SGOS Upgrade/ Downgrade Guide

Guide Revision: 3/14/2018

Symantec

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

3/14/2018

Contents

About this Document

This document is intended to assist you with any upgrade or downgrade of SGOS, as long as you follow a supported upgrade/downgrade path. For information specific to SGOS versions, refer to the appropriate Release Notes.

See the following for more information about this document:

- "Documentation Conventions" on the facing page
- "Terminology" on page 8

Download Files from MySymantec

To download release notes, the SGOS image, and other files:

1. Go to MySymantec:

   https://support.symantec.com

2. Select **Downloads > Network Protection (Blue Coat) Downloads**.
3. When prompted, log in with your MySymantec credentials.
4. Select your product.
5. Select your appliance model (if applicable).
6. Select a software version.
7. Accept the License Agreement.
8. Select the file(s) to download and click **Download Selected Files**.

   The first time you download files, you are prompted to install the Download Manager. Follow the onscreen prompts to download and run the installer. For more information, refer to https://www.symantec.com/support-center/getting-started.

9. The Download Manager window opens. Select the download location.

   Complete instructions are also available online at https://www.symantec.com/support-center/getting-started. Bookmark this page for future reference.

Documentation Conventions

Blue Coat ProxySG documentation uses the following typographical conventions:

Convention	Description
bold sans serif type	Field, option, and page labels in the Management Console or on a website such as MySymantec.
italicized type	Document titles, variables, and the first instance of special terms. Some of these terms are described in "Terminology" on the next page.
`monospaced` type	Used for CPL and CLI examples.
`monospaced bold` type	CLI commands that must you enter exactly as written.
Square brackets, as in [*value*]	Optional command parameters.
Curly braces, as in {*value*}	Required command parameters.
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified.

Terminology

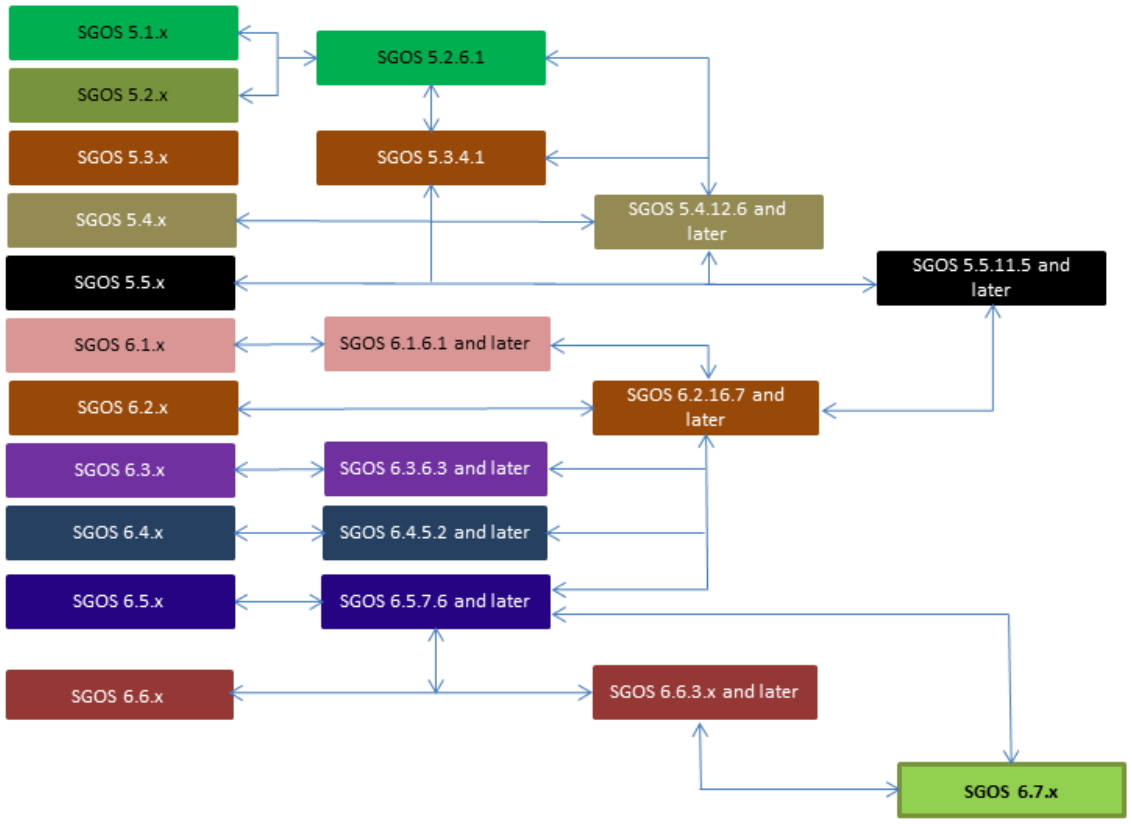
This document uses abbreviations instead of expanded forms. Refer to the following table to determine the meaning or expanded form of a term.

