SSL Appliance Release Notes

Version 3.8.6
First Published: 6/1/16

Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation instructions for the Cisco SSL 1500, 2000, and 8200 appliances.

For detailed information on the Cisco SSL Appliance, refer to the online help or download the *Cisco SSL Appliance 1500 Administration & Deployment Guide, Cisco SSL Appliance 1500 Administration & Deployment Guide, Cisco SSL Appliance 2000 and 8200 Administration & Deployment Guide, Cisco SSL Appliance 1500 Getting Started Guide,* or *Cisco SSL Appliance 2000 and 8200 Getting Started Guide* from the Support site or Cisco.com.

These release notes are valid for Version 3.8.6 of the Cisco SSL Appliance. You can update appliances running at least Version 3.6.3 or at least Version 3.7.1 of the Cisco SSL Appliance to Version 3.8.5.

For more information, see the following sections:

Upgrading Cisco SSL Appliance

This section provides instructions for upgrading your appliance. Make sure to follow the instructions for the version you are currently running. Upgrades are supported for:

- 3.6.3
- 3.7.x up to and including 3.7.4-41

Cisco Systems, Inc.
www.cisco.com

- 3.8.2 up to and including 3.8.2-424
- 3.8.3 up to and including 3.8.3-126
- 3.8.4 up to and including 3.8.4-26
- 3.8.5 up to and including 3.8.5-19

Terminology

- .p7b: PKCS#7 encoded external certificate file; updates the list of external CA certificates.
- .patch: Updates the main partition; includes only the changes from one version to the next, all data and configurations are retained, applied through the WebUI.
- .nru: Replaces the existing rescue image with the new image; all data and configurations are retained, applied through the WebUI.
- .nsu: System update file; replaces the active image, re-images the rescue partition, triggers restore factory defaults, retains management IP address; all existing data and configurations are wiped, applied through the console.

Files associated with this release:

- sslv-3.6-to-3.8.6-4-cisco.patch
- sslv-3.8.6-4-cisco.iso
- sslv-3.8.6-4-cisco.nru
- sslv-3.8.6-4-cisco.nsu
- sslv-3.8.6-4-cisco.patch
- sslsessions-1.6.2.zip
- ssldiags-1.1.0.zip
- sslv-3.8.6-p7b_certificates-and-SNMP_MIBS.zip
  - sslv_3.6.3_to_3.8.0_ca_certificates.p7b
  - sslv_3.7.0_to_3.8.0_ca_certificates.p7b
  - sslv_3.8.0_to_3.8.3_ca_certificates.p7b
  - MIBS_SSLV-3.8.3.zip
  - CHECKSUMS.txt
  - README.txt

Note sslv-3.8.6-p7b_certificates-and-SNMP_MIBS.zip contains sslv_3.6.3_to_3.8.0_ca_certificates.p7b, sslv_3.7.0_to_3.8.0_ca_certificates.p7b, sslv_3.8.0_to_3.8.3_ca_certificates.p7b, MIBS_SSLV-3.8.3.zip, and README.txt. Do not download these files individually.

Upgrade the Appliance

If the appliance is running 3.7.0 or greater, upgrade using the **sslv-3.8.6-4-cisco.patch**, see Upgrade from 3.7.x or Later to 3.8.6, page 3.

If the appliance is running 3.6.3, a two step upgrade process is required, as described in Upgrading the Cisco SSL Appliance from Version 3.6.3 to 3.8.6, page 4.

The patch mechanism will not update the rescue image in the system. Hence, if you use the Restore factory defaults option, the appliance will be re-imaged with the version of the rescue image. You must re-apply the patch.

Following the patch upgrade, Cisco recommends you upgrade the rescue image to the latest software version by applying the related .nru (for example, **sslv-3.8.6-4-cisco.nru**).

Upgrade from 3.7.x or Later to 3.8.6

Upgrading the SSL Appliance to a new software version is straightforward. Make sure the appliance is running software version 3.7.x or later; if it is running software version 3.6.3 see Upgrading the Cisco SSL Appliance from Version 3.6.3 to 3.8.6, page 4

Apply a Patch

To apply the patch, access the **(Platform Management) > Update menu** option on the WebUI, select the **sslv-3.8.6-4-cisco.patch** file, and click OK.

The patch upgrade preserves your existing configuration data and existing logs.

Apply the NRU

To apply the .nru file which will update the rescue image, access the **(Platform Management) > Update** menu option on the WebUI, select the **sslv-3.8.6-4-cisco.nru** file, and click OK.

The existing rescue image will be replaced with the new image.

Tip As a precaution, back up all configuration and policy data before the upgrade.

Patch Upgrade Procedure

Step 1 Access the (Platform Management) > Update menu.

Step 2 Click Choose File to select the patch upgrade file, then click OK.

Step 3 Reboot the appliance when prompted.

Step 4 Wait for the upgrade to complete. This might take several minutes, and involves the appliance rebooting a number of times.

Step 5 Update the list of external CA certificates.

3.8.x Process: To import the PKCS#7 encoded external CA certificate file (such as **sslv-3.8.0_to_3.8.3_ca_certificates.p7b**), follow this procedure.

- Go to the **PKI > External Certificate Authorities Lists** window, click **Add** to browse to the file, then click OK. You will see a "Upload Successful" message.

- On the bottom of the **External Certificate Authorities Lists** window, click **Apply** next to the **PKI Changes** message.

After a 3.8.x upgrade, the list of external CA certificates does not include the CA certificates provided with the 3.8.x release. Without the new list of external CA certificates, the X.509 status for some sites (for example, www.google.com) is "Invalid Issuer." Import the **sslv-3.8.0_to_3.8.3_ca_certificates.p7b** file to update the external CA list.

3.7.x Process: To import the SSL Appliance 3.7 PKCS#7 encoded external CA certificate file (**sslv_3.7.0_to_3.8.0_ca_certificates.p7b**), follow this procedure.

- Go to the **PKI > External Certificate Authorites Lists** window, click Add to browse to the file, then click OK. You will see a "Upload Successful" message.
- On the bottom of the **External Certificate Authorties Lists** window, click **Apply** next to the **PKI Changes** message.
- Use the same process to import the 3.8 external CA file (**sslv-3.8.0_to_3.8.3_ca_certificates.p7b**).

After a 3.7.x to 3.8.x upgrade, the list of external CA certificates does not include the CA certificates provided with the 3.8.x release. Without the new lists of external CA certificates, the X.509 status for some sites (for example, www.google.com) is "Invalid Issuer." Import the ca_certificates.p7b file to update the external CA list.

