through the first software version that the device supports.
- For Sx250 devices that support PoE chipset 0x4b42, downgrades to software version 2.2.7 or earlier are prevented.
- For SG250-10P, SG250-26HP/P, SF250-48HP devices, which support chipset 0x4a02, downgrading from software release 2.4 is prevented.
- For SF250-24P, SG250-08HP, SG250-50HP, SG250-50P, SG250X-24P, and SG250X-48P devices, which support chipset 0x4a02, you can downgrade only to version 2.3.5 (the first software version that supports these devices).
- For Sx350 or Sx550 PoE devices that support chipset 0x4a02 or 0x4b42, downgrading software version 2.2.7 or lower is prevented.

Known Issues

Caveats Acknowledged in Release Version 2.5.5.47

Bug ID	Description
CSCvu16265	**Symptom** PNP through HTTP fails when attempting to install via FindIT a P12 certificate which includes a certificate chain. **Workaround** Issue will be fixed in next FindIT manager drop. For current version either Use self-signed certificates install in FindIT, or use DHCP option 43 to download certificate bundle.
CSCvu16276	**Symptom** Following stack switchover to backup unit the system does not automatically reconnect to FindIT Manager. **Workaround** Disable and re-enable probe or disable and reenable connection to manger to restart connection to manager. Or reload stack.

Bug ID	Description
CSCvp69075	**Symptom** Config file time stamp is not updated when changing time zone setting. **Workaround** This issue has no functional effect on config file content or behavior and will be fixed in next version.
CSCvu16298	**Symptom** After device reboot the port PoE LED are not shut off even though device LEDs are disabled. **Workaround** None

Resolved Issues

Caveats Resolved in Release Version 2.5.5.47

Bug ID	Description
CSCvn74799	**Symptom** In rare cases, certain NIC connection to 10G interface may cause a link flap every few days. A command was added to allow to tune negotiation with such link partners. Command syntax “ports negotiation tuning”. It is recommended to use command only under circumstances where such link flap occurs on 10G interfaces. See more details in CLI guide.
CSCvo49699	**Symptom** In some cases device may reboot if a specific link in a LAG flaps (reboot message “PSET-FILLEGAL_IFINDEX:PSETG_add_port_to_set: Illegal ifIndex 0”).
CSCvq71611	**Symptom** LLDP advertisement by some Avaya IP phones may cause device to reboot (reboot message: “Msg:%AUTOSMARTPORT-F- DEV_CALC_FAILED: XDP device type calculation failed: interface gi1/0/40 - capability 3”).
CSCvp64740	**Symptom** Upon HTTP or HTTPS timeout web GUI does not automatically redirect user to login page. Automatic redirection works once browsing to any webpage following HTTP/HTTPS timeout.
CSCvr01301	**Symptom** In some cases the switch may stop passing PVST/RPVS+ BPDUs for a VLAN which may cause an STP loop.

Bug ID	Description
CSCvp40307	**Symptom** Cisco Plug and Play connect – discovery of server Ipv4 adress will faile if both Ipv4 and IPv6 DNS records are received. Make sure that there is no default IPv6 route.
CSCvp64778	**Symptom** Even the trunk port is not a member of a vlan, port RPVST status still indicates this vlan is active. This is a display issue, no real impact on functionality.
CSCvs51601	**Symptom** After http(s) session timeout, the WEB GUI does not go back to login page automatically Browse any web pages, it goes back to login page.

Release Notes for SF250, SG250, SF350, SG350/350X/ 350XG, SF550X, SG550X/550XG, SX350X, SX550X Series Switches Software Version 2.5.0.90

November 2019

Release Notes for SF250, SG250, SF350, SG350/350X/ 350XG, SF550X, SG550X/550XG, SX350X, SX550X Series Switches Software Version 2.5.0.90

What's New

This section details new features and modifications in release 2.5.0.92

- The output of the show system command now displays the temperature of a single sensor per each unit in stack, even if a board supports multiple sensors. This output shows information from the sensor that detected the highest temperature. In previous versions, the output of this command displayed the temperature of a specified sensor on each unit in stack. The updated functionality can improve your ability to detect potential issues with the temperature on a switch. To see temperature readings for all sensors, use the show system sensors command, which also displays additional details for each sensor such as sensor location and alert thresholds.