Abbreviation	Expanded Term	Description
ADN	application delivery network	Defines the framework that enables application acceleration between corporate offices in a WAN.
BCAAA	Blue Coat Authentication and Authorization Agent	Software installed on a domain server, acting as an intermediary between the Blue Coat ProxySG appliance and the domain.
-	Symantec point of contact	Your Symantec Sales Engineer (SE) or reseller.
CA	certification authority	Organization that issues digital certificates.
CIFS	Common Internet File System	Protocol based on the Server Message Block (SMB) protocol used for file sharing, printers, serial ports, and other communications. The Blue Coat ProxySG appliance supports CIFS proxy.
CLI	Command Line Interface	Command line tool you use to execute administrative and configuration commands.
CPL	Content Policy Language	Language in which Blue Coat ProxySG appliance policy is written. You can customize policies to an organization's specific set of users and unique enforcement needs.
CRL	Certificate Revocation List	List of certificates that have been revoked and should not be trusted.
FIPS	Federal Information Processing Standards	Standards developed by the United States federal government for use in computer systems. The Blue Coat ProxySG appliance supports FIPS mode.
HTB	hash table block	Object store format that the Blue Coat ProxySG appliance uses.
-	interim release	An SGOS version to which you must upgrade or downgrade before you can install the *target release*. Some upgrade/downgrade paths might require more than one interim release.
JAR	Java archive	Archive files that aggregate Java classes. JAR files have a .jar extension.
OCS	origin content server	The source of the internet content that the client is requesting. A web server is an example of an OCS.
OCSP	Online Certificate Status Protocol	Protocol that provides a secure means of checking certificate revocation status in real time.

Abbreviation	Expanded Term	Description
RTMP/RTMPE	real time messaging protocol (encrypted)	Protocols used for streaming audio, video, and data.
-	SGOS	The Blue Coat ProxySG appliance operating system.
SWG	secure web gateway	Describes Symantec network security solutions.
-	target release	The SGOS version to which you want to upgrade or downgrade. See *interim release*.
VPM	Visual Policy Manager	A graphical policy editor that you can access in the Blue Coat ProxySG appliance Management Console. In the VPM, you can define policies without having to manually edit policy files.

Determine the Upgrade/Downgrade Path

Refer to the following diagram of supported SGOS upgrade/downgrade paths.



When downgrading to SGOS 6.5.6.1 from a 6.6.2.x version later than 6.6.2.3, add an intermediate downgrade step, as follows:
6.6.2.x > 6.6.2.3 > 6.5.6.1
Downgrading to 6.6.2.3 before downgrading to 6.5.6.1 will prevent a known issue from occurring. For details, refer to ALERT2300:
http://www.symantec.com/docs/ALERT2300

How to read the diagram

Locate your current SGOS release in the diagram. Then, locate the target release.

- If there are no interim releases between your current and target releases, you can upgrade/downgrade directly to the target release.
- If there is one or more interim release between your current and target releases, you must upgrade/downgrade to each interim release before you reach the target release.

After determining your upgrade/downgrade path, ensure that:

- The target release supports your hardware.
- You read the relevant Release Notes to learn about known issues, fixed issues, limitations, and more about the target release.

Upgrade path in FIPS mode

If you use FIPS mode on the ProxySG appliance, the upgrade/downgrade path is different from the one outlined in the diagram.

