Blue Coat SSL Visibility Appliance 3.9.x.x - 3.7.x Release Notes

Release Information

These release notes provide information for each release in the SSL Visibility Appliance operating system line, plus additional information about version upgrading, compatibility with other Blue Coat and third-party products, and documentation location.

Blue Coat recommends upgrading all SSL Visibility Appliance models to software version 3.9.6.1 build 12. See Upgrade & Downgrade the SSL Visibility Appliance.

Most Current Version: SSLV 3.9.6.1-12

Release Date: October 20, 2016

Document Revision: October 20, 2016

Release Note Directory

These release notes present information about the 3.9.6.1-12 release for the SSL Visibility Appliance. The release notes also include information for each release in the SSL Visibility Appliance 3.9.x.x, 3.8.x, and 3.7.x software lines. Each section for a specific release provides feature descriptions, changes, and fixes. Sections about known issues are listed separately.

Release Index

Information About All Releases

- SSL Visibility 3.9.x.x - 3.7.x Known Issues
- Blue Coat Technical Support Resource

Subscribe to SSL Visibility Appliance Documentation

Subscribing to the RSS feed for your appliance will provide you with automatic information updates, including all knowledge base articles. Follow these steps:

1. Go to: https://bto.bluecoat.com/support/blue-coat-support-rss-feeds.
2. Select SSL Visibility from the **Products** list.
3. Copy the URL.
4. Go to Outlook and right-click the **RSS Feeds** folder.
5. Select **Add a New RSS Feed**.
6. Paste in the URL and click **Add**.
7. Click **Yes**. A new folder is created, called **knowledgebase - datacategory - SSL Visibility**.

   When new SSL Visiblity Appliance knowledge base articles are published, Blue Coat will send an email notification to the SSL Visibility RSS Feeds folder. The email will contain a link to the article.

SSL Visibility Appliance 3.9.6.1

Release Information

- **Version:** 3.9.6.1
- **Build Number:** 12
- **Release Date:** October 20, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800/SV2800B, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.6.1 build 12 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1
  - Fixes in 3.9.3.2
  - Fixes in 3.9.3.3
  - Fixes in 3.9.3.6
  - Fixes in 3.9.4.1
  - Fixes in 3.9.5.1

Changes in 3.9.6.1

There are no new features in SSL Visibility 3.9.6.1. This maintenance release provides bug fixes and important security updates. See Fixes in 3.9.6.1 for information.

Upgrading

SSL Visibility 3.9.6.1 supports the SV3800B-20 appliance. The SV3800B-20 appliance currently ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

SSL Visibility 3.9.6.1 supports the SV2800B appliance. The SV2800B appliance currently ships with SSL Visibility 3.9.5.1 installed.

After upgrading to SSL Visibility 3.9.6.1 from a 3.9.3.x or 3.9.2.x release on an SV800 or SV3800B-20 appliance, you must update the BIOS. See Upgrade & Downgrade the SSL Visibility Appliance for information.

After upgrading to SSL Visibility 3.9.6.1 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS. See Upgrade & Downgrade the SSL Visibility Appliance for information.

Due to backup format changes, backup files created with 3.9.6.1 cannot be restored on systems running 3.9.3.x or earlier versions of SSL Visibility. (Backups created on appliances running earlier versions of SSL Visibility can be restored to appliances running version 3.9.6.1.)

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com
- cn=contentanalysis.es.bluecoat.com
- cn=contentanalysis-ma-u.es.bluecoat.com
- cn=list.bluecoat.com
- cn=license.soleranetworks.com
- cn=tracking.soleranetworks.com
- cn=sp.cwfservice.net
- cn=maa-updates.es.bluecoat.com
- cn=ti.soleranetworks.com
- cn=bto.bluecoat.com
- cn=hb.bluecoat.com
- cn=bluecoat.flexnetoperations.com
- cn=bchashlookup.es.bluecoat.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.3 or later. Management Center 1.4.1.1 or earlier is not supported.

The files associated with this release are:

- sslv-3.9.6.1-12-bluecoat.patch
- sslv-3.9.6.1-12-bluecoat.nru
- sslv-3.9.6.1-12-bluecoat.nsu
- sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.9.4.1.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.7.zip

See Upgrade & Downgrade the SSL Visibility Appliance for details on downloading files and performing upgrades.

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.6.1

There are no new features in SSL Visibility 3.9.6.1.

Fixes in 3.9.6.1

Release Information

- **Release Date:** October 20, 2016
- **Build Number:** 12

SSL Visibility Appliance software 3.9.6.1 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2766 SSLV-2611	Optimized X.509 certificate caching behavior.
SSLV-2755	Daylight Saving Time changes for Turkey.
SSLV-2744	Corrected a platform interface timeout issue when active inline appliances are rebooted.
SSLV-2743	Corrected a segment fault that could occur during a policy update.
SSLV-2738	Corrected a retransmission issue with the updated TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 cipher suite.
SSLV-2702	Optimized interface stability when attached devices restart on segments configured for high availability with auto-recovery.
SSLV-2686	Ensures adequate memory before Host Categorization database downloads.
SSLV-2683	Addresses libidn11 security vulnerabilities. (CVE-2016-6263, CVE-2016-6262, CVE-2016-6261, CVE-2015-8948, CVE-2015-2059)
SSLV-2678	Added support for cipher suite: TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256.
SSLV-2663	Corrected an issue in which an empty Subject/Domain List used in a rule could cause a fail-to-wire event.
SSLV-2648	Corrected a crash in `ssldata` that could occur with packet fragmentation.
SSLV-2638	Addresses libcurl3 security vulnerabilities. (CVE-2016-5421, CVE-2016-5420, CVE-2016-5419)
SSLV-2637	Addresses openssh-server security vulnerabilities. (CVE-2016-6515, CVE-2016-6210)
SSLV-2620	Optimized watchdog timers to prevent incorrect fault detection.
SSLV-2591	Added support for Google updated (non-standard) cipher suites: TLS_CECPQ1_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_CECPQ1_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_CECPQ1_RSA_WITH_AES_256_GCM_SHA384 TLS_CECPQ1_ECDSA_WITH_AES_256_GCM_SHA384
SSLV-2546	Removed URLs from Certificate Revocation List.
SSLV-2531	The updated ChaCha20-Poly1305 cipher suites display under the correct names in the SSL Session log.
SSLV-2454	IPv6 addresses in the source/destination fields are no longer truncated when SSL Session logs are sent to a remote syslog server.
SSLV-2235	Added logic to bring system into failure mode when disks fail.

Upgrade & Downgrade the SSL Visibility 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:

- 3.7.x up to and including 3.7.4-41
- 3.8.0 up to and including 3.8.0-152
- 3.8.1 up to and including 3.8.1-172
- 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
- 3.8.6 up to and including 3.8.6-12
- 3.9.2.1 up to and including 3.9.2.1-18
- 3.9.2.2 up to and including 3.9.2.2-2
- 3.9.3.1 up to and including 3.9.3.1-34
- 3.9.3.2 up to and including 3.9.3.2-7
- 3.9.3.3 up to and including 3.9.3.3-6
- 3.9.3.4 up to and including 3.9.3.4-11
- 3.9.3.5 up to and including 3.9.3.5-5
- 3.9.3.6 up to and including 3.9.3.6-23
- 3.9.4.x up to and including 3.9.4.5-3
- 3.9.5.1 up to and including 3.9.5.1-2

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 WebUI.

Prerequisites

Log In to BTO and Download Files

To download files, log in to your BlueTouch Online (BTO) account at https://bto.bluecoat.com/. Select the **Downloads** tab, then **Blue Coat Product Downloads**, then browse to SSL Visibility and your appliance model.

If you don't have an account, go to the BlueTouch Request Login screen at https://www.bluecoat.com/forms/contact, and follow the registration process.

Licensing

Before you begin, make sure you have the SSL Visibility Appliance license ready to install, as the SSL Visibility Appliance requires a license to be fully operational. Before you can license your SSL Visibility Appliance, you must have the following:

- A user with the Manage Appliance authentication role configured on the appliance.
- The serial number of your appliance. To locate the serial number, go to **(Platform Management) > Information**. View the serial number under **Chassis FRU Info**. The serial number can also be found on the front panel LCD screen.

- A BlueTouch Online account. If you need a BlueTouch Online login, go to the BlueTouch Request Login screen (https://www.bluecoat.com/forms/contact), and follow the registration process.

If you already have a license installed on the appliance and plan to perform a .nsu update, export the license by using the **Platform Management > License** menu. You can restore the license when the update is complete.

Download a Blue Coat License

1. Using your BlueTouch Online account information, log in to the Blue Coat Licensing Portal (https://services.bluecoat.com/eservice_enu/licensing/register.cgi).
2. From the menu on the left side, select **SSL Visibility**, then **License Download**.
3. When prompted, enter the serial number of your appliance, then click **Submit**.
4. When the license has been generated, click **Download License File** for the required SSL Visibility Appliance.

Upgrade the Appliance

If the appliance is running 3.7.0 or greater, upgrade using the sslv-3.9.6.1-12-bluecoat.patch.

Rescue Image Notes

- **3.7.x or Later**: 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 any patches released since the latest rescue image version.

  Following the patch upgrade, Blue Coat recommends you upgrade the rescue image to the latest software version by applying the related .nru (for example, sslv-3.9.6.1-12-bluecoat.nru).

Overview

Upgrading the SSL Visibility Appliance to a new software version is straightforward.

Apply a Patch

To apply the patch, access the **(Platform Management) > Update** menu option on the WebUI, select the sslv-3.9.6.1-12-bluecoat.patch file, and click **OK**.

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

Apply the NRU (3.7.x or Later)

To apply the .nru file, which will update the rescue image, access the **(Platform Management) > Update** menu option on the WebUI, select the sslv-3.9.6.1-12-bluecoat.nru file, and click **OK**.

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

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

Patch Upgrade Procedure

1. Access the **(Platform Management) > Update** menu.
2. Click **Choose File** to select the patch upgrade file appropriate to your software version, then click **OK**.
3. Reboot the appliance when prompted.

4. Wait for the upgrade to complete. This might take several minutes, and involves the appliance rebooting a number of times.
5. Update the list of external CA certificates, if required.

Without the new list of external CA certificates, the X.509 status for some sites (for example, www.google.com) is "Invalid Issuer." The external CA certificate file (sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b) incrementally updates the CA certificates list provided in previous sslv_3.x.x_to_3.x.x_ca_certificates.p7b files. Import the CA certificate file to update the external CA certificates list.

3.9.4.x Process: After a 3.9.x.x to 3.9.4.x upgrade, the list of external CA certificates may not include the CA certificates provided with the 3.9.4.x release. If you have not previously done so, import the sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b file to update the external CA list with the 3.9.2.1 CA certificates. Then import the sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b file to update the external CA list with the 3.9.3.1 CA certificates. Then import the sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b file. If you have previously imported an external CA certificate file, you do not need to import it again.

To import the PKCS#7 encoded external CA certificate file (such as sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b), follow this procedure.

a. Go to the **PKI > External Certificate Authorities Lists** window and select the **all-external-certificate-authorities** list.
b. In the **External Certificate Authorities** panel below, click **Add** to browse to the file, then click **OK**. You should see an "Upload Successful" message.
c. On the bottom of the **External Certificate Authorities Lists** window, click **Apply** next to the **PKI Changes** message.
d. Use the same process to import the 3.9.3.x external CA file (sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b)
e. Use the same process to import the 3.9.4.x external CA file (sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b).

3.8.x Process: After a 3.8.x to 3.9.4.x upgrade, the list of external CA certificates may not include the CA certificates provided with the 3.8.x or 3.9.x.x release. If you have not previously done so, import the sslv_3.8.0_to_3.8.3_ca_certificates.p7b file to update the external CA list. Then, import the sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b file, then the sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b file, and then the sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b file. If you have previously imported an external CA certificates file, you do not need to import it again.

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.

a. Go to the **PKI > External Certificate Authorities Lists** window and select the **all-external-certificate-authorities** list.
b. In the **External Certificate Authorities** panel below, click **Add** to browse to the file, then click **OK**. You should see an "Upload Successful" message.
c. On the bottom of the **External Certificate Authorities Lists** window, click **Apply** next to the **PKI Changes** message.
d. Use the same process to import the 3.9.2.x external CA file (sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b).

e. Use the same process to import the 3.9.3.x external CA file (sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b).
f. Use the same process to import the 3.9.4.x external CA file (sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b).