3.6.3 Process: To import the SSL Appliance 3.6.3 PKCS#7 encoded external CA certificate file (**sslv_3.8.0_to_3.8.3_ca_certificates.p7b**), follow this procedure.

- Go to the **PKI > External Certificate Authorites Lists** window, click Add to browse to the file, then click OK. You will see a "Upload Successful" message.
- On the bottom of the **External Certificate Authorties Lists** window, click **Apply** next to the **PKI Changes** message.
- Use the same process to import the 3.8 external CA file (**sslv-3.8.0_to_3.8.3_ca_certificates.p7b**).

After a 3.6.3 to 3.8.x upgrade, the list of external CA certificates does not include the CA certificates provided with the 3.8.x release. Without the new lists of external CA certificates, the X.509 status for some sites (for example, www.google.com) is "Invalid Issuer." Import the ca_certificates.p7b file to update the external CA list.

Back up the PKI store after importing the CA certificates. The system log contains many warnings about duplicate entries; these log entries can be safely ignored.

Upgrading the Cisco SSL Appliance from Version 3.6.3 to 3.8.6

Before You Begin:

- Make sure the appliance is running software version 3.6.3; upgrade the unit to 3.6.3 if it is running older software.
- As a precaution, back up all configuration and policy data before the upgrade.
- Have an account with the Manage Application authentication role configured on the appliance

When you are ready to proceed:

Step 1 Access the (Platform Management) > Update menu.

Step 2 Use the Choose File button to select the sslv-3.6-to-3.8.6-4-cisco.patch, then press OK.

Step 3 Reboot the appliance when prompted.

Step 4 Wait for the upgrade to complete. This may take several minutes, and involves the appliance rebooting a number of times.

Step 5 Import the PKCS#7 encoded external CA certificate file (such as sslv_3.6.3_to_3.8.0_ca_certificates.p7b.) After a 3.6.x to 3.8.6 upgrade, the list of external CA certificates will not include the CA certificates provided with the 3.7.x and 3.8.x releases. Without the new list of external CA certificates, the X.509 status for some sites will be "Invalid Issuer." The sslv_3.6.3_to_3.8.0_ca_certificates.p7b file should be imported to update the external CA list.

Note Be sure to backup the PKI store after importing the CA certificates. Note that the system log may have many warnings about duplicate entries; these log entries can be safely ignored.

Downgrading the Cisco SSL Appliance

In the unlikely event you want to downgrade from 3.7, contact Customer Support for assistance.

Changes

The following sections list the changes in the Version 3.8.6 update.

Features in Version 3.8.6

- SSL Appliance Host Categorization Database Update: The Blue Coat Global Intelligence Network that maintains the Cloud services responsible for servicing the Host Categorization functionality on SSL Visibility appliances will be upgrading their root certificate on February 2, 2016, as the previous certificate is due to expire then. The SSL Appliance 3.8.6 release installs the new certificate required to access the Global Intelligence Network services. Following an upgrade to SSL Appliance 3.8.6, the Host Categorization functionality on SSL Appliances will continue to operate without issue and upgraded appliances will be able to update the Host Categorization database.
- Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.8.6-12. Management Center 1.4.1.1 or earlier is not sup- ported.
- Cisco SSL Appliance 3.8.6 implements IF-MIB ifXTable support for 64-bit SNMP interface octet and packet counters. The following new counters are supported.
  - `64-bit Counter=`
  - `ifHCInOctets`
  - `ifHCInUcastPkts`
  - `ifHCInMulticastPkts`
  - `ifHCInBroadcastPkts`
  - `ifHCOutOctets`
  - `ifHCOutUcastPkts`
  - `ifHCOutMulticastPkts`
  - `ifHCOutBroadcastPkts`

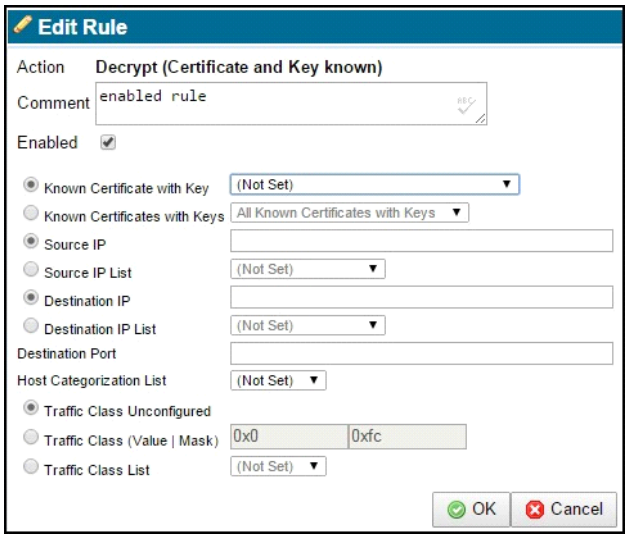
- Version 1.6.2 of the off-box Python SSL Sessions tool is available. Version 1.6.2 supports data export in space-delimited format, for use with Blue Coat Reporter. Use the SSL Sessions tool to parse SSL session log information within an exported session log generated by a Cisco SSL Appliance. The tool and tool documentation (`sslsessions.pdf`) are available on `cisco.com`. A Getting Started Guide is also available.
- Version 1.1.0 of the off-box Python SSL Diagnostics tool is available. Version 1.1.0 supports data export in space-delimited format, for use with Blue Coat Reporter. Use the SSL Diagnostics tool to parse statistics within a diagnostic package collected by a Cisco SSL Appliance. The tool and tool documentation (`ssldiags.pdf`) are available on `cisco.com/`. A Getting Started Guide is also available.

Features in Version 3.8.5

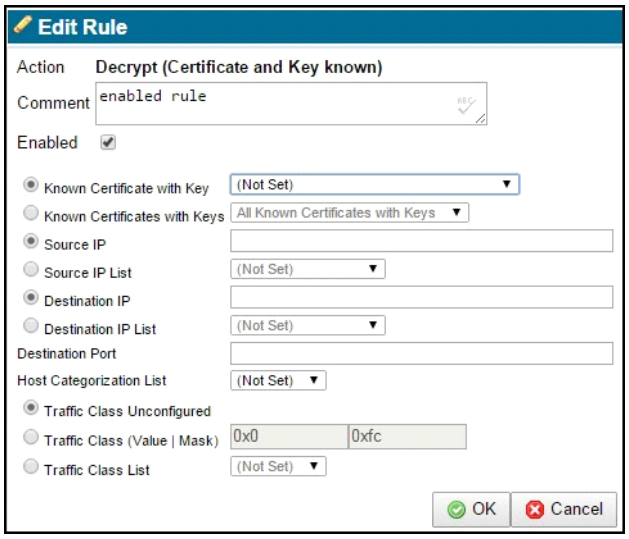
There are no new features in 3.8.5.