To upgrade appliances in FIPS mode, use the following path:

- 5.3.1.9 > 5.5.10.1 > 6.1.6.1 > 6.5.x

To downgrade appliances in FIPS mode, use the following path:

- 6.5.x > 6.1.6.1 > 5.5.10.1
- 6.5.x > 6.1.6.1 > 5.5.10.1 > 5.3.1.0

For more information on FIPS and Common Criteria certifications, refer to *ProxySG FIPS Mode WebGuide*:

http://www.symantec.com/docs/DOC9778

Upgrade path in an ADN

If you use transparent tunnels in an ADN and are upgrading to SGOS 6.x from a version older than 5.5.1.1, the target release must be one of the following:

- 6.1.6.1 or later
- 6.2.10.1 or later
- 6.3.4.1 or later
- 6.4.1.1 or later

Prepare for Your Upgrade or Downgrade

Symantec recommends that you perform the following steps to prepare for your SGOS upgrade or downgrade.

Verify Basic Requirements

You must meet these basic requirements before starting the upgrade/downgrade.

1. Obtain or verify access to a serial or SSH console.
   Why: You require CLI access to complete some upgrade/downgrade steps.
   How: Log in to the CLI using a serial or SSH console.
2. Obtain or verify your MySymantec credentials.
   Why: You must have MySymantec credentials to download the SGOS image, release notes, and any other relevant files (such as the BCAAA setup file and MIBs).
   How: Log in to MySymantec and verify that you can browse to the target SGOS release.
   If you cannot log in, search MySymantec for an appropriate solution. If maintenance on your Blue Coat ProxySG appliance has expired, contact your Symantec point of contact to purchase maintenance.
3. Verify browser and Java compatibility. To determine supported Java, operating system, and browser versions, refer to TECH245893.

Learn About the Target SGOS Release

Learn about the SGOS release to which you want to upgrade or downgrade, including any issues or behaviors that you might have to address during the upgrade/downgrade process.

1. Review the *Release Notes* for the target SGOS release.
   Why: Before upgrading/downgrading, you should verify that the target version supports your hardware and be aware of any limitations and issues in the target version.
   How: Download the release notes:
2. Review Symantec's end-of-life documents.
   Why: Before downgrading, you should know if your target release or hardware is nearing end-of-life or end-of-support.
   How: Refer to the end-of-life policies and documents at https://www.bluecoat.com/support/support-policies/eol-docs.
3. Review any changes in behavior that could affect your target SGOS release.
   Why: Be aware of any issues that could arise due to changes in behavior, and plan how to work around the changes.
   How: See "SGOS Changes in Behavior" on page 15.
4. Review deprecated policy.
   Why: It is important to migrate all deprecated constructs before performing a major version upgrade. If you fail to do so and the construct has been abandoned in the target release, use of the abandoned syntax can cause CPL compiler errors. As a result, policy fails to install, and the appliance uses the default policy of ALLOW or DENY for all traffic.
   How: See "Deprecated Policy Constructs" on page 53. During the upgrade process, you will resolve any CPL deprecation errors that occur.

If you have questions or comments about Symantec documentation, send an e-mail to documentation_inbox@symantec.com.

Prepare Your Environment

Depending on your deployment configuration, you might have to perform additional steps to prepare for the upgrade/-downgrade.

1. (If you use Director to manage your appliances) Decide whether to use Director for some upgrade/downgrade steps.
   Why: You can use Director to perform some upgrade/downgrade steps, such as clearing the byte cache and rebooting the Blue Coat ProxySG appliance.
   How: For information about using Director to manage configurations, refer to the *Director Configuration and Management Guide*.
   Advanced users can write scripts to automate the steps that Director cannot perform; contact your SE for more information.
2. (If you configured authentication on the appliance) Set up a backup BCAAA server. Alternatively, schedule authentication downtime.
   Why: Prevent authentication interruption during the BCAAA upgrade.
   How: Refer to the *BCAAA Service Requirements* document at MySymantec:
   For BCAAA 6.1: http://www.symantec.com/docs/DOC10043
3. (If you have appliances in a managed ADN) Plan the order in which to upgrade the appliances in the managed ADN.
   Why: Make sure that ADN managers recognize the versions of software that all ADN peers are running.
   How: Upgrade the appliances configured as the Primary and Backup Managers, before upgrading the other ADN nodes.
   If the ADN uses transparent tunnels, Symantec recommends that you upgrade nodes in the following order: managers, branches, concentrators.
   For more information, see "Enable Fast Transparent Tunnels" on page 86.

Schedule Time for the Upgrade/Downgrade

Symantec recommends that you perform the upgrade/downgrade during off-peak hours to avoid interrupting day-to-day functions.