3.7.x Process: After a 3.7.x to 3.9.x.x upgrade, the list of external CA certificates may not include the CA certificates provided with the 3.8.x or 3.9.x.x release. If you have not previously done so, import the sslv_3.7.0_to_3.8.0_ca_certificates.p7b file. Then, import the sslv_3.8.0_to_3.8.3_ca_certificates.p7b and sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b CA certificates files. If you have previously imported an external CA certificates file, you do not need to import it again.

To import the SSLV 3.7 PKCS#7 encoded external CA certificates file (sslv_3.7.0_to_3.8.0_ca_certificates.p7b), follow this procedure.

a. Go to the **PKI > External Certificate Authorites Lists** window and select the **all-external-certificate-authorities** list.
b. In the **External Certificate Authorities** panel below, click **Add** to browse to the file, then click **OK**. You should see an "Upload Successful" message.
c. On the bottom of the **External Certificate Authorties Lists** window, click **Apply** next to the **PKI Changes** message.
d. Use the same process to import the 3.8.x external CA file (sslv_3.8.0_to_3.8.3_ca_certificates.p7b).
e. Use the same process to import the 3.9.2.x external CA file (sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b).
f. Use the same process to import the 3.9.3.x external CA file (sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b).
g. Use the same process to import the 3.9.4.x external CA file (sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b).

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

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

Update the BIOS

You must update the BIOS:

- After upgrading an SV1800, SV2800, or SV3800 appliance to SSL Visiblilty 3.9.x.x from any 3.8.x or 3.7.x release
- After upgrading an SV800 , or SV3800-B20 appliance to SSL Visiblilty 3.9.4.x from any previous 3.9.x release

After the upgrade you will see a message indicating that a firmware update is needed. A message is also displayed on the LCD and in the system log.

To update the BIOS, access the Command Line Diagnostics (CLD) interface, and enter the **`bios update`** command.

The update will take 15 to 20 minutes (or possibly longer, depending on the appliance) and may include a system reboot. Do not interrupt the process.

When you see the message "`SSLV startup stage 3: CONFIRMED`" displayed on the serial console, the process is complete.

Each appliance model may have a distinct BIOS and BMC version. The following table presents the correct BIOS version for each model, as well as the BMC software version.

Model	BIOS	BMC
SV800-250M-C SV800-500M-C	r1	r1
SV1800-C/F	r3	r3
SV2800	r1	r1
SV2800B	r6	r6
SV3800	r1	r1
SV3800B-20	r7	r7

To view the BIOS and BMC versions, open **Information** on the **Platform Management (system hostname)** menu and click the **Show Advanced** button.

Downgrade the Appliance

If you require appliance downgrade information, contact Customer Support for assistance.

SSL Visibility Appliance 3.9.5.1

Release Information

- **Version:** 3.9.5.1
- **Build Number:** 2
- **Release Date:** September 1, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800/SV2800B, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.5.1 build 12 includes no new fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1
  - Fixes in 3.9.3.2
  - Fixes in 3.9.3.3
  - Fixes in 3.9.3.6
  - Fixes in 3.9.4.1

Changes in 3.9.5.1

There are no new features in SSL Visibility 3.9.5.1. This release adds additional web sites to the Unsupported Sites list.

Upgrading

SSL Visibility 3.9.5.1 supports the SV3800B-20 appliance. The SV3800B-20 appliance currently ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

SSL Visibility 3.9.5.1 supports the SV2800B appliance. The SV2800B appliance currently ships with SSL Visibility 3.9.5.1 installed.

After upgrading to SSL Visibility 3.9.5.1 from a 3.9.3.x or 3.9.2.x release on an SV800 or SV3800B-20 appliance, you must update the BIOS. See Upgrade & Downgrade the SSL Visibility Appliance for information.

After upgrading to SSL Visibility 3.9.5.1 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS. See Upgrade & Downgrade the SSL Visibility Appliance for information.

Due to backup format changes, backup files created with 3.9.5.1 cannot be restored on systems running 3.9.3.x or earlier versions of SSL Visibility. (Backups created on appliances running earlier versions of SSL Visibility can be restored to appliances running version 3.9.5.1.)

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com
- cn=contentanalysis.es.bluecoat.com
- cn=contentanalysis-ma-u.es.bluecoat.com
- cn=list.bluecoat.com
- cn=license.soleranetworks.com
- cn=tracking.soleranetworks.com
- cn=sp.cwfservice.net
- cn=maa-updates.es.bluecoat.com
- cn=ti.soleranetworks.com
- cn=bto.bluecoat.com
- cn=hb.bluecoat.com
- cn=bluecoat.flexnetoperations.com
- cn=bchashlookup.es.bluecoat.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.3 or later. Management Center 1.4.1.1 or earlier is not supported.

The files associated with this release are:

- sslv-3.9.5.1-12-bluecoat.patch
- sslv-3.9.5.1-12-bluecoat.nru
- sslv-3.9.5.1-12-bluecoat.nsu
- sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.9.4.1.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.7.zip

See Upgrade & Downgrade the SSL Visibility Appliance for details on downloading files and performing upgrades.

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

SSL Visibility Appliance 3.9.4.1

Release Information

- **Version:** 3.9.4.1
- **Build Number:** 94
- **Release Date:** August 5, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.4.1 build 94 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1
  - Fixes in 3.9.3.2
  - Fixes in 3.9.3.3
  - Fixes in 3.9.3.6

Changes in 3.9.4.1

SSL Visibility 3.9.4.1 introduces the following new features:

- Online Query for Blue Coat Host Categorization Database
- Support for local, user-created Host Categorization Database
- Updated SSL Sessions tool available

See Features in 3.9.4.1 for more information.

SSL Visibility 3.9.4.1 adds the following enhancements:

Configurable Facility Level for Remote Log Server - SSL Visibility 3.9.4.1 provides configurable facility levels in the **Remote Logging** setup options to better identify syslog messages logged by the SSL Visibility appliance, for example, in the event of conflicts with other devices on a network. See the *Blue Coat SSL Visibility Admnistration and Deployment Guide, version 3.9.4.1* for details.

X.509 Fingerprint in System Logs - SSL Visibility 3.9.4.1 includes X.509 Certificate Fingerprint information in the SSL Session log data that is sent to a remote syslog server, if one is enabled.

Option to Exclude Specific Rules from Logging - SSL Visibility 3.9.4.1 adds an option to prevent details for flows processed by specific rules from being included in the SSL Session logs. The **Insert Rule** and **Edit Rule** windows now include an **Include in Session Log** check box. The check box is enabled by default; to exclude details for flows processed by a particular rule from the SSL Session log, clear the check box when inserting or editing the rule.

Segment Comment in Dashboard - The contents of the **Segment Comment** field are visible on the **Segments Status** pane of the SSL Visibility **Dashboard**. The Segment Comment is also propagated to SNMP through the updated Blue Coat SEGMENT-MIB.

Ruleset Deletion Check - SSL Visibility 3.9.4.1 checks if a ruleset is assigned to an active or inactive segment when a user attempts to delete the ruleset and warns the user appropriately before allowing the deletion. Appropriate warnings are also displayed if a user attempts to delete a rule in a ruleset assigned to an active or inactive segment. The **Policies > Rulesets** pane indicates segments to which a ruleset is assigned.

Configurable TLS Support - SSL Visibility 3.9.4.1 allows users to set the minimum and maximum versions of TLS supported for the following connections:

- SSL Visibility web server (WebUI)
- HSM appliances
- Alert mail notifications

  Note: SSL Visibility 3.9.4.1 uses TLS 1.2 for Alert mail notifications by default. If your e-mail server is configured to use TLS but does not support TLS 1.2, you must modify the Alert mail configuration after installing 3.9.4.1.

Configurable HSM Connection Limit - SSL Visibility 3.9.4.1 HSM connection setup adds an option to limit the maximum number of simultaneous resign connections per HSM. You can reduce the number of connections from the default (65) to avoid overloading when multiple HSMs are configured.

Debug traceroute Command - SSL Visibility 3.9.4.1 adds the `debug traceroute` and `debug traceroute6` commands to the Command Line Diagnostics (CLD) interface to assist troubleshooting in IPv4 and IPv6 environments.

Security Updates

SSL Visibility 3.9.4.1 provides important security updates that address Blue Coat Security Advisories SA112, SA121, SA126, and SA128. See Fixes in 3.9.4.1 for information.

SSL Visibility 3.9.4.1 no longer supports the use of NTP servers advertised by DHCP.

SSL Visibility 3.9.4.1 does not import RSA keys of less than 1024 bits for resigning CA certificates, and generates a warning when importing a 1024 bit key.

Due to backup format changes, backup files created with 3.9.4.1 cannot be restored on systems running earlier versions of SSL Visibility. (Backups created on appliances running earlier versions of SSL Visibility can be restored to appliances running version 3.9.4.1.)

Upgrading

SSL Visibility 3.9.4.1 supports the SV3800B-20 appliance. The SV3800B-20 appliance currently ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

After upgrading to SSL Visibility 3.9.4.1 from a 3.9.x release on an SV800 or SV3800B-20 appliance, you must update the BIOS.

After upgrading to SSL Visibility 3.9.4.1 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com
- cn=contentanalysis.es.bluecoat.com
- cn=contentanalysis-ma-u.es.bluecoat.com
- cn=list.bluecoat.com
- cn=license.soleranetworks.com
- cn=tracking.soleranetworks.com
- cn=sp.cwfservice.net
- cn=maa-updates.es.bluecoat.com
- cn=ti.soleranetworks.com
- cn=bto.bluecoat.com
- cn=hb.bluecoat.com
- cn=bluecoat.flexnetoperations.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.3 or later. Management Center 1.4.1.1 or earlier is not supported.

The files associated with this release are:

- sslv-3.9.4.1-12-bluecoat.patch
- sslv-3.9.4.1-12-bluecoat.nru
- sslv-3.9.4.1-12-bluecoat.nsu
- sslv_3.9.3.1_to_3.9.4.1_ca_certificates.p7b
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.9.4.1.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.7.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.4.1

SSL Visibility 3.9.4.1 adds the following new features. See the *Blue Coat SSL Visibility Admnistration and Deployment Guide, version 3.9.4.1* for information.

Online Query for Host Categorization Database

The Online Query sends a categorization request for any URL not already categorized in the installed Host Categorization Database (or in-memory ratings cache) to the cloud-based Blue Coat ratings service. The request is processed in the background, so the SSL Visibility appliance initially processes the URL as uncategorized. Once the in-memory ratings cache on the appliance has been updated with the Online Query results, future requests for the URL are categorized appropriately. New URLs categorized by the ratings service are added to the master copy of the Blue Coat Host Categorization database on the Blue Coat server, so future downloads of the database to the SSL Visibility appliance will include newly rated URLs from the ratings service. Note: Online Query is available only for the Blue Coat Host Categorization database.

Local Host Categorization Database

A Local Host Categorization database is a separate user-created database that is used by the SSL Visibility appliance in conjunction with the Blue Coat Host Categorization database. A Local database can have up to 200 defined categories and supports an unlimited number of URLs. The Local database is used in the same way as the Blue Coat Host Categorization database; the Local database categories are appended to the Blue Coat categories in the **Change Selected Categories** list used to create rules for policy enforcement. The Local database is downloaded to the SSL Visibility appliance from a customer-designated web server, from which it can be updated automatically or manually.

Updated SSL Sessions Tool

Version 1.6.7 of the off-box Python SSL Sessions tool is available. Use the SSL Sessions tool to parse SSL session log information within an exported session log generated by a Blue Coat SSL Visibility Appliance. The tool and tool documentation (sslsessions.pdf) are available on BlueTouchOnline (https://bto.bluecoat.com/) in Downloads. A *Getting Started Guide* is available on BTO Documentation.