Features in Version 3.8.4

- **Enable/Disable Rule Setting**: You can now disable a rule within a ruleset. When creating or editing a rule, the new **Enabled** option is selected by default; the rule is active (and its location in the ruleset matters as usual). When cleared, the rule is not processed.



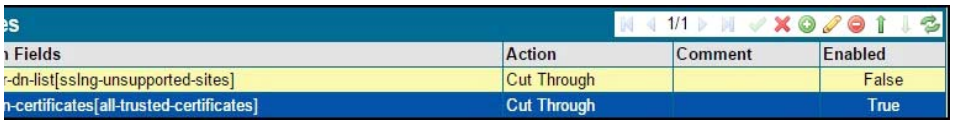
The setting is also shown per rule in the **Rulesets > Rules** panel, as **True** (enabled) or **False** (disabled) in the new **Enabled** column.



In most situations, all rules should be set to **True**. If you are debugging a ruleset, you might use the **False** setting (that is, deselect **Enabled** for that rule), applying it to one rule at a time.

Two new tools display in the Rules panel, as part of the disable rules feature:
Click **Enable Rule** to enable a highlighted disabled rule.
Click **Disable Rule** to disable the highlighted rule.

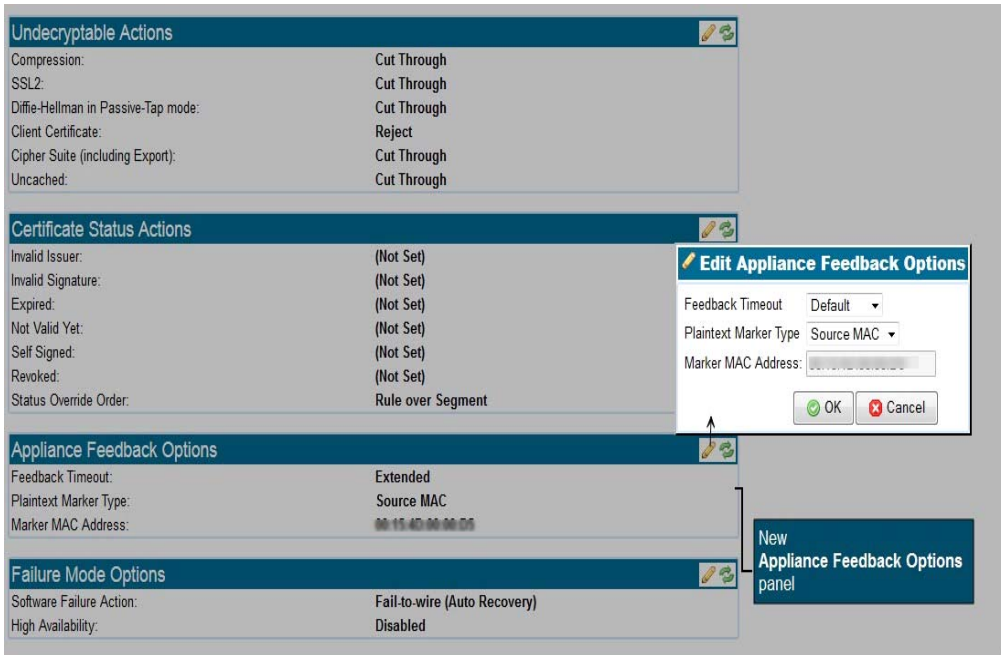
When a rule is disabled, its background display is yellow:



Click **Apply** at the **Policy Changes** message in the footer after enabling or disabling a rule.

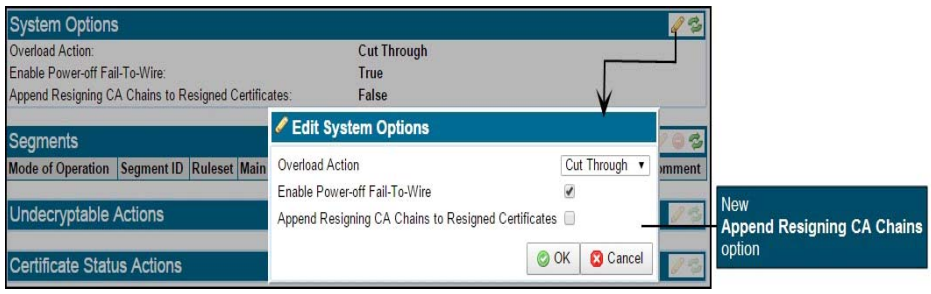
- Feedback Timeout Setting: SSL Appliance 3.8.4 supports a new loopback feedback timer. The new **Appliance Feedback Options** panel replaces the **Plaintext Marker** panel on the **Segments** window. **Feedback Timeout** is a new setting in that panel, which determines how long the SSL Appliance waits for a response before canceling a request and interrupting the SSL flow. Selecting the **Extended** timeout allows a more time-consuming request, such as one to the cloud, to complete. The **Default** is 1

second. The **Extended** period is 5 seconds.



The **Plaintext Marker Type** and **Marker MAC Address** settings are unchanged.

- **Resigning CA Certificate Chain**: SSL Appliance 3.8.4 provides support for including the resigning CA certificate chain in resigned SSL sessions. This allows SSL clients to validate resigned certificates without auto-downloading the resigning CA certificate chain. Here is the basic procedure:
  - On the **Segment > System Options** panel, check the new **Append Resigning CA Chains** to **Resigned Certificates** option. The SSL Appliance will include the resigning CA certificate chain (configured in the PKI store) in the SSL session.



  - On the PKI > External Certificate Authorities window, add all CAs from the resigning certificate chain to the External Certificate Authorities list.
    Once certificates have been added to the default **External Certificate Authorities List**, optionally create a new **External Certificate Authorities List**, and add the intermediate CAs which are included in the chain.

– On the **PKI > Resigning Certificate Authorities** window, add or edit a resigning certificate, Local or HSM. Select the required **Certificate Chain External CAs**.

Local CA example

HSM CA example

Click **OK** (on an **Edit** window) or **Add** (on an **Add** window), then **Apply** the changes.