Release 2.5.0.90 provides fixes for the bugs that are listed in the Resolved section below.

Release 2.5.0.83 provides fixes for the bugs CSCvo48821 and CSCvp12473.

Release 2.5.0.82 provides a fix for the bug CSCvp95489.

Release 2.5.0.79 includes these updates:

- Mgig 5G interface support—This release adds support for the SG350X12PMV, SG350X-24PV, and SG350X-48PV switch models, which include multi-gigabit (Mgig) RJ45 copper ports. These switches add support for 5G interfaces, which support 100M/1G/2.5/5Gbps speeds. Mgig ports negotiation is based on 2.5G/5Gbase-T IEEE 802.3bz-2016 and is fully compliant to NBASE-T final spec (version 2.3). The Mgig ports location depends on the switch model. As in previous versions, an interface that supports Mgig is named after its maximum port speed. The interface that supports a maximum speed of 5G is named “FiveGigabitEthernet1/0/1,” or “fi 1/0/1” for short. As with 2.5G interfaces in previous

releases, the numbering of the 5G interfaces is sequential with the 1G interfaces. For example, if the 5G ports were located physically on the seventh and eighth ports, they would be named “tw 1/0/7” and “tw1/0/8.”

- Enhanced security—To enhance device management security, this release introduces the following:
  - After you complete the initial connection to a device by logging in with the default user name cisco and the default password cisco, the system requires you to change the user name and password. In previous releases, you were asked to change only the password and could choose to skip the password change process.
  - Note: Default credentials replacement is also enforced when upgrading from a previous release to this release, if the startup configuration in the previous release does not include level 15 credentials.
  - If you disable password complexity, you can configure the user name cisco and the password cisco as your log in credentials. If you save these credentials to startup, you are not prompted to change the credentials.
  - The cisco/cisco credentials appear in the device configuration file. In previous releases, the cisco/cisco default credentials did not appear in configuration file.
  - You cannot remove or delete the last privilege level 15 default username and password. This functionality prevents you from reverting (possibly without intention) to the default cisco/cisco credentials. In previous releases, you could remove last level 15 user, and in this case cisco/ cisco credentials became active.
  - Deleting device configuration or rebooting a device to factory default restores the default login credentials. In this case, you will need to change the credentials again.
- Runtime defense features include operating system, compiler, and processor features to protect the systems from hacking. The device supports the following related features:
  - X-SPACE—protects the running of unauthorized applications by preventing code from running if it is located in unauthorized memory areas, for example, in a data segment.
  - ASLR—Randomizes the addresses used by the operating system (Linux) for running applications and processes. Each time a process runs, the operating system uses a different address for the process, making it harder for hackers to gain execution permission for their own code.
  - BOSC—Adds protection from buffer overflow (code that tries to access memory that is out of its own memory)
- The following PnP feature support were added to the existing PnP agent behavior:
  - This version supports Cisco Plug and Play connect, which allows full out-of-the-box PNP server discovery that runs over HTTPS. The switch contacts the redirection service using the FQDN devicehelper.cisco.com and then obtains PNP server information from it.
  - Certificate handling (SSL client)/ HTTPS as first choice via DHCP and Cisco Plug and Play connect methods.
  - Downloading of an image and configuration file is protected by MD5 checksum, which is added by the PNP server and validated by the switch.
- The PNP agent and DHCP auto config and image features can now be enabled simultaneously, and both features are enabled by default. If a switch receives a DHCP reply with a PNP agent related option (option

43) and DHCP auto update related options (either options 57 or 125), the switch ignores the PNP agent option information.