Fixes in 3.9.4.1

Release Information

- **Release Date:** August 5, 2016
- **Build Number:** 94

SSL Visibility Appliance software 3.9.4.1 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2562	Addresses Blue Coat Security Advisory SA112.
SSLV-2498	Addresses libexpat1 security vulnerabilities. (CVE-2016-5300, CVE-2012-6702)
SSLV-2457	The rsyslog message "`warning: ~ action is deprecated, consider using the 'stop' statement instead`" no longer occurs in the system log.
SSLV-2424	Addresses dosfstools security vulnerabilities. (CVE-2016-4804, CVE-2015-8872)
SSLV-2422	Addresses libxml2 security vulnerabilities. (CVE-2016-4483, CVE-2016-4449, CVE-2016-4447, CVE-2016-3705, CVE-2016-3627, CVE-2016-2073, CVE-2016-1840, CVE-2016-1839, CVE-2016-1838, CVE-2016-1837, CVE-2016-1836, CVE-2016-1835, CVE-2016-1834, CVE-2016-1833, CVE-2016-1762, CVE-2015-8806)
SSLV-2375	Addresses libexpat1 security vulnerabilities. (CVE-2016-0718)
SSLV-2373	Addresses libarchive12 security vulnerabilities. (CVE-2016-1541)
SSLV-2364	Addresses Blue Coat Security Advisory SA128.
SSLV-2362	Addresses libtasn1-3 security vulnerabilities. (CVE-2016-4008)
SSLV-2358	Addresses Blue Coat Security Advisories SA121 and SA126.
SSLV-2230 SSLV-2211	Addresses security vulnerabilities in libpam-modules. (CVE-2015-3238, CVE-2014-2583, CVE-2013-7041)
SSLV-2312	Security update to increase the HTTP Strict Transport Security (HSTS) timeout and add IncludeSubdomains parameter.
SSLV-2184	Corrected an issue in which the Unfail button in the WebUI was unavailable following an App Port Failure.
SSLV-2165	Sessions with messages spanning multiple records no longer produce excessive entries in the system log.
SSLV-2140	Corrected an issue in which duplicate messages were displayed in remote syslog files and e-mail alerts.
SSLV-2134	Addresses cpio security vulnerabilities. (CVE-2016-2037, CVE-2015-1197)
SSLV-2119	Addresses libgcrypt11 security vulnerabilities. (CVE-2015-7511)
SSLV-2099	Sessions are no longer reported as "invalid issuer" because the certificate validation cache was reset.
SSLV-2091	Addresses libcurl3 security vulnerabilities. (CVE-2016-0755)
SSLV-674 SSLV-662	Import of RSA keys of less than 1024 bits for resigning CA certificates is no longer supported. SSL Visibility generates a warning when importing a 1024 bit key.

SSL Visibility Appliance 3.9.3.6

Release Information

- **Version:** 3.9.3.6
- **Build Number:** 12
- **Release Date:** October 20, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.3.6 build 12 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1
  - Fixes in 3.9.3.2
  - Fixes in 3.9.3.3

Changes in 3.9.3.6

SSL Visibility 3.9.3.6 correctly handles SSL connections to Google servers that use Elliptic Curve (EC) X25519 for the ECDHE cipher, introduced in Google Chrome version 50.

SSL Visibility 3.9.3.6 supports Google sessions using the updated ChaCha20-Poly1305 cipher suites. Connections to Google servers that use the new ciphers are no longer cut through as unknown cipher suites.

SSL Visibility 3.9.3.6 provides important security updates that address Blue Coat Security Advisories SA117 and SA123. See Fixes in 3.9.3.6 for information.

SSL Visibility 3.9.3.6 supports the SV3800B-20 appliance. The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

After upgrading to SSL Visibility 3.9.3.6 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.3. Management Center 1.4.1.1 or earlier is not supported.

The files associated with this release are:

- sslv-3.9.3.6-12-bluecoat.patch
- sslv-3.9.3.6-12-bluecoat.nru
- sslv-3.9.3.6-12-bluecoat.nsu
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.4.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.3.6

There are no new features in SSL Visibility 3.9.3.6.

Fixes in 3.9.3.6

Release Information

- **Release Date:** October 20, 2016
- **Build Number:** 12

SSL Visibility Appliance software 3.9.3.6 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2393	SSL Visibility now correctly updates the IP list when overlapping subnets are configured in IP list policy rules.
SSLV-2387	SSL Visibility now supports the IF-MIB `ifDescr` object, OID .1.3.6.1.2.1.2.2.1.2.
SSLV-2386	Early ACK responses for partial certificates sent to the SSL Visibility appliance are now sent in the absence of a server response in symmetric topologies, if required.
SSLV-2385	Sessions using the latest Google ChaCha20-Poly1305 cipher suites are now supported and are no longer cut through as unknown cipher suites.
SSLV-2384	SSL Visibility correctly handles SSL connections to Google servers that use Elliptic Curve (EC) X25519 for the ECDHE cipher, introduced in Google Chrome version 50.
SSLV-2383	Updated UTF-8 support in CA certificates.
SSLV-2382	SSL Visibility correctly handles window scale options in the TCP handshake.
SSLV-2381	Fixed a file descriptor leak that could occur when pushing policy with an HSM configured while the system was under load.
SSLV-2365	SSL Visibility 3.9.3.6-23 opens a maximum of four connections per resigning certificate when using a Hardware Security Module (HSM) for Certificate Authority (CA) key storage and digital signature operations.
SSLV-2345	Security update to address multiple vulnerabilities in OpenSSL, including compromise of TLS sessions, memory access, corruption, or depletion, and arbitrary code execution. (CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, and CVE-2016-2176) See Blue Coat Security Advisory SA123 for more information.
SSLV-2168	Security update to address multiple vulnerabilities in OpenSSL that could result in application crashes, denial of service, and arbitrary code execution. (CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800, and CVE-2016-2842) See Blue Coat Security Advisory SA117 for more information.

SSL Visibility Appliance 3.9.3.3

Release Information

- **Version:** 3.9.3.3
- **Build Number:** 6
- **Release Date:** March 1, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.3.3 build 6 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1
  - Fixes in 3.9.3.2

Changes in 3.9.3.3

SSL Visibility 3.9.3.3 provides an important bug fix and a security update that addresses Blue Coat Security Advisory SA114. See Fixes in 3.9.3.3 for information.

SSL Visibility 3.9.3.3 supports the new SV3800B-20 appliance. The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

After upgrading to SSL Visibility 3.9.3.3 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com

- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.3. Management Center 1.4.1.1 or earlier is not supported.

The files associated with this release are:

- sslv-3.9.3.3-6-bluecoat.patch
- sslv-3.9.3.3-6-bluecoat.nru
- sslv-3.9.3.3-6-bluecoat.nsu
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- ss.v_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.4.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.3.3

There are no new features in SSL Visibility 3.9.3.3.

Fixes in 3.9.3.3

Release Information

- **Release Date:** March 1, 2016
- **Build Number:** 6

SSL Visibility Appliance software 3.9.3.3 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2129	E-mail alerts are now correctly triggered by events in the system log.
SSLV-2126	Early ACK responses for partial certificates sent to the SSL Visibility appliance are now sent to the correct interface in asymmetric topologies.
SSLV-2125	Security update to address a vulnerability in DNS resolution routines in the GNU C Library (glibc). (CVE-2015-7547) See Blue Coat Security Advisory SA114 for more information.

SSL Visibility Appliance 3.9.3.2

Release Information

- **Version:** 3.9.3.2
- **Build Number:** 7
- **Release Date:** February 3, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.3.2 build 7 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6
  - Fixes in 3.9.2.1
  - Fixes in 3.9.2.2
  - Fixes in 3.9.3.1

Changes in 3.9.3.2

SSL Visibility 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 Visibility 3.9.3.2 release installs the new certificate required to access the Global Intelligence Network services. Following an upgrade to SSL Visibility 3.9.3.2, the Host Categorization functionality on SSL Visibility appliances will continue to operate without issue and upgraded appliances will be able to update the Host Categorization database.

SSL Visibility 3.9.3.2 supports the new SV3800B-20 appliance. The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

After upgrading to SSL Visibility 3.9.3.2 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com

- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.2. Management Center 1.4.1.1 or earlier is not supported.

This release for the SV800, SV1800, SV2800, SV3800, and SV3800B-20 systems also provides important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.9.3.2-7-bluecoat.patch
- sslv-3.9.3.2-7-bluecoat.nru
- sslv-3.9.3.2-7-bluecoat.nsu
- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- ss.v_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.4.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.3.2

There are no new features in SSL Visibility 3.9.3.2.

Fixes in 3.9.3.2

Release Information

- **Release Date:** February 3, 2016
- **Build Number:** 7

SSL Visibility Appliance software 3.9.3.2 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2097	SSL Visibility no longer caches Invalid certificate validation results for reused sessions.
SSLV-2096	Security update to correct vulnerabilities in OpenSSL. (CVE-2016-0701, CVE-2015-3197) This update also extends the "Logjam" vulnerability mitigation for TLS clients by increasing the Diffie-Hellman parameter handshake requirement to 1024 bits. (CVE-2015-4000) **Note:** The SSL Visibility 3.9.3.2 Open Source Attributions file does not list the updated version of OpenSSL. However, the OpenSSL version used in SSL Visibility 3.9.3.2 does include these updates.
SSLV-2089	Enhanced the ability for SSL Visibility to restart flows in which multiple packets are lost between endpoints.
SSLV-2085	Original Time to Live (TTL) value is now used when generating Early Acknowledgements.

SSL Visibility Appliance 3.9.3.1

Release Information

- **Version:** 3.9.3.1
- **Build Number:** 34
- **Release Date:** January 21, 2016

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.3.1 build 34 provides these fixes. See also:
    - Fixes in 3.7.0
    - Fixes in 3.7.1
    - Fixes in 3.7.1-71
    - Fixes in 3.7.3
    - Fixes in 3.7.4
    - Fixes in 3.8.0
    - Fixes in 3.8.1
    - Fixes in 3.8.2
    - Fixes in 3.8.2-406
    - Fixes in 3.8.2-409
    - Fixes in 3.8.3
    - Fixes in 3.8.4
    - Fixes in 3.8.5
    - Fixes in 3.8.6
    - Fixes in 3.9.2.1
    - Fixes in 3.9.2.2

Changes in 3.9.3.1

SSL Visibility 3.9.3.1 includes new features:

- Increased security for user session management
- TLS 1.2 support for HSM connections
- Updated SSL Sessions tool available

Failure Mode Options Change: In SSLV 3.9.3.1, the **Failure Action** (formerly **Software Failure Action**) configured in the **Failure Mode Options** for a segment also applies to application port failures for segments configured in Active-Inline Fail-to-Network (AI-FTN) mode. For segments configured in AI-FTN mode, with the **Failure Action** set to **Fail-to-Wire** (the default), traffic will be allowed to pass on all network ports in a segment when an application port in that segment goes down (i.e., link-down is detected). When the link has been restored for all application ports, all network ports in the segment will be restored according to the configured **Failure Mode Options**.

If **Fail-to-Wire** is configured as the **Failure Action**, all traffic is allowed to pass while the application port is down. To restore the pre-3.9.3.1 behavior and prevent traffic passing on the network while an application port is down, choose a non-default **Failure Action**, for example, **Drop Packets** or **Disable Interfaces**.

System log enhancement: SSL Visibility 3.9.3.1 provides bracketed alphabetic severity indicators at the beginning of exported system log entries. These characters replace the symbols used in previous releases. If you have scripts that rely on the old prefixes, please update to use the new prefixes. There is no change to the color coding of system log entries in the WebUI.

Severity	3.9.3.1	Previous
FATAL	[F]	!
ERROR	[E]	*
WARN	[W]	#
INFO	[I]	?
DEBUG	[D]	-
EXTRA	[X]	:
VERBOSE	[V]	>

SSL Visibility 3.9.3.1 supports the new SV3800B-20 appliance. The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

After upgrading to SSL Visibility 3.9.3.1 from a 3.8.x or 3.7.x release on an SV1800, SV2800, or SV3800 appliance, you must update the BIOS.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com
- cn=upload.bluecoat.com
- cn=remote-support.bluecoat.com
- cn=courier.sandbox.push.apple.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.3.1. Management Center 1.4.1.1 or earlier is not supported.

This release for the SV800, SV1800, SV2800, SV3800, and SV3800B-20 systems also provides important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.9.3.1-34-bluecoat.patch
- sslv-3.9.3.1-34-bluecoat.nru
- sslv-3.9.3.1-34-bluecoat.nsu

- sslv_3.9.2.1_to_3.9.3.1_ca_certificates.p7b
- ss.v_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.4.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.3.1

- SSL Visibility 3.9.3.1 terminates an active user session if the user is deleted or the user's roles are changed. A user session is not terminated if the user changes his/her own roles.
- SSL Visibility 3.9.3.1 adds TLS 1.2 support for connections to versions of the SafeNet Java HSM (formerly Luna SP) that use TLS 1.2.
- Version 1.6.4 of the off-box Python SSL Sessions tool is available. Version 1.6.4 fixes an issue with data export from the user interface. Use the SSL Sessions tool to parse SSL session log information within an exported session log generated by a Blue Coat SSL Visibility Appliance. The tool and tool documentation (sslsessions.pdf) are available on BlueTouchOnline (https://bto.bluecoat.com/) in Downloads. A *Getting Started Guide* is available on BTO Documentation.