SGOS Changes in Behavior

This section describes important changes to SGOS 5.x (starting with 5.4.x) and 6.x releases that affect the behavior of the appliance. These changes include changes in default settings, deprecations, and new, changed, and removed functionality.

It is good practice to review the changes applicable to your target release before performing an upgrade or downgrade.

SGOS does not recognize policy gestures from later versions of SGOS. If you downgrade SGOS, policy will not compile if it contains gestures implemented in a later version. Before you downgrade SGOS, refer to this section and the *SGOS Release Notes* for your target release to identify any policy gestures you must remove to maintain policy integrity.

Review the behavior changes in your target release:

Behavior Changes Applicable to SGOS 5.4.x Upgrade

The behavior changes below are listed under the SGOS 5.4.x version in which they were introduced. After a change is introduced, it is included in all subsequent 5.4.x releases.

Behavior Changes in SGOS 5.4.1.1

CIFS

- MacOS 10.5.6 clients and later cannot connect to CIFS Shares on EMC servers.

CLI Console

- The archive configuration file `archconf_post_setup.txt` contains configuration for content filtering with MACH5 Edition license. Because the MACH5 Edition license does not include the content filtering features, restoring a configuration using `archconf_post_setup.txt` can fail.

Health Check

- Health checks display on the **Statistics** tab of the Management Console with the MACH5 Edition license, but you cannot edit them.

IM

- Non-ASCII character replacement policy does not work with Yahoo! Instant Messenger.
- The im.reflect policy does not work for MSN Messenger.

Policy

- Reflect Client IP policy for CIFS cannot be implemented in the `<Forward>` layer. You must define `Client.protocol=cifs reflect_ip(client)` in the `<Proxy>` layer.

SSL

- Access log fields `x-cs-ocsp-error` and `x-rs-ocsp-error` are not part of the SSL format by default when upgrading from SGOS 4.x or 5.2 to 5.4. You must add these two fields manually.

TCP/IP and General Networking

- Internet traffic might not work if you use the Trust-Destination MAC feature.

Behavior Changes in SGOS 5.4.1.3

IM

- The SOCKS Forwarding policy combined with `im.transport (HTTP)` property is not supported if you use Yahoo! Instant Messenger.

WCCP

- When upgrading to SGOS 5.4, the WCCP configuration fails if the `forwarding-type` information is not defined. To prevent a packet return mismatch error during WCCP negotiation, you must explicitly define `forwarding-type` in the WCCP configuration.

  For example, the configuration should read:

```
wccp enable
wccp version 2
service-group 9
forwarding-type GRE
assignment-type hash
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 80 443 0 0 0 0 0 0
interface 0
home-router 172.16.11.1
```

Behavior Changes in SGOS 5.4.1.12

Content Filtering

- After upgrading to SGOS 5.x from 4.x, ADP connection limit counts connections in all TCP states.
  - In SGOS 4.x, only established connections are counted.
  - In SGOS 5.x, connections in all TCP states are counted.

    Clients that did not reach the ADP connection limit now reach the limit after upgrading; thus, before upgrading, plan for an appropriate ADP connection limit.

SSL Proxy

- The SSL Proxy now supports the TLS SessionTicket extension within the SSL Proxy, allowing for a secure Firefox/Gmail connection.

Behavior Changes in SGOS 5.4.3.3

CLI Console

- The CLI does not accept `max-cache-size` values larger than 2047 MB.

Behavior Changes in SGOS 5.4.3.7

Caching

- The `max-cache-size` value that can be entered in the CLI and Management Console has been increased to 8.25 GB.

  The Blue Coat ProxySG appliance does not cache objects greater than 4 GB when a patience page is configured and the `max-cache-size` is greater than 4 GB; however, caching occurs when trickling is enabled.

  If you downgrade from this version to an earlier version of SGOS, the system resets the `max-cache-size` value to the default value of 1024 MB. This option can be configured in **Do not cache objects larger than [ ] megabytes** in the **Configuration > Proxy Settings > HTTP Proxy > Policies** tab in the Management Console.

HTTP Proxy

- The MACH5 Edition license now supports HTTP Compression.

TCP/IP and General Networking

- The `restore-sg4-config` command does not restore the static-route-table in an SGOS 4.x configuration.

Behavior Changes in SGOS 5.4.6.1

SNMP

- The SNMP MIB has been extended to support multiple CPU cores.

Behavior Changes in SGOS 5.4.7.1

FTP Proxy

- Support has been added for the MLSD and MLST FEAT commands for browsing an FTP server.