– Verify the CA chain. On the **PKI > Resigning Certificate Authorities** window, highlight the resigning CA, then click the **Test Certificate Chain** icon (chain link).
If the CA chain is complete, you will see a "Complete certificate chain is present" message.
If the CA chain in incomplete, you will see a "Incomplete certificate chain, first missing CA: <name>" message. Add the missing CA to the **External Certificate Authorities List**.

– Configure a new segment with a ruleset using the appended resigning CA.

– Notes:
During policy activation, the appliance will load the certificate chain for each active resigning CA from the External CAs.
If a full certificate chain is not found for a resigning CA, a message will appear in the System Log, which identifies the first missing CA. The SSL Appliance will load the partial CA chain and include it with resigned certificates in inspected SSL sessions.

Features in Version 3.8.3

- The power-off Fail-to-Wire mode is now configurable. On the **Segments > Systems Options** panel, **Enable Power-off Fail-To-Wire** is selected by default; on power-off, traffic is directed from the incoming port to the paired port. When deselected, traffic is redirected into the SSL Appliance rather than the paired port. No traffic gets through.
- The SNMP configuration is now configurable under a new **SNMP Access** tab in the **Platform Management** menu. SNMP v3 is now supported. You can configure, enable, or disable SNMP management access; v1/2c and v3 may be enabled or disabled independently. The MIBs are available in a separate zip file (MIBS_SSLV- 3.8.3.zip).
All SNMP access is disabled be default. SNMP v1/v2c access is disabled by default until a **Community String** is configured. SNMP v3 access is disabled until a **SNMP User** account is created. Separate, unique **Trap User** accounts are required for generating traps.

- VLAN tags may be translated between ports on the new **VLAN Mappings** panel on the **Segments** screen.
- A new off-box Python SSL Diagnostics tool is available. Use it to parse statistics within a diagnostic package collected by a SSL Appliance. The tool and tool documentation (ssldiags.pdf) are available in a ssldiags-n.n.n.zip file (where n.n.n is the version number) on BTO.
- A new off-box Python SSL Sessions tool is available. Use it to parse SSL session log information within an exported session log generated by a SSL Appliance. The tool and tool documentation (sslsessions.pdf) are available in a sslsessions-n.n.n.zip file (where n.n.n is the version number) on BTO.
- The new default RSA key size for generating client certificates and keys is 2048-bit. The default RSA key size for generating a local resigning CA remains 1024-bit.
- Support has been added for identifying additional Camellia, ARIA, and AES CCM cipher suites in the **SSL Session Log**.
- The SSL Appliance now supports inspecting SSL sessions with the following cipher suites:
  - TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
- A new CLD command for exporting SSL Session Logs is available: `session log export`.
- If an appliance receives a VLAN tagged packet of less than 68 bytes, the appliance will pad it to 68 bytes before forwarding the packet.
- Each appliance model may have a distinct BIOS and BMC version. The BIOS and BMC versions are now displayed on the LCD screen. The following table presents the correct version for each model, as well as the BMC software version.

Model	BIOS	BMC	Notes
SSL1500	AQNIS100	4.00	
SSL2000	S5500.86B.01.00.0061.030920121535	0.60	BIOS: Only the four unique digits display on the LCD. For example, "0061."
SSL8200	S5500.86B.01.00.0061.030920121535	0.60	BIOS: Only the four unique digits display on the LCD. For example, "0061."

Note If you are getting a "Firmware Mismatch" message on the LCD, run the bios update Command Line Diagnostic (CLD) command in order to upgrade the BMC. The BIOS upgrade may take up to an hour; do not interrupt the process.

- The SSL Appliance has a new root OID based on the prefix .1.3.6.1.4.1.3417. The SSL Appliance models are now represented by this root OID plus the following OID extensions:
  - 1.5.2 = SSL1500
  - 1.5.3 = SSL2000

  - 1.5.4 = SSL8200

Features in Version 3.8.2

There are no new features in 3.8.2.

Features in Version 3.8.1

- The Dashboard panel graphic for the SSL1500 now reflects the -C or -F connectors appropriate for the appliance in use.
- An Uptime indicator now appears on the Dashboard, indicating the length of time since the appliance was last restarted or reset.The supporting CLD command uptime is also available.
- The Change Selected Categories window in the Host Categorization feature now includes an Invert button; use it to quickly select or deselect all categories
- The SSL Appliance license may now be exported from the License window.
- The SSL Appliance now has a root OID:
  - 14501.12 = Cisco SSL Appliance Product Family
  - 14501.12.2 = SSL1500
  - 14501.12.3 = SSL2000
  - 14501.12.4 = SSL8200
- Luna SP HSM support enables the SSL Appliance to use the networked Luna SP HSM to store resigning CA keys and to perform digital signature operations.
- IPv6 is now supported for use on the management network port. IPv4 and IPv6 may be configured con- currently on the management network. IPv6 is supported in the following configuration modes: SLAAC, SLAAC + Stateless DHCP, and Static.
- Meeting the STIG V-3013 requirements, a notice and consent login banner may be configured. The banner is presented to the user before login, and must be accepted in order for the login to proceed.
- Access Control Lists (ACL) may be configured to authorize or restrict access to incoming connections on the management network. Independent ACLs are available for IPv4 and IPv6 traffic. This feature meets STIG V-19076 requirements.
- Traffic Class Lists may be used to construct policy which decides whether or not to intercept an SSL flow based on QoS bytes, including but not limited to DiffServ values.

Resolved Issues

The following issues have been resolved in Version 3.8.6:

- Security updates to remove SPI CA and CA certificates with 1024-bit RSA keys from the GnuTLS package.
- Security update to correct a vulnerability in GNU cpio.
- Security update to address a vulnerability in DNS resolution routines in the GNU C Library (glibc). See Blue Coat Security Advisory SA114 for more information.
- Security update to correct a vulnerability in which Libgcrypt could be made to expose sens- itive information by an attack via physical side channels.
- Security updates to correct vulnerabilities to malformed or specially crafted documents in libxml2.
- Security update to correct vulnerabilities in Portable Network Graphics file library (libpng).