Fixes in 3.9.3.1

Release Information

- **Release Date:** January 21, 2016
- **Build Number:** 34

SSL Visibility Appliance software 3.9.3.1 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-2061	Security update to correct vulnerabilities in Portable Network Graphics file library (libpng). (CVE-2015-8472, CVE-2015-8540)
SSLV-2058	Security update to correct vulnerabilities in use of MD5 in TLS 1.2 connections in Secure Socket Layer (SSL) cryptographic library and tools. (CVE-2015-7575)
SSLV-2055	Security update to correct vulnerabilities in use of MD5 in TLS 1.2 connections in GNU TLS. (CVE-2015-7575)
SSLV-2052	Security update to correct vulnerabilities in DHCP server, client, and relay. (CDE-2015-8605)
SSLV-2049	Security update to correct vulnerabilities in OpenSSH client experimental support for resuming connections. (CVE-2016-0777, CVE-2016-0778)
SSLV-2034	Fixed an issue in which the `debug ping` CLD command could cause high CPU usage.
SSLV-2018	Security update to correct vulnerabilities in libxml2. (CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317)
SSLV-2004 SSLV-2003	Security updates to correct vulnerabilities in OpenSSH authentication routines. (CVE-2015-5352, CVE-2015-5600, CVE-2015-6563, CVE-2015-6564) See Blue Coat Security Advisory SA104 for more information.
SSLV-1999	Security update to correct vulnerabilities in Secure Socket Layer (SSL) cryptographic library and tools. (CVE-2015-1794, CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196) See Blue Coat Security Advisory SA105 for more information.
SSLV-1994	Security update to correct vulnerabilities in GNU TLS library.
SSLV-1985	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.
SSLV-1978	Security update to correct vulnerabilities in Portable Network Graphics file library (libpng). (CVE-2012-3425, CVE-2015-7981, CVE-2015-8126)
SSLV-1937	The **ssldebug.log** file is correctly rotated and replaced after it reaches 200 MB.

SSL Visibility Appliance 3.9.2.2

Release Information

- **Version:** 3.9.2.2
- **Build Number:** 2
- **Release Date:** November 30, 2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.2.2 build 2 provides these fixes. See also:
    - Fixes in 3.7.0
    - Fixes in 3.7.1
    - Fixes in 3.7.1-71
    - Fixes in 3.7.3
    - Fixes in 3.7.4
    - Fixes in 3.8.0
    - Fixes in 3.8.1
    - Fixes in 3.8.2
    - Fixes in 3.8.2-406
    - Fixes in 3.8.2-409
    - Fixes in 3.8.3
    - Fixes in 3.8.4
    - Fixes in 3.8.5
    - Fixes in 3.8.6
    - Fixes in 3.9.2.1

Changes in 3.9.2.2

SSL Visibility 3.9.2.2 introduces support for the new SV3800B-20 appliance.

The SSL Visibility 3.9.2.2 patch release adds TLS 1.2 support for connections to versions of the SafeNet Java HSM (formerly Luna SP) that use TLS 1.2.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.2.2. Management Center 1.4.1.1 or earlier is not supported.

This patch release for the SV800, SV1800, SV2800, SV3800, and SV3800B-20 systems also provides important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.9.2.2-2-bluecoat.patch

The following files are available with the 3.9.2.1 release, if required:

- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b
- MIBS_SSLV-3.8.3.zip

Also available:

- ssldiags-1.1.0.zip
- sslsessions-1.6.3.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.2.2

SSL Visibility Appliance software 3.9.2.2 introduces support for the new SV3800B-20 appliance.

The SV3800B-20 is a new member of the SSL Visibility Appliance product family based on the SV3800 hardware. The SV3800B-20 provides greater decryption/re-encryption performance than the standard SV3800 model, due to the use of higher performance CPUs and increased system memory.

The SV3800B-20 installation and network interface configuration options are identical to the SV3800 appliance. All user installable components (power supply modules and Netmods) for the SV3800 are compatible with the SV3800B-20.

Fixes in 3.9.2.2

Release Information

- **Release Date:** November 30, 2015
- **Build Number:** 2

SSL Visibility Appliance software 3.9.2.2 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1971	Security update to correct vulnerabilities in libxml2. (CVE-2015-1819, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035)
SSLV-1964	Security update to correct vulnerabilities in the Network Time Protocol (NTP) and its utility programs. (CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7850, CVE-2015-7852, CVE-2015-7853, CVE-2015-7855, CVE-2015-7871) See Blue Coat Security Advisory SA103 for more information.
SSLV-1963	Security update to correct vulnerabilities in Kerberos. (CVE-2002-2443, CVE-2014-5355, CVE-2015-2694, CVE-2015-2695, CVE-2015-2696, CVE-2015-2697, CVE-2015-2698)

SSL Visibility Appliance 3.9.2.1

Release Information

- **Version:** 3.9.2.1
- **Build Number:** 18
- **Release Date:** November 12, 2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800, SV3800B-20

Fixes in 3.9.x.x

- 3.9.2.1 build 18 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5
  - Fixes in 3.8.6

Changes in 3.9.2.1

SSL Visibility 3.9.2.1 introduces support for the new SV3800B-20 appliance. The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed, and requires SSL Visibility 3.9.2.1 or later to run.

Blue Coat recommends adding the following web sites to the Unsupported Sites list, if they are not already present:

- cn=abrca.bluecoat.com
- cn=bto-services.es.bluecoat.com
- cn=device-services.es.bluecoat.com
- cn=subscription.es.bluecoat.com
- cn=validation.es.bluecoat.com

If you perform a patch upgrade, you must manually add the sites to the list. If you restore a previous policy configuration that did not include the new entries in the list, the current policy is overwritten, and the sites must be added again.

To view the complete list or to add sites to the list, open **Policies > Subject/Domain Names List** in the WebUI and select **sslng-unsupported-sites** in the **Subject/Domain Names** Lists panel.

Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.9.2.1. Management Center 1.4.1.1 or earlier is not supported.

This general release for the SV800, SV1800, SV2800, SV3800, and SV3800B-20 systems also provides important vulnerability and bug fixes.

Note: The SV3800B-20 appliance ships with SSL Visibility 3.9.2.1 installed.

The files associated with this release are:

- sslv-3.9.2.1-18-bluecoat.patch
- sslv-3.9.2.1-18-bluecoat.nru
- sslv-3.9.2.1-18-bluecoat.nsu
- sslv_3.8.3_to_3.9.2.1_ca_certificates.p7b
- sslv_3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.3.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.9.x.x.

Features in 3.9.2.1

SSL Visibility Appliance software 3.9.2.1 introduces support for the new SV3800B-20 appliance.

The SV3800B-20 is a new member of the SSL Visibility Appliance product family based on the SV3800 hardware. The SV3800B-20 provides greater decryption/re-encryption performance than the standard SV3800 model, due to the use of higher performance CPUs and increased system memory.

The SV3800B-20 installation and network interface configuration options are identical to the SV3800 appliance. All user installable components (power supply modules and Netmods) for the SV3800 are compatible with the SV3800B-20.

Fixes in 3.9.2.1

Release Information

- **Release Date:** November 12, 2015
- **Build Number:** 18

SSL Visibility Appliance software 3.9.2.1 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1867	TLS 1.2 is now correctly detected as SSL when searching in SSLv2 records.
SSLV-1854	SSL Visibility VLAN translation now correctly translates SNAP encapsulated packets.
SSLV-1847	Increased the flow table size.
SSLV-1814	Corrected an issue in which running a packet capture could interrupt VLAN translated traffic.
SSLV-1812	Corrected an issue in which IPv4 Access Control Lists did not take effect for several minutes.
SSLV-1811	Corrected an issue that caused certificate verification errors with ECDSA resigned flows.
SSLV-1809	The User Management screens in the WebUI now correctly show more than ten users.
SSLV-1607	Corrected an issue in which the High Availability Manual Reset option behaved inconsistently in Passive-Inline deployments.
SSLV-1454	Corrected an issue in which power-off fail-to-wire (FTW) did not work on the SV1800-F fiber interface.
SSLV-875	Corrected an issue in which the appliance became unmanageable from the WebUI if the Host-name was set to localhost.localdomain and the configured DNS server became unreachable.

SSL Visibility Appliance 3.8.6

Release Information

- **Version:** 3.8.6
- **Build Number:** 4
- **Release Date:** September 10, 2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.6 build 4 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3
  - Fixes in 3.8.4
  - Fixes in 3.8.5

Changes in 3.8.6

SSL Visibility 3.8.6 includes new features:

- Support for 64-bit SNMP octet and packet counters.
- Updated versions of SSL Diagnostics and SSL Sessions tools.

In order to enhance security, TLS v1.0 is not supported in the SSL Visibility WebUI. The WebUI supports TLS v1.1 and TLS v1.2. As a result, Blue Coat Management Center 1.4.2.1 or later is required for monitoring appliances running SSL Visibility 3.8.6. Management Center 1.4.1.1 or earlier is not supported.

This general release for the SV800, SV1800, SV2800, and SV3800 systems also provides a number of important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.8.6-4-bluecoat.patch
- sslv-3.6-to-3.8.6-4-bluecoat.patch
- sslv-3.8.6-4-bluecoat.nru
- sslv-3.8.6-4-bluecoat.nsu
- sslv-3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b
- sslv_3.6.3_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-1.1.0.zip
- sslsessions-1.6.2.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.x.

Features in 3.8.6

SSL Visibility Appliance software 3.8.6 introduces the following enhancements and new features.

- SSL Visibility 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 Blue Coat SSL Visibility Appliance. The tool and tool documentation (sslsessions.pdf) are availableon BlueTouchOnline (https://bto.bluecoat.com/) in Downloads. A *Getting Started Guide* is available on BTO Documentation.
- 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 Blue Coat SSL Visibility Appliance. The tool and tool documentation (ssldiags.pdf) are available on on BlueTouchOnline (https://bto.bluecoat.com/) in Downloads. A *Getting Started Guide* is available on BTO Documentation.

Fixes in 3.8.6

Release Information

- **Release Date:** 9/10/2015
- **Build Number:** 4

SSL Visibility Appliance software 3.8.6 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1766	Fixed an issue that prevented connections to Google Chrome services (such as Gmail) when SSL Visibility was decrypting the traffic.
SSLV-1693	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**.
SSLV-1689 SSLV-1667 SSLV-1666 SSLV-1665 SSLV-1664 SSLV-1653	Fixed potential memory leaks in PKI handling routines.
SSLV-1688	Fixed an issue in which SNMP traps could be sent for unused interfaces.
SSLV-1657	Security update to correct vulnerabilities in the SQLite v3 library. (CVE-2013-7443, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416)
SSLV-1655	Security updates to correct vulnerabilities in Perl 5 Compatible Regular Expression Library (PCRE). (CVE-2014-8964, CVE-2015-2325, CVE-2015-2326, CVE-2015-3210, CVE-2015-5073)
SSLV-1552 SSLV-1553	Security updates to correct vulnerabilities in Python 2.7.x. (CVE-2013-1752, CVE-2013-1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185)
SSLV-1548	Fixed a certificate validation timeout issue that could produce **Invalid Issuer** errors.
SSLV-1522	Fixed a memory leak in a statistics collection routine.
SSLV-1341	Fixed a condition that produced a **CSRF tokens required** or **CSRF token mismatch** error when logging in after a WebUI session had expired.

SSL Visibility Appliance 3.8.5

Release Information

- **Version:** 3.8.5
- **Build Number:** 16
- **Release Date:** 7/24/2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.5 build 16 provides these fixes. See also:
    - Fixes in 3.7.0
    - Fixes in 3.7.1
    - Fixes in 3.7.1-71
    - Fixes in 3.7.3
    - Fixes in 3.7.4
    - Fixes in 3.8.0
    - Fixes in 3.8.1
    - Fixes in 3.8.2
    - Fixes in 3.8.2-406
    - Fixes in 3.8.2-409
    - Fixes in 3.8.3
    - Fixes in 3.8.4

Changes in 3.8.5

SSL Visibility 3.8.5 includes the following changes:

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

  IMPORTANT: If SSL traffic traverses the SSL visibility 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

  IMPORTANT: 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 SSLV WebUI. The SSLV WebUI supports TLS v1.1 and TLS v1.2.
  As a result, Blue Coat Management Center 1.4.1.1 or earlier is not supported for monitoring appliances running SSLV 3.8.5. Contact Customer Support for more information.