Behavior Changes in SGOS 5.4.12.1

HTTP Proxy

- The Blue Coat ProxySG appliance no longer treats URLs starting with encoded forward slashes as relative URLs when transforming HTML pages. This caused server errors (code 500) to be sent back when transforming HTML pages.

Policy

- The `FORCE_DENY` rule does not take effect (the connection is still allowed) after an upgrade from SGOS 4.3.2.3 to SGOS 5.4.7.1, 5.4.9.1, or 5.4.10.1.

SNMP

- SNMP device IDs have been added in the MIB file for ProxySG 300/900/9000 and ProxyAV 1200/1400 product lines.

TCP/IP and General Networking

- The value of `tcp-keepalive-timeout` is now included in the configuration archive; previously, it was a hidden command.

Behavior Changes Applicable to SGOS 5.5.x Upgrade

The behavior changes below are listed under the SGOS 5.5.x version in which they were introduced. After a change is introduced, it is included in all subsequent 5.5.x releases.

Deprecations in 5.5.x

CPL Deprecation

- The `$(session.username)` has been deprecated and will be removed in a future release. This substitution will continue to refer to contents of the RADIUS `calling-station-id` attribute. Symantec recommends updating the policy to use the new format:
  `session-monitor.attribute.calling-station-id`

Command Deprecation

- The `#(config adn tunnel)` **`proxy-processing http {enable | disable}`** command has been deprecated.

Behavior Changes in SGOS 5.5.1.1

ADN

- The secure outbound setting **Secure only ADN routing connections** has been removed. After upgrading, the secure outbound setting of routing defaults to secure all management and tunnel connections made by secure proxies.

Content Filtering

- After upgrading to SGOS 5.5.x, you cannot configure third-party content filtering vendors, such as Intersafe, I-Filter, Surfcontrol, and Webwasher, using the Management Console.

Event Logging

- After upgrading to SGOS 5.5.x, the currently selected log host becomes the first entry in the Syslog log hosts list.

Networking

- SGOS 5.5.x does not support CIFS pre-population URLs that resolve to a distributed file system (DFS) redirected share.

Proxy Services

- In SGOS 5.5.x, the **Configuration > Services > Proxy Services** tab in the Management Console preserves the legacy service groups because policy based on previous SGOS versions might have references to the groups. In effect, for SGOS 5.4.x to 5.5.x upgrades:
  - The Standard group remains the same, with the same set of services.
  - All the other service groups display in Custom Service Groups.
  - The Bypass Recommended group and Tunnel Recommended group are empty.

In SGOS 5.5.x, if you restore the appliance to factory defaults, all legacy services are removed and the Management Console displays the SGOS 5.5.x default services and groups. You must reconfigure services, if necessary.

Threat Protection

- Malware scanning is disabled by default on the Blue Coat ProxySG appliance; however, the appliance attempts to create a ProxyAV service group for response modification of ICAP requests. If a service or service group titled **proxyav** exists, the Management Console displays an error when you attempt to enable malware scanning. To enable malware scanning, you must delete the **proxyav** service group.

Behavior Changes in SGOS 5.5.2.1

Session Monitoring

- SGOS 5.5.2.x introduces several updates for session monitoring.
  You can upgrade Blue Coat ProxySG appliances to SGOS 5.5.2.x without any loss of functionality; however, the Event Log displays deprecation warnings when using the `$(session.username)` expression.

CIFS

- After upgrading to SGOS 5.5.x, the CIFS service sometimes has only one of its ports (445) set to Intercept; the other port (139) is set to Bypass. If this occurs, edit the service to intercept port 139.

Behavior Changes in SGOS 5.5.3.1

ADN

- Transparent tunnels fail to establish when the concentrator's tunnel protocol version is greater than 5.5.3.1. Upgrading the branch to 5.5.4.1 or later fixes this issue.

Behavior Changes in SGOS 5.5.4.1

ADN

- When establishing connections through ADN, the ProxySG appliance now always replies to the client's MAC address (and not the router's) on all intercepted (inbound) connections.

CLI

- The `load forwarding` CLI command is now available on MACH5 Edition.

Miscellaneous

- The `restore-default keep-console` command now keeps console services that have been modified and restores the other proxy services to their defaults.