- Security update to correct vulnerabilities in use of MD5 in TLS 1.2 connections in GNU TLS.
- Security update to correct vulnerabilities to malformed UDP packets in DHCP server, client, and relay.
- Security update to correct vulnerabilities in OpenSSH client experimental support for resum- ing connections.
- Security update to correct a vulnerability in GnuTLS validation of padding bytes in CBC modes.
- Security update to correct vulnerabilities in Portable Network Graphics file library (libpng).
- Security update to correct vulnerabilities in Kerberos.
- Fixed an issue in which the SSL Visibility appliance could generate an ACK packet with an incorrect MAC during handling of network error conditions, if it had not seen both sides of a connection.
- TLS 1.2 is now correctly detected as SSL when searching in SSLv2 records.
- Increased the flow table size.
- Corrected an issue in which running a packet capture could interrupt VLAN translated traffic.
- Fixed an issue that prevented connections to Google Chrome services (such as Gmail) when SSL Visibility was decrypting the traffic.
- Fixed an issue in which use of a debug CLD command resulted in a failure in daemon communication, causing the Host Categorization license to be listed as `Unknown`.
- Fixed potential memory leaks in PKI handling routines.
- Fixed an issue in which SNMP traps could be sent for unused interfaces.
- Security update to correct vulnerabilities in the SQLite v3 library.
- Security updates to correct vulnerabilities in Perl 5 Compatible Regular Expression Library (PCRE).
- Security updates to correct vulnerabilities in Python 2.7.x.
- Fixed a certificate validation timeout issue that could produce `Invalid Issuer` errors.
- Fixed a memory leak in a statistics collection routine.
- Fixed a condition that produced a `CSRF tokens required` or `CSRF token mismatch` error when logging in after a WebUI session had expired.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.6:
  - CVE-2002-2443
  - CVE-2012-3425
  - CVE-2013-1752
  - CVE-2013-1753
  - CVE-2013-7443
  - CVE-2014-4616
  - CVE-2014-4650
  - CVE-2014-5355
  - CVE-2014-7185
  - CVE-2014-8964
  - CVE-2015-1197
  - CVE-2015-1819

- CVE-2015-2325
- CVE-2015-2326
- CVE-2015-2694
- CVE-2015-2695
- CVE-2015-2696
- CVE-2015-2697
- CVE-2015-2698
- CVE-2015-3210
- CVE-2015-3414
- CVE-2015-3415
- CVE-2015-3416
- CVE-2015-5073
- CVE-2015-5312
- CVE-2015-7497
- CVE-2015-7498
- CVE-2015-7499
- CVE-2015-7500
- CVE-2015-7511
- CVE-2015-7547
- CVE-2015-7575
- CVE-2015-7941
- CVE-2015-7942
- CVE-2015-7981
- CVE-2015-8035
- CVE-2015-8126
- CVE-2015-8241
- CVE-2015-8242
- CVE-2015-8317
- CVE-2015-8472
- CVE-2015-8540
- CVE-2015-8605
- CVE-2015-8710
- CVE-2016-0777
- CVE-2016-0778
- CVE-2016-2037

The following issues have been resolved in Version 3.8.5:

- The Cisco SSL Appliancee's session cache lookup logic has been redesigned in order to reduce the frequency of cache miss errors.

Note If SSL traffic traverses the Cisco SSL Appliance more than once, a Layer3/Layer4 cut-through rule to be applied at the Client Hello packet must be created as the first rule in the security policy for one direction of the flow (see below).

- Rulesets now allow Layer3/Layer4 rules to be applied at the Client Hello packet. To be applied at the Client Hello packet, rules must use Layer3/Layer4 match fields exclusively, and occur before any non- Layer3/Layer4 rules in the ruleset. Valid fields are:
  - Source IP address (or list of addresses)
  - Destination IP address (or list of addresses)
  - Destination Port
  - Traffic Class
  - An Action of Drop, Cut Through or Reject

Note All Layer3/Layer4 rules that you want to be applied at the Client Hello packet must occur before any non-Layer3/Layer4 rules in the ruleset. Once the policy reaches a rule that includes non- Layer3/Layer4 match fields, all subsequent rules will be applied at the Server Hello/Server Certificate level.

- In order to enhance security, TLS v1.0 is no longer supported in the SSL Appliance WebUI. The SSL Appliance WebUI supports TLS v1.1 and TLS v1.2. As a result, Management Center 1.4.1.1 or earlier is not supported for monitoring appliances running SSL Appliance 3.8.5. Contact Customer Support for more information.
- Improved inter-process communication to reduce the frequency of "No such file or directory" error messages.
- This general release for the SSL1500, SSL2000, and SSL8200 systems includes no new features. It provides a number of important vulnerability and bug fixes.
- Users logged in under Terminal Access Controller Access-Control System (TACACS) can add licenses if the user has the appropriate roles.
- Reduced the frequency of "Alert 86 (invalid_fallback)" error messages error messages when using a web browser.
- Security improvement to address the "Logjam" vulnerability. The SSL Appliance WebUI now rejects Diffie-Hellman keys smaller than 768 bits.
- Security improvement to enable TLS v1.2 by default in the SSL Appliance WebUI.
- Fixed an issue in which the SSL Appliance could forward a packet dropped by an IPS if the stream is out of order.
- Fixed an issue in which a TCP flow could stall when an upstream server missed client acknowledgments.
- The bootstrap process no longer reverts to local storage if a USB drive is not inserted into the SSL appliance when USB is selected as the Master Key Storage Location. The appliance waits until a USB has been inserted to create the master key.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.5:
  - CVE-2011-3389

  - CVE-2014-8176
  - CVE-2015-1788
  - CVE-2015-1789
  - CVE-2015-1790
  - CVE-2015-1791
  - CVE-2015-1792
  - CVE-2015-4000
  - CVE-2015-3143
  - CVE-2015-3144
  - CVE-2015-3145
  - CVE-2015-3148
  - CVE-2015-3153
  - CVE-2015-3622

The following issues have been resolved in Version 3.8.4:

- Legacy browser versions now correctly display the declared content type and sets the X-Con tent-Type-Options to nosniff.
- The web browser's cross-site scripting prevention filter is now correctly enabled.
- Javacript code which sets HTML elements is no longer at risk of attack due to HTML misinterpretation. The risk was eliminated by replacing code that sets HTML elements with code that sets innerText (which is not interpreted), or with code that directly manipulates the Document Object Model (DOM).
- Resolved an issue where MAC or Windows users browsing with Chrome encountered bad-record-mac messages when contacting sites such as Facebook.com and Panera.com.
- Sensitive system error messages are no longer seen on the SSL Appliance.
- Added cross-site request forgery (CSRF) protection. Cookies used in user requests to sites are protected transparently.
- Sensitive cookies are now marked as such, so they may not be modified by client-side script- ing languages. This reduces users' susceptibility to web-based attack vectors.
- Sensitive cookies are marked as secure, so they may no longer be transmitted over unen- crypted connections, potentially exposing their values to attackers.
- The SSL Appliance now includes protections against certain frame-based attacks such as clickjacking and cross-frame scripting.
- A user's session ID is now renewed after login, reducing the vulnerability of a session to hijacking.
- When configuring IPv6 DHCP, the appliance now allows a default gateway to be set.
- When an appliance is rebooted only once after applying several management network changes at the same time, the appliance no longer stops responding.