This general release for the SV800, SV1800, SV2800, and SV3800 systems includes no new features. It provides a number of important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.8.5-16-bluecoat.patch
- sslv-3.6-to-3.8.5-16-bluecoat.patch
- sslv-3.8.5-16-bluecoat.nru
- sslv-3.8.5-16-bluecoat.nsu
- sslv-3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b
- sslv_3.6.3_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-0.1.0.zip
- sslsessions-1.6.1.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.x.

Fixes in 3.8.5

Release Information

- **Release Date:** 7/24/2015
- **Build Number:** 16

SSL Visibility Appliance software 3.8.5 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1529	Improved inter-process communication to reduce the frequency of "No such file or directory" error messages.
SSLV-1503	Security update to correct vulnerabilities in OpenSSL. (CVE-2014-8176, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792)
SSLV-1490	Users logged in under Terminal Access Controller Access-Control System (TACACS) can add licenses if the user has the appropriate roles.
SSLV-1459	Reduced the frequency of "Alert 86 (invalid_fallback)" error messages error messages when using a web browser.
SSLV-1445	Security improvement to address the "Logjam" vulnerability. The SSLV WebUI now rejects Diffie-Hellman keys smaller than 768 bits. (CVE-2015-4000)
SSLV-1412	Security improvement to enable TLS v1.2 by default in the SSLV WebUI.
SSLV-1373	Security update to address vulnerabilities in `curl`. (CVE-2015-3143, CVE-2015-3144, CVE-2015-3145, CVE-2015-3148, CVE-2015-3153)
SSLV-1361	Fixed an issue in which the SSLV appliance could forward a packet dropped by an IPS if the stream is out of order.
SSLV-1292	Fixed an issue in which a TCP flow could stall when an upstream server missed client acknowledgements.
SSLV-1252	The bootstrap process no longer reverts to local storage if a USB drive is not inserted into the SSLV 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.

SSL Visibility Appliance 3.8.4

Release Information

- **Version:** 3.8.4
- **Build Number:** 15
- **Release Date:** 5/11/2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.4 build 15 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409
  - Fixes in 3.8.3

Changes in 3.8.4

- Software SSLV 3.8.4 includes new features: enable/disable rule, resigning CA certificate chain, feedback timeout setting.
- The new **Appliance Feedback Options** panel replaces the **Plaintext Marker** panel on the **Segments** window. See the new features.
- When changing a password, the system now prevents a user from reusing previous passwords.

This general release for the SV800, SV1800, SV2800, and SV3800 systems includes several new features. It also provides a number of important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.8.4-15-bluecoat.patch
- sslv-3.6-to-3.8.4-15-bluecoat.patch
- sslv-3.8.4-15-bluecoat.nru
- sslv-3.8.4-15-bluecoat.nsu
- sslv-3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b
- sslv_3.6.3_to_3.8.0_ca_certificates.p7b

Also available:

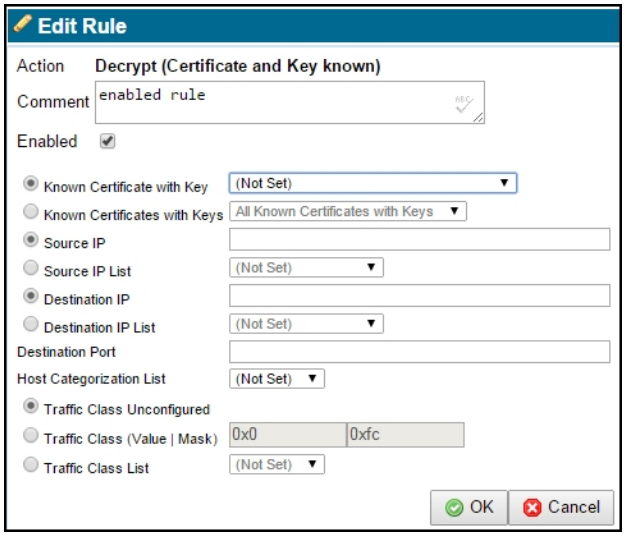
- MIBS_SSLV-3.8.3.zip
- ssldiags-0.1.0.zip
- sslsessions-1.6.1.zip

Known Issues

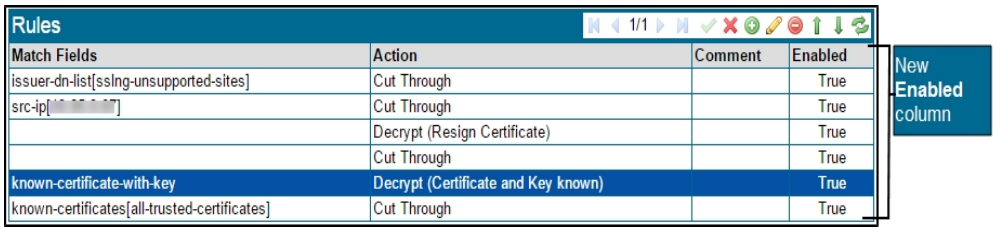
See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.x.

Features in 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.



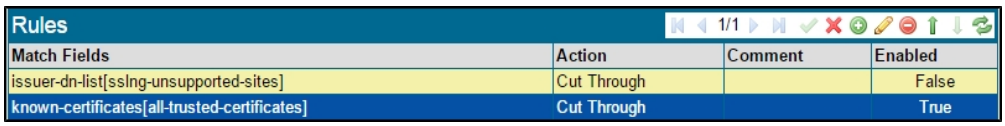
The setting is also shown per rule in the **Rulesets > Rules** panel, as **True** (enabled) or **False** (disabled) in the new **Enabled** column.



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.

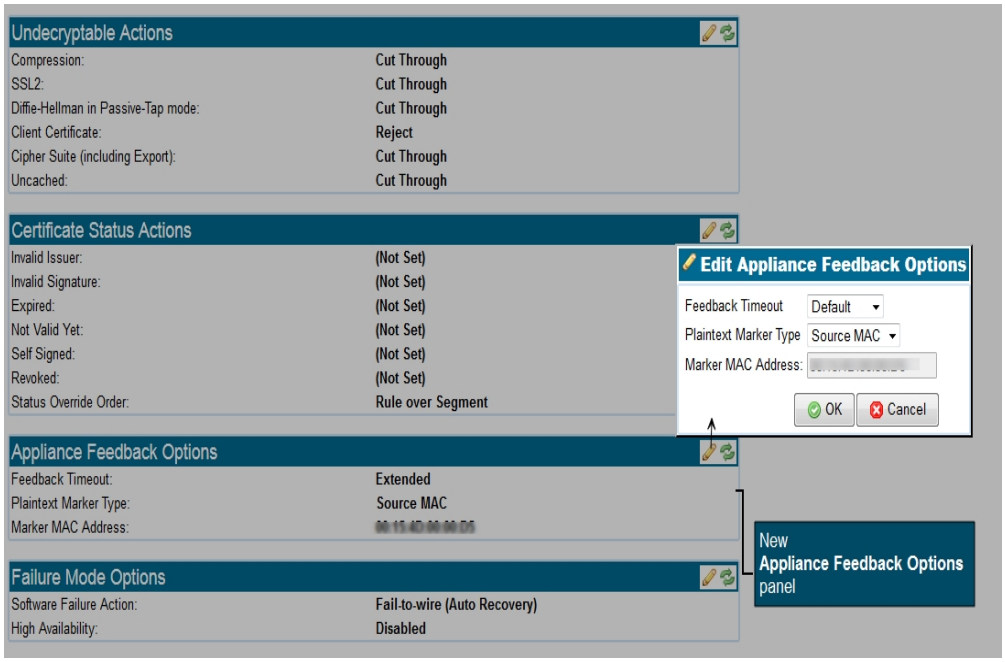
> **New Tools Note**
>
> Two new tools display in the **Rules** panel, as part of the disable rules feature:
>
> - Click Enable Rule ( ) to enable a highlighted disabled rule.
> - Click Disable Rule ( ) to disable the highlighted rule.

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.

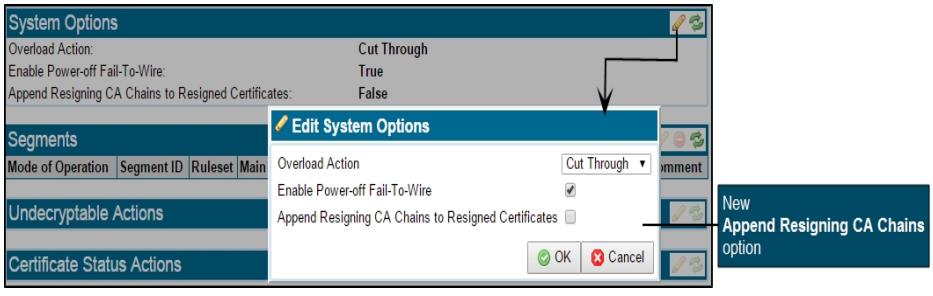
- **Feedback Timeout Setting**: SSLV 3.8.4 supports a new loopback feedback timer. The new **Appliance Feedback Options** panel replaces the **Plaintext Marker** panel on the **Segments** window. **Feedback Timeout** is a new setting in that panel, which determines how long the SSL Visibility Appliance 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**: SSLV 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:

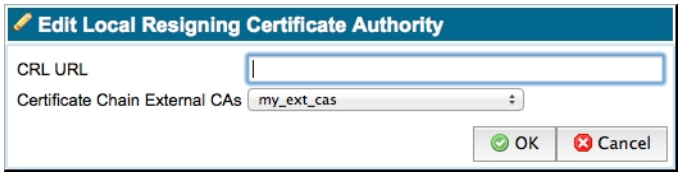
  1. On the **Segment > System Options** panel, check the new **Append Resigning CA Chains to Resigned Certificates** option. The SSL Visibility Appliance will include the resigning CA certificate chain (configured in the PKI store) in the SSL session.



  2. 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.

3. 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.

4. 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.

5. 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 Visibility Appliance will load the partial CA chain and include it with resigned certificates in inspected SSL sessions.

Fixes in 3.8.4

Release Information

- **Release Date:** 5/11/2015
- **Build Number:** 15

SSL Visibility Appliance software 3.8.4 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1327	Legacy browser versions now correctly display the declared content type and sets the `X-Content-Type-Options` to `nosniff`.
SSLV-1326	The web browser's cross-site scripting prevention filter is now correctly enabled.
SSLV-1322	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).
SSLV-1319	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.
SSLV-1317	Sensitive system error messages are no longer seen on the SSL Visibility Appliance.
SSLV-1312	Added cross-site request forgery (CSRF) protection. Cookies used in user requests to sites are protected transparently.
SSLV-1311	Sensitive cookies are now marked as such, so they may not be modified by client-side scripting languages. This reduces users' susceptibility to web-based attack vectors.
SSKV-1310	Sensitive cookies are marked as secure, so they may no longer be transmitted over unencrypted connections, potentially exposing their values to attackers.
SSLV-1309	The SSL Visibility Appliance now includes protections against certain frame-based attacks such as clickjacking and cross-frame scripting.
SSLV-1308	A user's session ID is now renewed after login, reducing the vulnerability of a session to hijacking.
SSLV-1283	Corrected an issue that could cause lockups during maintenance of the resigned certificate cache.
SSLV-1280	When configuring IPv6 DHCP, the appliance now allows a default gateway to be set.
SSLV-1275	When an appliance is rebooted only once after applying several management network changes at the same time, the appliance no longer stops responding.

SSL Visibility Appliance 3.8.3

Release Information

- **Version:** 3.8.3
- **Build Number:** 120
- **Release Date:** 4/03/2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.3 build 120 provides these fixes. See also:
  - Fixes in 3.7.0
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406
  - Fixes in 3.8.2-409

Changes

Changes in 3.8.3

- Software SSLV 3.8.3 includes these new features.
- Updates to the **Dashboard** provide additional **Power Supply** status, and more granular disk utilization information.
- 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 Visibility 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
SV800-250M-C SV800-500M-C	0ACDI005	1.30	
SV1800-C/F	AQNIS100	4.00	
SV2800	S5500.86B.01.00.0061.030920121535	0.60	BIOS: Only the four unique digits display on the LCD. For example, "0061."
SV3800	S5500.86B.01.00.0061.030920121535	0.60	BIOS: Only the four unique digits display on the LCD. For example, "0061."

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 Visibility Appliance has a new Blue Coat root OID based on the prefix .1.3.6.1.4.1.3417. The Blue Coat SSL Visibility Appliance models are now represented by this root OID plus the following OID extensions:
  - 1.5.1 = SV800
  - 1.5.2 = SV1800
  - 1.5.3 = SV2800
  - 1.5.4 = SV3800

This general release for the SV800, SV1800, SV2800, and SV3800 systems includes several new features, as well as providing a number of important vulnerability and bug fixes.