SNMP

- The Blue Coat ProxySG private MIB file (BLUECOAT-SG-DISK-MIB) now includes an SNMP trap for disk read/write errors (io_error). To download the modified MIB file, see "Download Files from MySymantec" on page 6.

TCP/IP and General Networking

- To eliminate the "too many home routers" error when a configuration has multiple WCCP groups with multiple home routers, the WCCP global router affinity has been increased from 32 to 256.
- When an interface goes down, the appliance now drops ARP packets instead of queuing them, preventing a continuous stream of ARP packets to the default gateway when the interface comes back up.

Behavior Changes in SGOS 5.5.5.1

Authentication

- Changes have been made to the BCAAA installer to disable the sync port by default (changed value EnableSyncServer=0 in sso.ini). This modification does not change pre-existing settings.

SNMP

- Missing MIB definitions for ProxySG 300/9000, and ProxyAV 1200/1400 models have been added.

Behavior Changes in SGOS 5.5.10.1

Cache Engine

- A restart in Cache Administrator in ce_admin.dll due to a watchdog timer alarm has been fixed. This fix sets the maximum cacheable object size for the SG300 to 10 GB.

Behavior Changes Applicable to SGOS 6.1.x Upgrade

The behavior changes below are listed under the SGOS 6.1.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.1.x releases.

Upgrading from pre-SGOS 5.4.x releases

The following feature change impacts upgrades from pre-5.4.x releases.

Access Logging

- This change impacts LDAPv2 users. In SGOS 5.4.3.3 and later, the `cs-username` field of the access log reports firstname%20lastname, instead of firstname.lastname as in previous releases.
  To revert to the prior behavior (firstname.lastname), type the following CLI command:
  `#(config) security legacy-relative-usernames enable`

Upgrading from SGOS 5.5.x

The following feature changes impact upgrades from SGOS 5.5.x.

Malware Scanning (ICAP)

- Default settings for new ICAP service:
  - Data Trickle Start—disabled for both interactive and non-interactive
  - Deferred scan on
- Threat Protection speed setting:
  - Data Trickle End—enabled for both interactive and non-interactive
  - Deferred scan on
- Threat Protection security setting:
  - Data Trickle—none for both interactive and non-interactive
  - Deferred scan on

Behavior Changes in SGOS 6.1.2.1

Networking

- When RTS outbound is enabled, the refcnt field for static route increases by 1 for every connection using that route.

SOCKS Proxy

- SOCKS services are unavailable on MACH5 Edition appliances.

Command Deprecation in SGOS 6.1.2.1

- The Proxy Processing feature was deprecated starting in SGOS 5.5.x. In SGOS 6.1.2.1, the Proxy Processing tab was removed from the Management Console, but you can still configure the feature in the CLI. Because the feature will be completely removed in the future,Symantec recommends that you discontinue using this feature and deploy a separate secure web gateway to handle proxy processing.

- The following CLI command is deprecated:

  ```
  # (config adn tunnel)proxy-processing http {enable | disable}
  ```

Behavior Changes in SGOS 6.1.4.1

SNMP

- SNMP MIBS have been added for device IDs for the ProxySG 300/9000 and ProxyAV 1200/1400 models.

Behavior Changes in SGOS 6.1.5.1

CLI Consoles

- SSH host and client keys are not retained when upgrading from SGOS 5.5.3.1 or 5.5.4.1 to SGOS 6.1.3.1, which causes Blue Coat ProxySG appliances to become disconnected from Director. The only way to reconnect the appliance is to add it to Director again.

Behavior Changes in SGOS 6.1.5.4

CIFS Proxy

- Previously, when remote storage optimization was disabled, the Blue Coat ProxySG appliance didn't mark files as being offline; this sometimes increased the number of requests that the client issued for particular files or directories. The behavior of the CIFS proxy has been changed so that it does not attempt to prefetch directories when the Directory cache time is set to 0.

Behavior Changes Applicable to SGOS 6.2.x Upgrade

The behavior changes below are listed under the SGOS 6.2.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.2.x releases.

Command Deprecations in SGOS 6.2.x

The following CLI commands are deprecated in SGOS 6.2.x.

Adaptive Refresh

- The following caching configuration CLI commands are deprecated starting in SGOS 6.2.6.1:

  ```
  #(config caching) refresh automatic
  ```

  ```
  #(config caching) refresh bandwidth kbps
  ```

  ```
  #(config caching) refresh no automatic
  ```

  The deprecated commands are replaced starting in SGOS 6.2.6.1 by the following commands, also in caching configuration mode:

  ```
  #(config caching) refresh bandwidth {automatic | kbps }
  ```

  ```
  #(config caching) no refresh
  ```

  Refresh bandwidth is now disabled by default.