- By default, VLAN Mapping Tunneling edge ports drop on ingress L2 PDUs that have the following destination MAC addresses:
  - 01:80:C2:00:00:00-01:80:C2:00:00:FF
  - 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
  - 01:00:0C:CD:CD:D0

  In previous versions, you could not forward frames that had these destination MAC addresses. In this version, you can define a specific port to forward PDUs in any of the following protocols: CDP, LLDP, STP or VPT. (Before the PDUs are forwarded, you must specify a VLAN tag for them.) This functionality allows the forwarding of such untagged frame over the provider network. You also can assign a specific CoS value to such packets and set a threshold rate.
- In addition to STP, RSTP, and MSTP, the device supports PVST+ and RPVST+. PVST+ and /RPVST+ run in separate instances of the 802.1Q STP per VLAN. Rapid PVST runs in a separate instance of the 802.1Q RSTP per VLAN. The device supports up to 126 PVST/RPVST instances
- The trunk port VLAN membership command line syntax has been enhanced to support the option of specifying the allowed VLAN list, in addition to adding and removing. The configuration file also has been enhanced to display the allowed VLAN list instead of the removed VLAN list. The configuration is migrated automatically when upgrading or downgrading.

Known Issues

Caveats Acknowledged in Release Version 2.5.0.92

Bug ID	Description
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.
CSCvs51601	**Symptom** After http(s) session timeout, WEB GUI does not go back to login page automatically. **Workaround** Browse to another web page, select a control such as Edit or Apply on the existing page, or re-enter the device URL in your browser menu bar and you will be redirected to the login page.

Caveats Acknowledged in Release Version 2.5.0.92

Bug ID	Description
CSCvr54104	**Symptom** In some cases FindiT Probe GUI will not work across subnets if connected router sends switch ICMP redirect messages for gateway address. This issue was found when connected RV325 router. **Workaround** Configure router not to send ICMP redirect messages to device. If redirect messages are required on the network, use ACL on device interfaces to block redirect messages.

Caveats Acknowledged in Release Version 2.5.0.79

Bug ID	Description
CSCvp64751	**Symptom** Stack with master and backup cannot be downgraded to version 2.2.5 (or lower) and then upgraded back to version 2.5. **Workaround** Option 1 (use before downgrading is initiated): Delete startup configuration on version 2.5 and then downgrade to version 2.2.5. Option 2 (use if downgrade was already preformed but before upgrading back to 2.5): After downgrading, disconnect the backup unit and then delete the backup unit startup configuration. Reboot the master and backup units, and reconnect the backup unit to the master unit.
CSCvp64768	**Symptom** Loopback detection is triggered when PVST/ RPVST is enable, even though it should not be. **Workaround** Do not enable Loopback detection with PVST/ RVPST.
CSCvp64778	**Symptom** Even if the trunk port is not a member of a VLAN, port RPVST status indicates this VLAN is active. **Workaround** Display issue, no real affect on functionality.

Caveats Acknowledged in Release Version 2.5.0.78

Bug ID	Description
CSCvp40302	**Symptom** Loopback detection is triggered when PVST/ RVPST is enabled, even though it should not be. **Workaround** Do not enable Loopback detection with PVST/RVPST.
CSCvp40307	**Symptom** Cisco Plug and Play connect—discovery of server IPv4 address fails if both Ipv4 and IPv6 DNS records are received. **Workaround** Configure only IPv4 records on the DNS server
CSCvp40311	**Symptom** The cable-diagnostics tdr always displays “short cable” on 10G ports. **Workaround** None.
CSCvp40317	**Symptom** PSE port connected to specific NICs (not PD device) displays status of “Short” condition. **Workaround** None.

Caveats Acknowledged in Release Version 2.5.0.71

Bug ID	Description
CSCvn31532	**Symptom** In some cases, an image upgrade fails when upgrading the image simultaneously to a few devices by using the FindIT Network Probe. **Workaround** Wait for the download for each switch to end before upgrading the next switch.