The files associated with this release are:

- sslv-3.8.3-120-bluecoat.patch
- sslv-3.8.3-120-bluecoat.nru
- sslv-3.8.3-120-bluecoat.nsu
- sslv-3.8.0_to_3.8.3_ca_certificates.p7b
- sslv_3.7.0_to_3.8.0_ca_certificates.p7b

Also available:

- MIBS_SSLV-3.8.3.zip
- ssldiags-0.1.0.zip
- sslsessions-1.6.1.zip

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.x.

Features in 3.8.3

SSL Visibility Appliance software 3.8.3 introduces the following enhancements and new features.

- 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 Visibility 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 Blue Coat SSL Visibility 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 Blue Coat SSL Visibility 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.

Fixes in 3.8.3

Release Information

- **Release Date:** 4/03/2015
- **Build Number:** 120

SSL Visibility Appliance software 3.8.3 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1236	When running a packet capture on an SV2800 or SV3800, existing flows are cut-through, so traffic is no longer dropped.
SSLV-1203	The SSL Visibility Appliance no longer intermittently forwards packets dropped by the attached appliance.
SSLV-1167	TCP packets are no longer received at the client out of order.
SSLV-1161	Recent SV1800-C/-F 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 SSLV 3.8.3, run the `bios update` CLD command. The upgrade may take up to an hour; do not interrupt the process.
SSLV-1104	When performing a manual test, or if an HSM resigning failure occurs, the corresponding System Log message now correctly appears in red text.
SSLV-975	After upgrading to SSLV-3.8.3, you will no longer see the message `mount: special device /dev/dom2 does not exist` during the boot process.
SSLV-937	When running packet captures, the `SSL_CAPTURE_ERROR` is no longer seen, and captures occur correctly.
SSLV-717	Cut through, reject, and drop rules matching Anonymous Diffie-Hellman flows are no longer bypassed.
SSLV-712	Appliances no longer experience intermittent disruption to new flows when a new Host Categorization database is loaded.
SSLV-485	The management port on an SV800 no longer resets to 10 Mbps following a power restoration if you use the power button prior to the green status LED illuminating.

SSL Visibility Appliance 3.8.2-409

Release Information

- **Version:** 3.8.2
- **Build Number:** 409
- **Release Date:** 3/02/2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.2 build 409 provides these fixes. See also:
  - Fixes in 3.7.0,
  - Fixes in 3.7.1
  - Fixes in 3.7.1-71
  - Fixes in 3.7.3
  - Fixes in 3.7.4
  - Fixes in 3.8.0
  - Fixes in 3.8.1
  - Fixes in 3.8.2
  - Fixes in 3.8.2-406

Changes

- There are no new features in SSLV 3.8.2 build 409.

This maintenance release for the SV800, SV1800, SV2800, and SV3800 systems provides critical fixes including a memory leak fix associated with Host Categorization policy. It also includes a new version of the SV800 BMC firmware, which resolves a freeze on boot issue seen on SV800s.

After upgrading to 3.8.2-409 on an SV800, 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 files associated with this release are:

- sslv-3.8.2-409-bluecoat.patch
- sslv-3.6-to-3.8.2-409-bluecoat.patch
- sslv-3.8.2-409-bluecoat.nru
- sslv-3.8.2-409-bluecoat.nsu

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.x.

Fixes in 3.8.2-409

Release Information

- **Release Date:** 3/02/2015
- **Build Number:** 409

SSL Visibility Appliance software 3.8.2-409 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1175	Resolved a memory leak issue associated with Host Categorization policy.
SSLV-1050	SV3800s in an Active-Inline Fail to Appliance deployment with a Cut Through rule now correctly forward `server hellos`.
SSLV-1048	New BMC software version 1.30 resolves an issue where the SV800 sometimes froze on booting.
SSLV-795	The Active-Inline attached appliance correctly receives the SSL ServerHello message for cut-through SSL sessions using 4096-bit RSA keys.

SSL Visibility Appliance 3.8.2-406

Release Information

- **Version:** 3.8.2
- **Build Number:** 406
- **Release Date:** 1/30/2015

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.2 build 406 provides these fixes.
  See also Fixes in 3.7.0, Fixes in 3.7.1, Fixes in 3.7.1-71, Fixes in 3.7.3, Fixes in 3.7.4, Fixes in 3.8.0, Fixes in 3.8.1, and Fixes in 3.8.2.

Changes

- There are no new features in SSLV 3.8.2 build 406.

This maintenance release for the SV800, SV1800, SV2800, and SV3800 systems provides critical fixes, including the following:

- Ghost vulnerability (CVE-2015-0235)
- Traffic from Chrome on Windows to Google servers that used an experimental TLS extension was automatically cut through and could not be inspected. This traffic can now be inspected, and the automatic cut through no longer occurs.

The files associated with this release are:

- sslv-3.8.2-406-bluecoat.patch
- sslv-3.6-to-3.8.2-406-bluecoat.patch
- sslv-3.8.2-406-bluecoat.nru

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.2.

Fixes in 3.8.2-406

Release Information

- **Release Date:** 1/30/2015
- **Build Number:** 406

SSL Visibility Appliance software 3.8.2-406 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-1107	Fixed the Ghost vulnerability (CVE-2015-0235).
SSLV-1089	The SSL Visibility appliance no longer forwards invalid `Hello` messages, consuming resources, due to a certificate chain issue.
SSLV-1086	Resolved an issue where **Invalid issuer** was incorrectly displayed in a Passive-Inline deployment
SSLV-1084	HSM CA status now shows the validity of the signatures returned on a connection.
SSLV-1073	Addressed the OpenSSH Denial of Service vulnerability (CVE-2010-5107).
SSLV-989	The appliance no longer experiences slow down and high memory utilization.
SSLV-863	The SSL Visibility 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).
SSLV-523	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.

SSL Visibility Appliance 3.8.2

Release Information

- **Version:** 3.8.2
- **Build Number:** 301
- **Release Date:** 11/23/2014

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.2 provides these fixes.
  See also Fixes in 3.7.0, Fixes in 3.7.1, Fixes in 3.7.1-71, Fixes in 3.7.3, Fixes in 3.7.4, Fixes in 3.8.0, and Fixes in 3.8.1.

Changes

- There are no new features in SSLV 3.8.2.

This maintenance release for the SV800, SV1800, SV2800, and SV3800 systems provides critical fixes, including a fix for an issue in which SSL Visibility SV2800 and SV3800 systems might fail to boot with software versions 3.7.x, 3.8.0, and 3.8.1.

The files associated with this release are:

- sslv-3.8.2-301-bluecoat.patch
- sslv-3.6-to-3.8.2-301-bluecoat.patch
- sslv-3.8.2-301-bluecoat.nru

Important

See the Blue Coat Technical Alert SSL Visibility SV2800 and SV3800 systems may not boot with software versions 3.7.x, 3.8.0, and 3.8.1 for more information, including serial numbers of the affected products.

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.2.

Fixes in 3.8.2

Release Information

- **Release Date:** 11/23/2014
- **Build Number:** 301

SSL Visibility Appliance software 3.8.2 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-966	Fixed an issue in which SSL Visibility SV2800 and SV3800 systems might fail to boot with software versions 3.7.x, 3.8.0, and 3.8.1.
SSLV-926	Multiple VLAN tags in QinQ Ethernet headers are now handled correctly.
SSLV-923	TCP flows no longer stall due to advertising a window larger than the previously seen receive window.
SSLV-917	Fixed an issue in which SSL packet capture would not work on some ports on the SV3800 appliance.

SSL Visibility Appliance 3.8.1

Release Information

- **Version:** 3.8.1
- **Build Number:** 158
- **Release Date:** 10/09/2014

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.1 provides these fixes.
  See also Fixes in 3.7.0, Fixes in 3.7.1, Fixes in 3.7.1-71, Fixes in 3.7.3, Fixes in 3.7.4, and Fixes in 3.8.0.

Changes

- There are no new features in SSLV 3.8.1.

This maintenance release for the SV800, SV1800, SV2800, and SV3800 systems provides critical fixes, including the newly discovered "Shell Shock" vulnerability (CVE-2014-6271 and CVE-2014-7169) in the GNU Bourne Again shell (Bash) command interpreter used in Linux systems.

The files associated with this release are:

- sslv-3.8.1-158-bluecoat.patch
- sslv-3.8.1-158-bluecoat.nru

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.1..

Fixes in 3.8.1

Release Information

- **Release Date:** 10/09/2014
- **Build Number:** 158

SSL Visibility Appliance software 3.8.1 contains the following fixes.

Resolved Issues

Issue #	Description
SLV-823	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). See Blue Coat Security Advisory SA82 for more information.
SSLV-781	Loss of management network connectivity no longer occurs when IPv6 address mode is configured for DHCP.

SSL Visibility Appliance 3.8.0

Release Information

- **Version:** 3.8.0
- **Build Number:** 150
- **Release Date:** 09/25/2014

Compatible With

- **Hardware:** SV800, SV1800, SV2800, SV3800

Fixes in 3.8.x

- 3.8.0 provides these fixes.

  See also Fixes in 3.7.0, Fixes in 3.7.1, Fixes in 3.7.1-71, Fixes in 3.7.3,, and Fixes in 3.7.4.

Changes

Changes in 3.8.0

- Software version 3.8.0 introduces these New Features in 3.8.0.
- The new SV800 hardware platform is introduced with this release. The platform is available in two models, the SV800-500M-C and the SV800-250M-C.
- The Dashboard panel graphic for the SV1800 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 Visibility Appliance license may now be exported from the **License** window.
- The SSL Visibility Appliance now has a Blue Coat root OID:
  - 14501.12 = Blue Coat SSL Visibility Product Family
  - 14501.12.1 = SV800
  - 14501.12.2 = SV1800
  - 14501.12.3 = SV2800
  - 14501.12.4 = SV3800

The files associated with this release are:

- sslv-3.8.0-150-bluecoat.patch
- sslv-3.8.0-150-bluecoat.nru

This general release for the newly introduced SV800, as well as the SV1800, SV2800, and SV3800 systems, includes several new features, as well as addresses multiple issues.

Known Issues

See Known Issues for the issues Blue Coat is aware of in SSL Visibility Appliance 3.8.0.

Features in 3.8.0

SSL Visibility Appliance software 3.8.0 introduces the following enhancements and new features.

- Luna SP HSM (now SafeNet Java HSM) support enables the SSL Visibility 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 concurrently on the management network. IPv6 is supported in the following configuration modes: SLAAC, SLAAC + Stateless DHCP, 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.

Fixes in 3.8.0

Release Information

- **Release Date:** 09/25/2013
- **Build Number:** 150

SSL Visibility Appliance software 3.8.0 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-773	Resolved the issue described in SSLV-276, 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.
SSLV-701	Resolved an issue that resulted in a fault when activating policy.
SSLV-614	Resolved a case where a segment did not recover on software failure.
SSLV-401	First-time boot no longer takes up to 5 additional minutes if no network cable is plugged into the management network port
SSLV-335	Resolved an issue where all platform configuration changes required rebooting the appliance in order to take effect.
SSLV-185	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.
SSLV-63	The following characters are now allowed in alert e-mail addresses: !, #, $, %, &, ‘, *, +, /, =, ?, ^, `, {, }, |, ~

SSL Visibility Appliance 3.7.4

Release Information

- **Version:** 3.7.4
- **Build Number:** 31
- **Release Date:** 08/22/2014

Compatible With

- **Hardware:** SV1800, SV2800, SV3800

Fixes in 3.7.4

- 3.7.4 provides these fixes. See also Fixes in 3.7.0, Fixes in 3.7.1, Fixes in 3.7.1-71, and Fixes in 3.7.3.

Changes in 3.7.4

- SSL Visibility Appliance 3.7.4 contains no new features.

This maintenance release for the SV1800, SV2800, and SV3800 systems addresses multiple issues, including an important issue with how the appliance handles Online Certificate Status Protocol (OCSP) stapling. In addition, this version includes fixes for a number of publicly disclosed vulnerabilities in standard libraries. Due to these issues, Blue Coat strongly recommends upgrading all systems to software version 3.7.4. Previous SSL Visibility Appliance software versions will shortly become unavailable.

The files associated with this release are:

- sslv-3.7.4-31-bluecoat.patch
- sslv-3.6-to-3.7.4-31-bluecoat.patch
- sslv-3.7.4-31-bluecoat.nru

Known Issues

Blue Coat is aware of these Known Issues in SSL Visibility Appliance 3.7.4.