The following issues have been resolved in Version 3.8.3:

- When running a packet capture on an SSL2000 or SSL8200, existing flows are cut-through, so traffic is no longer dropped.

- The SSL Appliance no longer intermittently forwards packets dropped by the attached appliance.
- TCP packets are no longer received at the client out of order.
- Recent SSL1500 hardware no longer report a firmware version mismatch message on the LCD screen or in the System Log. If you see a mismatch message on the LCD screen after upgrading to SSL Appliance 3.8.3, run the BIOS update CLD command. The upgrade may take up to an hour; do not interrupt the process.
- When performing a manual test, or if an HSM resigning failure occurs, the corresponding System Log message now correctly appears in red text.
- After upgrading to SSL Appliance-3.8.3, you will no longer see the message mount: special device /dev/dom2 does not exist during the boot process.
- When running packet captures, the SSL_CAPTURE_ERROR is no longer seen, and captures occur correctly.
- Cut through, reject, and drop rules matching Anonymous Diffie-Hellman flows are no longer bypassed.
- Appliances no longer experience intermittent disruption to new flows when a new Host Categorization database is loaded.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.3:
  - CVE-2014-9672
  - CVE-2014-9673
  - CVE-2014-9674
  - CVE-2014-9675
  - CVE-2015-0235
  - CVE-2015-0247
  - CVE-2015-1472
  - CVE-2015-1473
  - CVE-2015-1572
  - CVE-2015-0293
  - CVE-2015-0292
  - CVE-2015-0289
  - CVE-2015-0288
  - CVE-2015-0287
  - CVE-2015-0286
  - CVE-2015-0209
  - CVE-2015-0206
  - CVE-2015-0205
  - CVE-2015-0204
  - CVE-2014-8275
  - CVE-2014-3707
  - CVE-2014-3572

  - CVE-2014-3571
  - CVE-2014-3570
  - CVE-2014-3569
  - CVE-2014-3567
  - CVE-2014-3513

The following issues have been resolved in Version 3.8.2:

- Resolved a memory leak issue associated with Host Categorization policy.
- SSL8200s in an Active-Inline Fail to Appliance deployment with a Cut Through rule now correctly forward server hellos.
- The Active-Inline attached appliance correctly receives the SSL ServerHello message for cut-through SSL sessions using 4096-bit RSA keys.
- Fixed the Ghost Vulnerability (CVE-2015-0235).
- The SSL Appliance no longer forwards invalid Hello messages, consuming resources, due to a certificate chain issue.
- Resolved an issue where Invalid issuer was incorrectly displayed in a Passive-Inline deployment.
- HSM CA status now shows the validity of the signatures returned on a connection.
- Addressed the OpenSSH Denial of Service vulnerability (CVE-2010-5107).
- The SSL Appliance no longer experiences slow down and high memory utilization.
- The SSL Appliance no longer allows SSLv3 connections to an HSM device. This is related to changes made to mitigate the Shell Shock vulnerability (CVE-2014-6271 and CVE- 2014-7169).
- Resolved an issue where due to a proprietary TLS extension, the appliance was unable to inspect traffic to some Google sites from Chrome on Windows.
- Fixed an issue in which SSL2000 and SSL8200 systems might fail to boot with software versions 3.7.x, 3.8.0, and 3.8.1.
- Multiple VLAN tags in QinQ Ethernet headers are now handled correctly.
- TCP flows no longer stall due to advertising a window larger than the previously seen receive window.
- Fixed an issue in which SSL packet capture would not work on some ports on the SSL8200 appliance.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.1:
  - CVE-2010-5107
  - CVE-2014-3566
  - CVE-2015-0235

The following issues have been resolved in Version 3.8.1:

- Resolved the "Shell Shock" vulnerability to specially-crafted environment variables (CVE-2014-6271 and CVE-2014-7169) in the Red Hat Enterprise Linux Bourne Again shell (Bash).
- Loss of management network connectivity no longer occurs when IPv6 address mode is configured for DHCP.

- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.1:
  - CVE-2014-3635
  - CVE-2014-3636
  - CVE-2014-3637
  - CVE-2014-3638
  - CVE-2014-3639
  - CVE-2014-6273
  - CVE-2014-6271
  - CVE-2014-7169
  - CVE-2014-7186
  - CVE-2014-7187
  - CVE-2014-0487
  - CVE-2014-0488
  - CVE-2014-0489
  - CVE-2014-0490

The following issues have been resolved in Version 3.8.0:

- Resolved the issue where following an upgrade an additional manual reboot was needed for the fix to be applied. A user no longer needs to perform the additional reboot.
- Resolved an issue that resulted in a fault when activating policy.
- Resolved a case where a segment did not recover on software failure.
- First-time boot no longer takes up to 5 additional minutes if no network cable is plugged into the management network port.
- Resolved an issue where all platform configuration changes required rebooting the appliance in order to take effect.
- System log files are rotated once per-day regardless of the size of the file, and only removed when the log disk space threshold of 3GB is reached.
- The following characters are now allowed in alert e-mail addresses: !, #, $, %, &, ', *, +, /, =, ?, ^, `, {, }, |, ~
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.8.0:
  - CVE-2012-1016
  - CVE-2013-1415
  - CVE-2013-1416
  - CVE-2013-1418
  - CVE-2013-6800
  - CVE-2014-4341
  - CVE-2014-4342
  - CVE-2014-4343
  - CVE-2014-4344

- CVE-2014-4345
- CVE-2014-3477
- CVE-2014-3532
- CVE-2014-3533
- CVE-2014-3467
- CVE-2014-3468
- CVE-2014-3469
- CVE-2013-4357
- CVE-2013-4458
- CVE-2014-0475
- CVE-2014-4043
- CVE-2014-5119
- CVE-2014-5270
- CVE-2014-0191
- CVE-2014-0224
- CVE-2014-0195
- CVE-2014-0221
- CVE-2014-0224
- CVE-2014-3470
- CVE-2014-3466
- CVE-2014-0195
- CVE-2014-0221
- CVE-2014-0224
- CVE-2014-3470
- CVE-2014-0195
- CVE-2014-0221
- CVE-2014-0224
- CVE-2014-3470
- CVE-2014-4617
- CVE-2014-0478
- CVE-2014-3505
- CVE-2014-3506
- CVE-2014-3507
- CVE-2014-3508
- CVE-2014-3509
- CVE-2014-3510
- CVE-2014-3511
- CVE-2014-3512