Bug ID	Description
CSCvn31587	**Symptom** If HTTPS is disabled on a device, you cannot connect to the FindIT Network Probe application from the log in page; relevant for switches on which FindIT Network Probe is enabled. You still can connect to the probe by accessing regular Switch Management from the Login page, and then clicking the FindIT link at the top of the page. **Workaround** Enable HTTPS. **Note** This bug is resolved in software version 2.5.0.92.
CSCvn31596	**Symptom** FindIT Network Manager fails to cross-launch to a switch on which HTTPS is disabled. **Workaround** Enable HTTPS.
CSCvn31554	**Symptom** When changing a device IP address from a DHCP to a static IP address, Bonjour broadcasts sent by the switch may contain old IP address information. A new device IP address with a short netmask (less than 20 bits) will not be updated on FindIT Network Probe. **Workaround** Reboot the device with the changed IP address.

Caveats Acknowledged in Release Version 2.4.0.94 and 2.4.0.91

Bug ID	Description
CSCvj32368	**Symptom** When using the show green-ethernet command, the display of Power Savings % as a result of short reach setting is not accurate. **Workaround** None. **Note** This bug is resolved in software version 2.5.0.92.

Bug ID	Description
CSCvj32379	**Symptom** On some SKUs, fan RPM (Rounds Per Minutes) is displayed as “0” when issuing the show fans system CLI command. Fan functionality is not affected. **Workaround** None
CSCvj32418	**Symptom** In rare scenarios (adding 700 certain IPv6 routes), hardware routing is disabled even though the resource table is not full. **Workaround** Configure fewer or different IPv6 routes. If the issue still occurs, reduce some routes that are not needed and reactivate hardware based routing.
CSCvj32432	**Symptom** Sx550x in hybrid stack mode supports 2,000 Layer 2 Multicast entries (should support 4,000). **Workaround** Use native mode if possible. **Note** This bug is resolved in software version 2.4.5.71.
CSCvj32442	**Symptom** The Show inventory command displays wrong information or format of PID and vid = “information not available” for the following SFPs: MFEFX1, MFELX1, MFEBX1, MFEBBX1, MFEBSX1, MFELH1, MFELX1 and MGBT1. This issue affects the display and has no functional effect. **Workaround** None.
CSCvj32448	**Symptom** : In some cases, a fiber link flaps when connecting a SFP MGBLX1 and a 40km fiber cable to some SFP ports. Eventually the link may go down due to link flap prevention. **Workaround** None.

Bug ID	Description
CSCvj32452	**Symptom** As of 2.4.0.x, TCP or UDP port range option is not supported in IPv6 ACL and you must use specific ports in ACE configuration. **Workaround** After upgrading to 2.4.0.x, ACEs with range configuration are removed from ACL and you must reconfigure specific ports of IPv6 ACL.

Caveats Acknowledged in Release Version 2.3.5.63

Bug ID	Description
CSCvf88706	**Symptom** When connecting an additional unit to an existing stack of 3 units, PoE info for unit 1 is not displayed in CLI or GUI. **Workaround** Reboot the stack. **Note** This bug is resolved in software version 2.4.0.91.
CSCvf88738	**Symptom** Port is suspended (shutdown) when unbinding a specific ACL from port under traffic if the ACL includes a deny ACE with a “disable-port” option. **Workaround** Shutdown then no shutdown the port to recover. **Note** This bug is resolved in software version 2.4.0.91.
CSCvf88746	**Symptom** SNA connection to switch is disconnected following switch reboot after upgrade of switch to a new firmware version. **Workaround** Refresh browser to reconnect to switch.
CSCvf88761	**Symptom** Enable Ipv6 routing first then configure an Ipv6 6to4 tunnel, tunnel status is “not present.” **Workaround** Disable then enable Ipv6 routing or configure the tunnel first then enable Ipv6 routing. **Note** This bug is resolved in software version 2.4.0.91.

Bug ID	Description
CSCvf88777	**Symptom** SSH connection is slow when connecting from one switch (SSH client) to another switch (SSH server) . **Workaround** None. **Note** This bug is resolved in software version 2.4.0.91.
CSCvf88810	**Symptom** Non-combo SFP ports will not support 100M SFP module. **Workaround** None.