Fixes in 3.7.4

Release Information

- **Release Date:** 08/22/2013
- **Build Number:** 31

SSL Visibility Appliance software 3.7.4 contains the following fixes.

Resolved Issues

Issue #	Description
SSLV-692	When an SSL Visibility appliance recovers from an overload condition it no longer flags some SSL sessions with the "Invalid cryptographic response" error code.
SSLV-677	Corrected an issue that exposed the following ports on the management interface: 9001, 9002, 9003, 9009 and 9010
SSLV-672	In Passive Inline mode, copy ports now correctly see Server Hello packets with a "cut-through" rule.
SSLV-669	Corrected vulnerabilities identified in the Ubuntu security notice USN-2275-1: CVE-2014-3477, CVE-2014-3532, CVE-2014-3533
SSLV-668	Corrected vulnerabilities identified in the Ubuntu security notice USN-2294-1: CVE-2014-3467, CVE-2014-3468, CVE-2014-3469
SSLV-667	Corrected vulnerabilities identified in the Ubuntu security notice USN-2306-1: CVE-2013-4357, CVE-2013-4458, CVE-2013-0475, CVE-2013-4043
SSLV-666	Corrected vulnerabilities identified in the Ubuntu security notice USN-2308-1: 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
SSLV-639	Corrected handling of dates in OCSP Response fields.
SSLV-634	Fixed an issue in which duplicate client/server hello packets were issued in passive-inline deployment for certain cut-through SSL flows.
SSLV-629	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.
SSLV-625/623/620/613	Corrected several memory allocation issues.
SSLV-614	Corrected an issue where a segment did not recover on software failure.
SSLV-60	The command line diagnostic interface can now be used during the bootstrap phase to set IP configuration on the management network interface.

Fixes in 3.7.3

Release Information

- **Release Date:** 07/21/2014
- **Build Number:** 8

Resolved Issues

Issue #	Description
SSLV-276	Resolved an issue in which the SSL Visibility appliance became unusable and GUI timeouts occurred when navigating screens, requiring a manual reboot of the appliance to recover.
SSLV-439	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.
SSLV-453	Resolved an issue where IP fragments would not pass successfully through the SSL Visibility Appliance.
SSLV-454	Resolved an issue where incorrect processing of IP fragments sometimes lead to a crash requiring a manual restart.
SSLV-470	Resolved an issue that resulted in NFE 0 overload messages and caused the SSL Visibility Appliance to stop decrypting.
SSLV-475	The SSL Debug log now rotates correctly. Previously, debug logs could fill up the internal disk.
SSLV-498	Addressed OpenSSL vulnerability CVE-2014-0224.
SSLV-513 / SSLV-565	Resolved an issue that prevented proper startup of the appliance after a patch upgrade.

Fixes in 3.7.1-71

Release Information

- **Release Date:** 04/29/2014
- **Build Number:** 71

SSL Visibility Appliance software 3.7.1-71 contains the following fix. This patch release addresses the HeartBleed exploit, protecting against it for SSL traffic passing through and inspected by the SSL Visibility 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 Issues

Description
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.

Fixes in 3.7.1

Release Information

- **Release Date:** 04/15/2014
- **Build Number:** 70

SSL Visibility Appliance software 3.7.1 contains the following fixes.

Resolved Issues

Description
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 Visibility 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.*.livefilestore.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 Visibility 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.

SSL Visibility Appliance 3.7.0

Release Information

- **Release Date:** 04/02/2014
- **Build Number:** 68

Compatible With

- **Hardware:** SV1800, SV2800, SV3800

Fixes in 3.7.0

- 3.7.0 provides these fixes.

Changes in 3.7.0

- Software version 3.7.0 introduces these New Features in 3.7.0.
- Appliance licenses are required as of 3.7.0. SSL Visibility Appliance customers will receive a license via the Blue Coat Licensing Portal. New customers can download a license once they receive their SSL Visibility Appliance. It is non-trivial to downgrade from 3.7.0 to a previous release; it is recommended to have the license file available before starting the upgrade process.
- A new **License** menu item appears in the **Platform** menu, and license status is presented via an icon in the main window footer (next to the System, Load and Network icons). See the *Blue Coat Systems SV2800 and SV3800 Administration Guide* for full details.

The SSL Visibility Appliance license must be installed in the following scenarios:

- After upgrading to 3.7 from 3.6.x
- On initial setup of a new appliance
- After a factory-reset, the license will not be restored

The SSL Visibility Appliance requires a license to be fully operational. Before you can license your SSL Visibility Appliance, you must have the following:

- A user with the Manage Appliance authentication role configured on the appliance.
- The serial number of your appliance. To locate the serial number, go to Platform Management > Information. View the serial number under Chassis FRU Info. The serial number can also be found on the front panel LCD screen.
- A BlueTouch Online account. If you need a BlueTouch Online login, go to the BlueTouch Request Login screen (https://bto.bluecoat.com/requestlogin), and follow the registration process.

Download a Blue Coat License

1. Using your BlueTouch Online account information, log in to the Blue Coat Licensing Portal (https://services.bluecoat.com/eservice_enu/licensing/register.cgi).
2. From the menu on the left side, select "SSL Visibility," then select "License Download."
3. When prompted, enter the serial number of your appliance, then press Submit.
4. When the license has been generated, press "Download License File" for the required SSL Visibility Appliance.

Install a Blue Coat License

1. Select Platform Management > License.
2. Click the Add (plus sign) tool. The Install License window displays.

3. On the Upload File tab, use the Browse button to browse to the file location.

   or

   On the Paste Text tab, paste in the previously copied license text.

4. Click Add. You will see a confirmation message. All standard SSL Visibility Appliance features are now operational.

- After a 3.6.x to 3.7.0 upgrade, or after restoring a 3.6.3 PKI store backup, the list of external CA certificates will not include the CA certificates added in the 3.7.0 release. Without the new list of external CA certificates, the X.509 status for some sites (for example, www.google.com) will be "Invalid Issuer." The following PKCS#7 encoded file should be imported to update the external CA list: sslv_3.6.3_to_3.7.0_ca_ certificates.p7b.
- Be sure to backup the PKI store after importing the CA certificates. Note that the system log will have many warnings about duplicate entries; these log entries can be safely ignored.
- Google has recently introduced an undocumented proprietary TLS extension that is used when the Chrome browser connects to Google sites over TLS. The SSL Visibility Appliance is unable to inspect TLS sessions using the proprietary extension, but will detect the presence of the TLS extension and apply the action specified by the per-segment Undecryptable Actions, specifically the action for "Cipher Suite".
- Most applications making TLS connections have an embedded list of trusted CA certificates, and some of those applications do not expose a mechanism to modify the trusted CA certificate store, which makes it impossible to inspect TLS sessions originating from those clients. Examples of such clients applications are: Skype, Evernote, Dropbox. Attempting to decrypt those sessions will likely result in a fatal SSL alert in the SSL session log, such as "Alert[C]: certificate unknown" or "Alert[C]: bad certificate."
- The **(Monitor) > Errors** screen shows counts of error codes since the last policy activation, which means that the error code list is cleared as soon as any changes to the policy and/or PKI store is committed. The implication is that the value in the #Error column on the **(Monitor) > SSL Statistics** page does not correspond with the sum of the error counts shown on the **(Monitor) > Errors** screen.
- The **Host Categorization** feature utilizes a local database of categories downloaded from Blue Coat servers. There might be a discrepancy in the category according to the local database when compared to the result on http://sitereview.bluecoat.com. Over time the local database will be updated with the latest confirmed categories on Blue Coat servers.

Known Issues

Blue Coat is aware of these Known Issues in 3.7.0 .

New Features in 3.7.0

SSL Visibility Appliance software 3.7.0 introduces the following enhancements and new features.

- SSL Visibility Appliance requires a license to be fully operational as of 3.7. See the Important Information section for details.
- Host categorization support enables category-based policies; you can write rules which are triggered by category matches. This optional feature requires a subscription license; if an installed license expires, policy will run, but you will see a category value of 'Unlicensed.' See the Important Information section for more information on installing a license. The first matched category will be logged in the SSL session log details.
- Server Name Identification (SNI) and Subject Alternative Name (SAN) support is added to policies, reflected in the renaming of the **Distinguished Name** and **Common Name Lists** to **Subject/Domain Name** and **Domain Name Lists**. Existing policies will be automatically updated to use the new naming conventions. Both the SAN and SNI information are captured in the SSL session log details, and the SNI will be displayed with the prefix "SNI:" in case the domain name is not available (missing from X.509 information); typically, this will be for a re-used SSL session.
- X.509 Subject Alternative Name (SAN) information is now displayed for all items in the **PKI** store.
- The EULA and software attributions information can now be accessed from the UI login screen.
- The list of external X.509 CA certificates bundled with the appliance now includes the latest root CA certificates from major browsers. Refer to the Important Information section for more details.
- Basic jumbo frames support; jumbo frames now cut through, so you no longer need to redirect jumbo frame traffic to avoid corruption.
- A command line diagnostic interface, accessed via serial or SSH session, helps you troubleshoot issues. Customer Service may request you compile a diagnostics report or perform other actions. The diagnostics interface is very useful if you cannot access the WebUI.
- The **SSL Session Lo**g now displays fatal SSL alerts received from endpoints. The alerts are indications that the endpoint SSL stack had a failure, and is not necessarily indicative of a failure in the SSL Visibility Appliance. Refer to the Important Information section for more details.
- The **SSL Session Log** now only logs entries after the SSL handshake has completed, compared to previous versions that logged the entries as soon as the policy decision was made. The advantage is that errors in the SSL handshake are logged as one SSL session log entry, instead of as an update on an existing SSL session log entry.
- The ruleset activation logic was changed to prevent segment activation if any inconsistencies were found from parsing the ruleset. The advantage is that invalid rules are caught at activation time.
- Support added for AES-GCM and ChaCha20-Poly1305 cipher-suites, as well as TLS heartbeats.
- The "Decrypt (Key known)" action has been removed because of the confusion caused when comparing it to the "Decrypt (Certificate and Key known)" action.
- **SSL Session Log** data now optionally sent to remote syslog server. You may select to send one of these sets of messages to each enabled syslog server:
    - Appliance Logs
    - Appliance Warning/Error Logs
    - Session and Appliance Logs
    - Session and Appliance Warning/Error logs
    - **Note**: Make sure to select the correct **Session Log Mode** on the activated Segments as well.
- The number of remote syslog servers supported increased to eight in the **(Platform) > Remote Logging** menu.
- **System Log** entries are now rate-limited to a maximum of 60,000 messages in a 3 second period.
- **SSL Session Log** entries now log the matched rule index, and can be viewed in the SSL session log details. This enhances the mechanism to debug rulesets.
- The cut-through performance of small Ethernet frames has been improved.
- Incomplete or broken SSH sessions will time out after 45 seconds (STIG NET1645).

- The major subsystems in the appliance were upgraded to the latest firmware versions, and the base operating system was updated to a long-term-support version of Linux. The UI web server was also updated to prevent recent vulnerabilities.
- Customers have the option of specifying the management network IP address on the front panel (keypad and LCD). The default address is now 0.0.0.0.
- In versions prior to 3.7 a restriction was enforced to only accept a custom X.509 UI certificate if the common name (CN) in the certificate matched the hostname of the SSL Visibility Appliance. This restriction has been removed, allowing the customer to install a customer UI certificate before setting the hostname of the appliance.
- The TACACS+ privilege level to SSL Visibility Appliance security role mapping was changed to the following:
    - 0 = Auditor
    - 1 = Auditor + Manage Appliance
    - 2 = Auditor + Manage Policy
    - 3 = Auditor + Manage Appliance + Manage Policy
    - 4 = Auditor + Manage PKI
    - 5 = Auditor + Manage Appliance + Manage PKI
    - 6 = Auditor + Manage Policy + Manage PKI
    - 7 = Auditor + Manage Appliance + Manage Policy + Manage PKI
- More advanced POST integrity checks were added to increase the security of the appliance.
- Improved the mechanism used to determine the appliance hostname after a DHCP lease is acquired.
- Improved TCP retransmit handling for certain TLS1.1/TLS1.2 cipher-suites using RSA key exchange
- Various functions of the appliance can now utilize the SCP protocol (Linux:scp or Windows:pscp.exe). For example, packet captures and diagnostics archives can be downloaded directly from the appliance using SCP. The appliance can also be updated remotely by uploading a patch file to [user]@[appliance]:update (the appliance must still be rebooted from the UI or diagnostics interface for the update to be applied).