  - CVE-2014-5139
  - CVE-2014-3613
  - CVE-2014-3620
  - CVE-2014-0487
  - CVE-2014-0488
  - CVE-2014-0489
  - CVE-2014-0490
  - CVE-2012-6151
  - CVE-2014-2284
  - CVE-2014-2285
  - CVE-2014-2310
  - CVE-2014-2525
  - CVE-2014-2532
  - CVE-2014-1912

The following issues have been resolved in Version 3.7.4:

- When an SSL Appliance recovers from an overload condition it no longer flags some SSL sessions with the "Invalid cryptographic response" error code.
- Corrected an issue that exposed the following ports on the management interface: 9001, 9002, 9003, 9009 and 9010.
- In Passive Inline mode, copy ports now correctly see Server Hello packets with a "cut- through" rule.
- Corrected handling of dates in OCSP Response fields.
- Fixed an issue in which duplicate client/server hello packets were issued in passive-inline deployment for certain cut-through SSL flows.
- Fixed an issue in which certificate resigning of traffic with an Online Certificate Status Protocol (OCSP) stapled response with a key larger than the originating key caused the system to fail.
- Corrected several memory allocation issues.
- Corrected an issue where a segment did not recover on software failure.
- The command line diagnostic interface can now be used during the bootstrap phase to set IP configuration on the management network interface.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.7.4:
  - CVE-2014-3477
  - CVE-2014-3532
  - CVE-2014-3533
  - CVE-2014-3467
  - CVE-2014-3468
  - CVE-2014-3469
  - CVE-2013-4357
  - CVE-2013-4458

  - CVE-2013-0475
  - CVE-2013-4043
  - CVE-2014-3505
  - CVE-2014-3506
  - CVE-2014-3506
  - CVE-2014-3507
  - CVE-2014-3508
  - CVE-2014-3509
  - CVE-2014-3510
  - CVE-2014-3511
  - CVE-2014-3512
  - CVE-2014-5139

The following issues have been resolved in Version 3.7.3:

- Resolved an issue in which the SSL Appliance became unusable and GUI timeouts occurred when navigating screens, requiring a manual reboot of the appliance to recover.
- Resolved a memory leak in the SSL intercept engine, when processing SSL flows with a large numbers of unique X.509 certificates. The issue resulted in no SSL sessions being inspected, and sometimes caused a restart.
- Resolved an issue where IP fragments would not pass successfully through the SSL Appliance.
- Resolved an issue where incorrect processing of IP fragments sometimes lead to a crash requiring a manual restart.
- Resolved an issue that resulted in NFE 0 overload messages and caused the SSL Appliance to stop decrypting.
- The SSL Debug log now rotates correctly. Previously, debug logs could fill up the internal disk.
- Resolved an issue that prevented proper startup of the appliance after a patch upgrade.
- The following Common Vulnerabilities and Exposures (CVE) have been addressed in 3.7.4:
  - CVE-2014-0224

The following issues have been resolved in Version 3.7.1:

- Addressed the HeartBleed exploit, protecting against it for SSL traffic passing through and inspected by the SSL Appliance. This patch allows you to protect internal servers and prevent vulnerable client systems from attack even if they visit a malicious SSL server.
- Resolved a memory leak in the SSL intercept engine. The main symptom was lockup in one or more processing threads, resulting in no SSL sessions being inspected. In the worst case scenario, the data-plane process would crash and restart. The symptoms manifested in scenarios where large number of unique X.509 certificates were seen on the wire.
- Fixed a crash in generating the platform diagnostics archive (archive process did not exclude the sparse file /var/log/lastlog).
- Fixed processing of out-of-order TCP packets as well as processing of large TCP headers in Passive-Tap mode.

- TCP FIN packets were not processed in the correct order in inline modes, resulting in TCP queue processing timeouts.
- When displaying SSL session log entry details the UI now checks for the availability of certificate information; previous releases would have triggered an exception in the UI. The same updated logic is also applied to the fingerprint calculation on unsupported certificate key types.
- The in-memory X.509 caches are now limited in size to prevent the OOM killer from terminating the data-plane. The issue used to manifest itself when a large number of unique X.509 certificates were detected by the SSL Appliance.
- Wild cards ('*' character) in X.509 subject fields are now treated as characters rather than wild cards in the policy engine. The rules in the policy may still use wild card characters. As an example: this fix allows the user to set up a rule to match the following CN: "cdn.*.live- filestore.com"
- TLS sessions with unsupported TLS extensions are now classified as undecryptable. Refer to the Important Information section for more details.
- The UI now allows the user to reset the hostname by entering an empty value, which then translates into "localhost.localdomain" in the configuration.
- The UI webserver would sporadically reject file uploads with a "502" error because of the size of the HTTP header; the allowed header size was increased to resolve the issue.
- Fixed handling of TCP retransmits while decrypting certain cipher-suites (using block ciphers, for example, AES-CBC, 3DES-CBC), in the process fixing various types of TCP queue processing timeouts. The issue was especially prevalent when deploying the SSL Appliance downstream from a F5 load-balance appliance.
- Process TLS CertificateStatus handshake messages; not processing those messages resulted in breaking certain browser page elements (such as twimg.com when connecting to Twitter).
- Allow setting the "Catch All Action" on rulesets; this was broken in version 3.6.3.
- Remove the X.509 Subject Key Identifier when applying "Decrypt (Resign Certificate)" and "Replace Key Only" actions to prevent invalid certificate errors in browsers.
- Empty user-defined policy lists used in rulesets no longer invalidate the rule referencing the list.
- Self-signed X.509 certificates seen on the wire had an erroneous validation status of both "Self-signed" and "Invalid Issuer".
- The IP header check logic was changed to allow fragments with the don't fragment (DF) bit set; those packets used to be discarded.
- Fixed issue when loading the UI in recent versions of the Chrome browser.
- When using user-defined PKI lists in rules and the list name has a specific length then the list would be ignored and would default to all entries of that specific type of PKI item.

Known Issues

The following known issues are reported in Version 3.8.6:

- When a new policy is pushed on the SSL Visibility appliance, the validation cache is reset, but the persistent certificate cache is not. When reused sessions look up the cer- tificate in the persistent certificate cache, it no longer has the correct certificate chain, causing the session to be reported as Invalid Issuer.