Caveats Acknowledged in Release Version 2.3.0.130

CSCve55065	**Symptom** 6to4 tunnel traffic is not forwarded in line rate when the tunnel outgoing port is trunk or general tagged. **Workaround** Configure tunnel outgoing port as access or no switch port. **Note** This bug is resolved in software version 2.4.0.91.
CSCve55069	**Symptom** : Some functions in the web GUI not response when using the Apple Safari browser: reboot button, logout, Stop button of Locate Device. **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. **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). **Workaround** None. **Note** This bug is resolved in software version 2.4.0.91.
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.. **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. **Note** This bug is resolved in software version 2.3.5.63.
CSCve55078	**Symptom** Egress traffic shaping on XG device uplink interfaces limits traffic to 80 Kbps, even if you configured a lower rate. **Workaround** Use an egress shaping value higher than 80 Kbps. **Note** This bug is resolved in software version 2.4.0.91.
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. **Workaround** None.
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 **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). **Workaround** Reload the unit. **Note** This bug is resolved in software version 2.3.5.63.
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. **Workaround** Refresh web page.
CSCve55094	**Symptom** Queue statistics: packet size is calculated based on the packet size on ingress, although statistics are egress statistics. **Workaround** None.
CSCve55102	**Symptom** PoE: In rare cases, the voltage display for ports connected to PD, is lower than actual voltage. **Workaround** None.
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 poepse inventory.” **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. **Workaround** None.

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. **Workaround** None.
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. **Workaround** None.
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. **Workaround** None.
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. **Workaround** Disconnect and then reconnect the “stuck” unit from the power source to re-add it to the stack. **Note** This bug is resolved in software version 2.3.5.63.

Caveats Acknowledged in Release Version 2.2.8.04

Bug ID	Description
CSCvc73697	**Symptom** Learned voice VLAN greater than 1024 flush existing VLAN. **Workaround** None. **Note** This bug is resolved in software version 2.3.0.130.

Caveats Acknowledged in Release 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). **Workaround** None. **Note** 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. **Workaround** Refresh the SNA display.
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. **Workaround** Remove all manual DAC related settings (802.1x/RADIUS) from the device before using the DAC feature. **Note** 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. **Workaround** None.
CSCva97588	**Symptom** : SNA—When logging in to a device with an IPv6 address using Win10 Edge, cannot view network topology **Workaround** Use an IPv4 address or other browsers to connect. **Note** This bug is resolved in software version 2.3.0.130.

Bug ID	Description
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. **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. **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. **Workaround** Perform a shutdown/no shutdown on the physical interface. **Note** This bug is resolved in software version 2.4.0.91.
CSCva97605	**Symptom** Upgrading boards running version 2.2.0.x to version 2.2.5.x is not possible via XMODEM. **Workaround** Use TFTP for upgrading from version 2.2.0.x to version 2.2.5.x.

Caveats Acknowledged in Release Version 2.2.0.63

Bug ID	Description
CSCuy97777	**Symptom** After reload, the actual spanning tree cost of portchannel is different with running-config. **Workaround** None. **Note** This bug is resolved in software version 2.2.5.

Bug ID	Description
CSCuy97791	**Symptom** When STP cost path is equal, Port channel is always selected as root port even if it has a higher priority value. **Workaround** STP still functions properly and no loops are created. If needed, use cost setting to change the root port. **Note** 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. **Workaround** None. **Note** This bug is resolved in software version 2.2.5
CSCuz01765	**Symptom** Some revisions of the Cisco IP Phone 7960 cannot be powered up on switch 60W ports. **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. **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. **Workaround** Occurs only if stack units are reloaded twice. Stack stabilizes following master reload. **Note** This bug is resolved in software version 2.2.5.

Bug ID	Description
CSCuy97946	**Symptom** DHCPv6 relay does not work if destination is set 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 **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. **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. **Note** This bug is resolved in software version 2.2.5.

Caveats Acknowledged in Release 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. **Workaround** Use CDP to negotiate. **Note** 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. **Workaround** None.