Fixes in 3.7.0

Release Information

- **Release Date:** 04/02/2014
- **Build Number:** 68

SSL Visibility Appliance software 3.7.0 contains the following fixes.

Resolved Issues

Description
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 Visibility 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.*.livefilestore.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 Visibility 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.

Reference Information

The following sections provide reference information for the SSL Visibility Appliance series.

SSL Visibility 3.9.x.x - 3.7.x Known Issues

Blue Coat is aware of the following issues in the SSL Visibility Appliance. Not all table fields are supplied for each issue. Issues resolved since their initial appearance are noted with the corresponding Fixed In version.

Issue #	Issue Workaround (if available)	Fixed In (when applicable)
SSLV-2542	SSH logins to an appliance that does not have TACACS configured result in authentication errors being added to the system log.	
SSLV-2531	The updated Google ChaCha20-Poly1305 cipher suites display as 0xcca8, 0xcca9, and 0xccaa in the SSL Session log. The names of the cipher suites are: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)	3.9.6.1
SSLV-2500	When switching views in the WebUI, pages may not display information immediately. **Workaround:** Refresh the browser window.	
SSLV-2471	When passing traffic from client to server with a Reject policy, a Client Hello may be seen in the output.	
SSLV-2454	When SSL Session logs are sent to a remote syslog server, IPv6 addresses in the source/destination fields are truncated.	3.9.6.1
SSLV-2202	On the SV800, "`ERROR: Type:2; Severity:80; Class:1; Subclass:1; Operation: 3`" may be seen on the console. It can be safely ignored.	
SSLV-2114	When reverting to an earlier version of the SSL Visibility software by performing a factory reset or applying an .nsu patch, you may get a "Firmware version not found" error when logging into the WebUI. **Workaround:** From the CLD, update the BIOS by entering the "bios update force" command.	
SSLV-2099	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 certificate in the persistent certificate cache, it no longer has the correct certificate chain, causing the session to be reported as Invalid Issuer.	3.9.4.1
SSLV-2036	An SSL Visibility SV-1800-F 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.	
SSLV-1967	When rebooting the SSL Visibility appliance, the message "`Interface subsystem returned errno: 88`" may be seen in the logs during the shutdown.	

SSLV-1922	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.	

Issue #	Issue Workaround (if available)	Fixed In (when applicable)

SSLV-1759	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.	

SSLV-1555	The CLD command "platform show ntp" truncates the address of IPv6 NTP servers.	
SSLV-1491	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.	
SSLV-1454	Power-off fail-to-wire (FTW) does not work on the SV1800-F fiber interface.	3.9.2.1
SSLV-1341	When a WebUI session times out, you may see a "Login Error - CSRF tokens required" error when attempting to log back in. **Workaround**: Restart the browser.	3.8.6
SSLV-1280	When configuring IPv6 DHCP, the appliance does not allow a default gateway to be set. **Workaround**: Use SLAAC to obtain the gateway address.	3.8.4
SSLV-1275	When an appliance is rebooted only once after applying several management network changes at the same time, the appliance may stop responding. **Workaround**: When making management network changes, click **Apply** and then reboot after each change, rather than applying all of the changes at once.	3.8.4
SSLV-1252	If when **USB** is selected as the **Master Key Storage Location**, a USB drive is not inserted into the appliance, the master key is stored locally without issuing a warning message. **Workaround**: Make sure to insert a USB drive before selecting **USB** as the **Master Key Storage Location**.	3.8.5
SSLV-1161	Recent SV1800-C/-F hardware may report a firmware version mismatch message on the LCD screen and in the System Log. You may safely ignore this message.	3.8.3
SSLV-1104	When performing a manual test, or if an HSM resigning failure occurs, the corresponding System Log message may appear in green text rather than red.	3.8.3
SSLV-975	After upgrading to SSLV-3.8.2, you may see the message `mount: special device /dev/dom2 does not exist` during the boot process. You can safely ignore these messages.	3.8.3
SSLV-966	Fixed an issue in which SSL Visibility SV2800 and SV3800 systems might fail to boot with software versions 3.7.x, 3.8.0, and 3.8.1.	3.8.2
SSLV-926	Multiple VLAN tags in QinQ Ethernet headers are now handled correctly.	3.8.2
SSLV-923	TCP flows no longer stall due to advertising a window larger than the previously seen receive window.	3.8.2
SSLV-919	When configuring SNMP v3, both the authentication and privacy passphrases are required, regardless of what security level is selected.	
SSLV-917	Fixed an issue in which SSL packet capture would not work on some ports.	3.8.2
SSLV-875	When the appliance Hostname is set to localhost.localdomain and DNS is configured, if the DNS server becomes unreachable, the appliance becomes unmanageable from the WebUI. **Workaround**: Configure a host name other than localhost.localdomain.	3.9.2.1
SSLV-823	Resolved a vulnerability to specially-crafted environment variables (CVE-2014-6271 and CVE-2014-7169) in the Red Hat Enterprise Linux Bourne Again shell (Bash). See Blue Coat Security Advisory SA82 for more information.	3.8.1

Issue #	Issue Workaround (if available)	Fixed In (when applicable)
SSLV-795	The Active-Inline attached appliance may not receive the SSL ServerHello message for cut-through SSL sessions using 4096-bit RSA keys.	3.8.2-409
SSLV-778	If log files take up more than 3 GB of disk space, the WebUI may fail to retrieve and display the System Log.	
SSLV-781	Loss of management network connectivity may occur when IPv6 address mode is configured for DHCP. The SV800 model is shipped with IPv6 management configured for DHCP. **Workaround**: To avoid this issue, as part of the initial configuration, SV800 users should set the IPv6 mode to a supported setting. To recover from this issue, configure a supported IPv6 setting from the CLD, and then reboot the appliance.	3.8.1
SSLV-773	Resolved the issue described in SSLV-276, 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.	3.8
SSLV-737	WebUI sessions may not always present an expiration indication.	
SSLV-717	Cut through, reject, and drop rules matching Anonymous Diffie-Hellman flows are bypassed.	3.8.3
SSLV-712	An appliance may experience intermittent disruption to new flows when a new Host Categorization database is loaded.	3.8.3
SSLV-701	Race condition may lead to failure when activating or editing PKI or policy configuration.	3.8
SSLV-692	When an SSL Visibility appliance recovers from an overload condition it may flag some SSL sessions with the “Invalid cryptographic response” error code	
SSLV-691	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 SV1800.	
SSLV-690	Internal CA certificates are not automatically checked for expiration. **Workaround**: Periodically check the certificates on the user interface.	
SSLV-689	A TCP FIN/FIN-ACK/ACK sequence is generated at the end of each decrypted SSL session. 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.	
SSLV-688	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.	
SSLV-687	Restoring a policy that contains active segments does not always activate the segments. **Workaround**: Manually activate the segments.	
SSLV-686	PKI objects (certificates or keys) can be removed even if they are referenced by the active policy.	
SSLV-680	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.	
SSLV-675	OCSP is not supported for server certificate validation. Only manually loaded CRLs can be used.	
SSLV-674	Importing a resigning CA 512-bit RSA key may not yield desired results.	3.8.3 3.9.4.1
SSLV-672	In Passive Inline mode, copy ports do no see Server Hello packets with a "cut-through" rule.	3.7.4

Issue #	Issue Workaround (if available)	Fixed In (when applicable)
SSLV-662	Flows through an appliance which use an imported resigning CA with a 512-bit RSA key may yield inconsistent results. Though the SSL Visibility Appliance allows the import of a 512-bit RSA key, it is not recommended.	3.9.4.1
SSLV-630	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.	
SSLV-614	Resolved a case where a segment did not recover on software failure.	3.8
SSLV-606	The WebUI doesn't distinguish between SV1800 Copper and Fiber.	3.8
SSLV-526	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.	
SSLV-523	The SSL Visibility Appliance is unable to inspect traffic to some Google sites from Chrome on Windows, due to a proprietary TLS extension. Sessions that meet these characteristics are cut through by the SSL Visibility Appliance. The Session Log Status will show: Unsupported TLS extension.	3.8.2-406
SSLV-485	The management port on an SV800 may be set to 10 Mbps following a power restoration if you use the power button prior to the green status LED illuminating. **Workaround**: To avoid this issue, let the SV800 boot without using the power button, or use the power button only after the green status LED is lit.	3.8.3
SSLV-434	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.	
SSLV-404	Maximum throughput performance of UDP traffic is affected when a small number of UDP flows is used.	
SSLV-401	First-time boot may take up to 5 additional minutes if no network cable is plugged into the management network port.	3.8
SSLV-396	The SSL session log may show sessions with harmless "Alert[C]: unknown (0)” error messages.	
SSLV-378	The vSphere VNC client sends an unencrypted ClientHello message, resulting in “Corrupt Record” session errors.	
SSLV-368	The web interface panel that notifies users to reboot the appliance after a configuration change disappears after the user has logged out.	
SSLV-364	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.	
SSLV-336	Installing a valid SSL Visibility license may cause a brief loss of connectivity while unfailing the port configured on active segments. This is only an issue on a SV1800.	
SSLV-335	All platform configuration changes require rebooting the SSL Visibility appliance in order to take effect.	3.8
SSLV-303	SSL error counts and invalid certificate information is cleared when the appliance policy is reactivated.	
SSLV-270	Deactivating an Active Inline segment may cause some packets to be received and retransmitted on the device ports in an endless loop. **Workaround**: Pull out and re-insert the cable on the deactivated segment.	
SSLV-259	Disabling a Remote Logging entry causes the options configured in the entry to be lost.	
SSLV-237	Timestamps in remote system log entries have one-second resolution and do not include fractions of seconds.	
SSLV-236	SNMP traps for link loss may not be generated if the link is recovered within 30 seconds.	

Issue #	Issue Workaround (if available)	Fixed In (when applicable)
SSLV-186	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.	
SSLV-185	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.	3.8
SSLV-182	The management features available on the web interfaces do not support IPv6 addresses.	3.8
SSLV-154	The default list of external certificate authorities includes CA certificates signed using the deprecated MD5 hash algorithm.	
SSLV-136	SSL sessions to the Blue Coat ThreatPulse service may occasionally be rejected due to cryptographic operation errors.	
SSLV-100	Patch upgrades do not update the default external CA list. New external CAs can be installed using the provided PKCS#7 file.	
SSLV-93	The SSLV appliance does not correctly match policy rules to SSL flows that contain non-ASCII characters in the "Subject" and "Issuer" server certificate fields.	
SSLV-74	DER-encoded PKCS#8 keys cannot be imported into the PKI store.	
SSLV-70	The SSL Visibility 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.	
SSLV-63	The following characters are not allowed in alert e-mail addresses: !, #, $, %, &, ‘, *, +, /, =, ?, ^, `, {, }, |, ~	3.8
SSLV-60	The command line diagnostic interface cannot be used during the bootstrap phase to set IP configuration on the management network interface. The front panel LCD can be used instead.	3.7.4
SSLV-54, SSLV-175	Manually failed segments are automatically unfailed when the SSL Visibility appliance is rebooted.	
SSLV-40	A half-duplex connection is negotiated if the SSL Visibility 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.	
SSLV-29	The SSL Visibility Appliance SV2800 and SV3800 models will try booting off of a USB stick if inserted into the front USB port	
SSLV-28	TCP connections with a small receive window may fail when a large amount of data is added to the flow.	
SSLV-22	The “Replace Certificate and Key” rule action is not supported for SSL flows using ECDSA authentication.	
SSLV-19	The SSL Visibility appliance may sporadically not send ClientHello messages of cut-through flows to the attached appliance.	
SSLV-15	DER-formatted keys and certificates cannot be used as web UI certificate/keys.	

Blue Coat Technical Support Resource

Blue Coat provides various methods of Technical Support, from self-help resources to call-in support centers.

To obtain additional information or to provide feedback, email customercare@bluecoat.com, or contact the nearest Blue Coat Systems technical support representative.

Visit https://bto.bluecoat.com/ to download the latest documentation and software, access the knowledge base, or log a support ticket.

Blue Coat Support Main Page

- http://www.bluecoat.com/support/contact.html

Self-help resource

- https://bto.bluecoat.com/support/blue-coat-deployment-assistance

Frequently Asked Questions (FAQ) and Knowledge Base

- https://bto.bluecoat.com/knowledgebase

Blue Coat Technical Publications documentation feedback (provide document title and chapter-/section)

- documentation.inbox@bluecoat.com

Third Party Copyright Notices

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

www.symantec.com