- An SSL SSL1500 appliance with a segment that includes port 4 configured in High Availability (HA) mode may not propagate failure state to attached switches. The port status on the switch connected to port 4 may appear to be Up (light on) when the segment is forced down due to a port failure. If you experience this issue, contact Customer Support.
- During boot up, the following messages may be seen in DMESG and in the system log:
  [23.503330] ACPI Warning: 0x0000000000000828-0x000000000000082f SystemIO conflicts with Region \ PMRG 1 (20121018 / utaddress-251)[23.503336] ACPI: If an ACPI driver is available for this device, you should use it instead of the native driver.
  The messages can be safely ignored.
- During boot up, the following messages may be seen in DMESG and in the system log:
  [0.000000] Calgary: detecting Calgary via BIOS EBDA area [0.000000] Calgary: Unable to locate Rio Grande table in EBDA - bailing!
  The messages can be safely ignored.
- The CLD command **platform show ntp** truncates the address of IPv6 NTP servers.
- The message **power_meter ACPI000D:00: Ignoring unsafe software power cap!** may display during boot up of an appliance. You can safely ignore this message.
- Power-off fail-to-wire (FTW) does not work on the SSL1500 fiber interface.
- When configuring SNMP v3, both the authentication and privacy passphrases are required, regardless of what security level is selected.
- When the appliance Hostname is set to localhost.local domain and DNS is configured, if the DNS server becomes unreachable, the appliance becomes unmanagemable from the WebUI.

  Workaround: Configure a host name other than localhost.localdomain.
- If log files take up more than 3 GB of disk space, the WebUI may fail to retrieve and display the System Log.
- When an SSL appliance recovers from an overload condition it may flag some SSL sessions with the "Invalid cryptographic response" error code
- Only network interfaces used by active segments will change color on the user interface dashboard, based on the status of the interface. This is only an issue for the SSL1500.
- Internal CA certificates are not automatically checked for expiration.

  Workaround: Periodically check the certificates on the user interface.
- A TCP FIN/FIN-ACK/ACK sequence is generated at the end of each decrypted SSL ses- sion. The three packets in this sequence might arrive at the attached device (e.g., IDS) out of sequence. This should not pose any problems for TCP reassembly devices.
- A segment configured to use any the Active-Inline (AI) modes will, under load, reject some SSL sessions because of packet feedback timeouts. This means that decrypted packets sent to the attached device (for example, IPS) did not return in time to complete the feedback loop required to trigger a re-encrypt of the original packets.
- Restoring a policy that contains active segments does not always activate the segments.

  Workaround: Manually activate the segments.
- PKI objects (certificates or keys) can be removed even if they are referenced by the active policy.
- If more than one administrator are making changes to the SSL appliance configuration, they will have to log out and log in again before changes made by the other person will be reflected in the user interface.

- OCSP is not supported for server certificate validation. Only manually loaded CRLs can be used.
- Flows through an appliance which use an imported resigning CA with a 512-bit RSA key may yield inconsistent results. Though the SSL Appliance allows the import of a 512-bit RSA key, it is not recommended.
- The system log is currently displayed in oldest-to-latest order, and updates will only be reflected on the last page, and only after pressing the Last button.
- If two or more instances of the web interface are opened in different tabs or windows of the same browser on the same computer, logging out of one instance causes the user to be logged out of all other instances.
- The Session Log may occasionally contain "could not sync on hand off" messages for flows matching a domain in a Domain Name list used in a cut through rule.
- Maximum throughput performance of UDP traffic is affected when a small number of UDP flows is used.
- The SSL session log may show sessions with harmless "Alert[C]: unknown (0)" error messages.
- The vSphere VNC client sends an unencrypted ClientHello message, resulting in "Corrupt Record" session errors.
- The web interface panel that notifies users to reboot the appliance after a configuration change disappears after the user has logged out.
- Diagnostic files generated via the command line are deleted when the user logs out or the SSH session is terminated. The diagnostics files should be downloaded as soon as possible and before logout.
- Installing a valid SSL license may cause a brief loss of connectivity while unfailing the port configured on active segments. This is only an issue on a SSL1500.
- SSL error counts and invalid certificate information is cleared when the appliance policy is reactivated.
- Deactivating an Active Inline segment may cause some packets to be received and re- transmitted on the device ports in an endless loop.

  Workaround: Pull out and re-insert the cable on the deactivated segment.
- Disabling a Remote Logging entry causes the options configured in the entry to be lost.
- Timestamps in remote system log entries have one-second resolution and do not include fractions of seconds.
- SNMP traps for link loss may not be generated if the link is recovered within 30 seconds.
- Policy activation failure on single segment causes policy activation failure on all other segments. Furthermore, policy errors in rulesets not used by active segments will also prevent policy activation.
- The default list of external certificate authorities includes CA certificates signed using the deprecated MD5 hash algorithm.
- SSL sessions to the Blue Coat ThreatPulse service may occasionally be rejected due to cryptographic operation errors.
- Patch upgrades do not update the default external CA list. New external CAs can be installed using the provided PKCS#7 file.
- The SSL Appliance does not correctly match policy rules to SSL flows that contain non- ASCII characters in the "Subject" and "Issuer" server certificate fields.

- DER-encoded PKCS#8 keys cannot be imported into the PKI store.
- The SSL appliance cannot process SSL renegotiation on inspected SSL flows and will terminate such flows. Cut-through policy rules must be used to prevent flow termination.
- Manually failed segments are automatically unfailed when the SSL Appliance is rebooted.
- A half-duplex connection is negotiated if the SSL Appliance is connected to a 1000 Mbps port that is forced to operate at 100 Mbps. Note that a full-duplex connection is negotiated if connected to a 100 Mbps port or a 1000 Mbps port running at full speed.
- The SSL Appliance 2000 and 8200 models will try booting off of a USB stick if inserted into the front USB port
- TCP connections with a small receive window may fail when a large amount of data is added to the flow.
- The "Replace Certificate and Key" rule action is not supported for SSL flows using ECDSA authentication.
- The SSL Appliance may sporadically not send ClientHello messages of cut- through flows to the attached appliance.
- DER-formatted keys and certificates cannot be used as web UI certificate/keys.
- WebUI sessions may not always present an expiration indication.

For Assistance

Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco SSL Appliances, see **What's New in Cisco Product Documentation** at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to **What's New in Cisco Product Documentation**, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance with the Cisco SSL Appliance, you can also contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.

Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.