Bug ID	Description
CSCux77654	**Symptom** Egress ACL cannot be applied to and interface if ACE includes TCP/UDP port range as a parameter. **Workaround** Apply required TCP/UDP ports as individual ports in ACL, or apply a range as ingress ACL on relevant interfaces. **Note** 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. **Workaround** None. **Note** 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. **Workaround** None. **Note** This bug is resolved in software version 2.2.0.
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. **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. **Workaround** None.

Bug ID	Description
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. **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. **Note** This bug is resolved in software version 2.5.0.90.
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. **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. **Note** 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. **Workaround** Manually set a limit of 60 watts if needed.
CSCux89611	**Symptom** Power negotiation for 60W PoE via LLDP may take up to 1 minute to complete. **Workaround** None.
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. **Workaround** None.

Caveats Acknowledged in Release 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. **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. **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.
CSCuu60952	**Symptom** When changing an ACE action using the configuration interface, (for example, from deny to shutdown) ACE may be removed from the ACL. **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 webbased configuration interface, creation of new ACE may fail with an error message of “Entry Already Exists,” even though it does not exist. **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. **Workaround** If VRRP is enabled on device, use DHCP relay without activating Option 82.

Bug ID	Description
CSCuu60986	**Symptom** When enabling flow control on the LAG using the user interface, the port LEDs will not light even if link is up. **Workaround** This bug is a LED display issue. The functions work as expected. If needed, enable flow control using the command line interface. **Note** This bug is resolved in software version 2.2.0.
CSCuu60989 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). **Workaround** Change the port VLAN membership that use switchport modes so that the port is not a static member in the desired VLAN. **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. This bug is resolved in software version 2.2.5.
CSCuu61008	**Symptom** Agreed Auto Voice VLAN cannot be defined as a primary VLAN, even after the voice VLAN is disabled. **Workaround** None.
CSCuu61061	**Symptom** If short reach is enabled on a port, the cable length test using a Cat6a cable fails. **Workaround** Disable short reach when running the cable length test on an interface. **Note** This bug is resolved in software version 2.2.5.

Bug ID	Description
CSCuu61080	**Symptom** DHCP router option (Option 3) is sent by the switch DHCP server, even if the option is not configured for this pool. **Workaround** None. **Note** This bug is resolved in software version 2.2.0.
CSCuu61084	**Symptom** IPv6 Routes always display a metric value of “0. **Workaround** None. **Note** 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. **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. **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). **Workaround** This bug is a display issue only.
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.

Bug ID	Description
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).
CSCuu65577	**Symptom** When using the web-based configuration interface to set a new keychain for RIP, include an acceptlifetime. If you don't include an accept-lifetime, the configuration doesn't take effect. **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 **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) **Workaround** None.

Resolved Issues

Caveats Resolved in Release Version 2.5.0.92

Bug ID	Description
CSCvr54104	**Symptom** Cisco Small Business Switches Information Disclosure Vulnerability.
CSCvo48821	**Symptom** SNMP Get for the specific OIDs cause the exception.
CSCvp12473	**Symptom** Intermittent connectivity in the 10G link between SG550XG and SG250X.

Caveats Resolved in Release Version 2.5.0.90

Bug ID	Description
CSCux89582 S	**Symptom** Interface will be suspended (down) if 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.
CSCvo26128	**Symptom** In some cases device may reboot when clearing IPv6 DHCP relay entries.
CSCvo48776	**Symptom** Port is suspended due to link flapping when using MGBT1 SFP with no cable. The issue is partially fixed with a limitation—if an RPS is connected to SG550XG series, link will still be suspended. In this case, insert SFP only together with cable.
CSCvp64736	**Symptom** Slave units in stack may reload, due to UDLD operation, under extreme conditions of traffic and perpetual link flapping.
CSCvq51790	**Symptom** Port 49/50 LEDs turn on when administratively shutdown, and turn off when administrative no shutdown.
CSCvq62235	**Symptom** Stack will reboot with fatal error when using FHS (First Hop Security) feature and LAGs (reboot syslog - SYSLOGF-OSFATAL: SW3P_pcl_vll_FHS_verify_reservations_of_all_units: Reservations for unit does not match the needed amount).
CSCvq31960	**Symptom** Device is vulnerable to TCP SACK (Selective ACK) vulnerabilities.
CSCvq02158	**Symptom** Unwanted software component detected on device: tcpdump
CSCvq02165	**Symptom** Unwanted software component detected on device: GNU Debugger (gdbserver).
CSCvp35677, CSCvp35688, CSCvo26471, CSCvo28159	**Symptom** “Cisco Small Business Switches CSRF Vulnerability.”
CSCvq02187	**Symptom** Switches include hardcoded password hashes.

Caveats Resolved in Release Version 2.5.0.82

Bug ID	Description
CSCvp95489	**Symptom** SG550X-48MP: Updating to 2.5.0.7x causes reboot loop with hardware version 2.

Caveats Resolved in Release Version 2.5.0.78

Bug ID	Description
CSCvn80396	**Symptom** sFlow is not working with IPv6, when using default IPv4 address.
CSCvn31587	**Symptom** If HTTPS is disabled on a device, you cannot connect to the FindIT Network Probe application from the log in page; relevant for switches on which FindIT Network Probe is enabled. You still can connect to the probe by accessing regular Switch Management from the Login page, and then clicking the FindIT link at the top of the page.
CSCvj32368	**Symptom** When using the show green-ethernet command, the display of Power Savings % as a result of short reach setting is not accurate.
CSCvp40263	**Symptom** DHCP server will keep offering the first decline address if there is no free address.
CSCvp40272	**Symptom** Default ARP timeout keeps 60000 seconds if IP Routing is disabled (but it should be 300 seconds in such case).
CSCvm76475	**Symptom** Some MIBs (ifOutDiscards 1.3.6.1.2.1.2.2.1.19) returns NULL value with Cisco Prime.
CSCvn49346	**Symptom** DOS: SNMP walking for pacific OID cause device to reboot.
CSCvi71623	**Symptom** Pacific Avaya phone LLDP crashes the switch.

Caveats Resolved in Release Version 2.5.0.71

Bug ID	Description
CSCvj32448	**Symptom** In some cases, a fiber link flaps when connecting a SFP MGBLX1 and a 40km fiber cable to some SFP ports. Eventually the link may go down due to link flap prevention.
CSCvj32432	**Symptom** Sx550x in hybrid stack mode supports 2,000 Layer 2 Multicast entries (should support 4,000).
CSCvg69635/ CSCvb96602	**Symptom** A device sometimes reboots when OOB interface is connected to network with the error message "%2SWPORTF-Failed2ConvertPort: SW2C_port_get_customer - failed to validate ifIndex -1 relativeIf -1."
CSCvj23510	**Symptom** VLAN membership on a trunk mode port is removed if the port native VLAN is not VLAN 1, the port is not a member of all VLANs, and configuration is downloaded and then copied back to the startup configuration.
CSCvk06454	**Symptom** Device supports TLS_RSA_WITH_SEED_CBC_SHA weak Cipher suite.
CSCvm20300	**Symptom** Device may reload when receiving certain DNS replies in which the DNS responses requested and received IP type (ipv6/ipv4) do not correlate.
CSCvk75871	**Symptom** Copying and pasting multiple CLI commands to a console via SSH causes device management to get stuck.
CSCvi65951	**Symptom** Packets flood on port-channel (LAG) when the MAC table timeout counter reaches twice its aging time.

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	

Cisco Business	
Cisco Business 350 Managed Series Switches	http://www.cisco.com/c/en/us/support/switches/350-series-managed-switches/tsd-products-support-series-home.html
Cisco Business 350x Series Stackable Managed Switches	http://www.cisco.com/c/en/us/support/switches/350x-series-stackable-managed-switches/tsd-products-support-series-home.html
Cisco Business 550x Series Stackable Managed Switches	http://www.cisco.com/c/en/us/support/switches/550x-series-stackable-managed-switches/tsd-products-support-series-home.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.