Behavior Changes in SGOS 6.2.x

This section describes behavior changes that occur from features introduced in SGOS 6.2.x. The upgrade information is provided by component.

Access Logging

- SGOS 6.2 offers a new access log format for streaming and adds new fields to the existing `bcreporterstreaming_v1` format; this format is the default on new systems.

  The legacy streaming log format, `streaming`, is used on upgrades to SGOS 6.2. To use the `bcreporterstreaming_v1` format after upgrade, perform one of the following:
  - Edit the `streaming` log and change its format to `bcreporterstreaming_v1`.
  - Create a new streaming log that specifies the `bcreporterstreaming_v1` log format, and then edit the various streaming protocols to use this new log.

Adaptive Compression

- Starting in SGOS 5.5, adaptive compression was enabled by default on multi-processor platforms, but disabled on uniprocessor platforms. All Blue Coat ProxySG platforms that are manufactured or remanufactured with the SGOS 6.2 release have adaptive compression enabled by default.

After upgrading to SGOS 6.2, the adaptive compression setting matches the configuration before the upgrade. For example, if adaptive compression was disabled in SGOS 6.1, it is disabled after upgrading to SGOS 6.2.

Asynchronous Adaptive Refresh

- When upgrading from 5.x to 6.x, the default setting for adaptive refresh has been changed from automatic to disabled.

Bandwidth Optimization

- Pre-6.2.x versions had a single control for enabling byte caching and compression optimization for a particular service (called `adn-optimize` in the CLI and **Optimize Bandwidth** in the Management Console). SGOS 6.2 introduces separate controls for byte caching (`adn-byte-cache` or **Enable byte caching**) and compression (`adn-compress` or **Enable compression**).

  The following table indicates how the value of the `adn-optimize` setting before an upgrade from SGOS 5.4.x, 5.5.x, or 6.1.x affects the values of the `adn-byte-cache` and `adn-compress` settings after upgrading to SGOS 6.2.x.

adn-optimize (Before upgrade)	adn-byte-cache (After upgrade)	adn-compress (After upgrade)
Enabled	Enabled	Enabled
Disabled	Disabled	Disabled

The default value for HTTP handoff on the Flash proxy has changed from disabled to enabled. The following table indicates the value of the HTTP handoff setting after upgrading to SGOS 6.2.x from certain pre-SGOS 6.2.x versions.

SGOS version	HTTP handoff setting on pre-6.2 version	HTTP handoff setting after upgrading to 6.2
5.4.x/5.5.x	N/A (Flash not supported)	N/A
5.5 LA	Enabled	Enabled
5.5 LA	Disabled	Enabled
6.1.x	Enabled	Enabled
6.1.x	Enabled	Enabled
6.1.x	Disabled	Disabled

Disk Object Capacity

- All multi-disk systems that are manufactured with SGOS 6.2 have an increased object capacity; you can get this extra capacity on other multi-disk systems by initiating the `disk increase-object-limit` command after upgrading to 6.2. The disks are re-initialized in a format that is not compatible with SGOS releases prior to 6.2.

Encrypted MAPI Acceleration

- SGOS 6.2 is able to accelerate encrypted MAPI sessions. To accelerate encrypted MAPI, you must upgrade all ADN Peers – Concentrator and Branch appliances – to SGOS 6.2.x.

If a peer is running a pre-6.2 SGOS release, the connection is tunneled but is not accelerated.

Last Peer Detection

- Last Peer Detection is enabled by default for new installations, but not for upgrades.

  When a Blue Coat ProxySG appliance is upgraded to 6.2, the feature is disabled by default. To use the feature, you must enable Last Peer Detection on intermediate concentrators and, optionally, the last concentrator on the path to the OCS. You do not have to upgrade branch peers to 6.2 for the feature to operate, but they must be running SGOS 5.5 or higher.

Reflect Client IP for ProxyClient Peers

- SGOS 6.2 offers independent controls for configuring how the Concentrator peer handles client IP reflection requests from Blue Coat ProxySG peers versus ProxyClient peers.
- If Reflect Client IP (RCIP) on the Concentrator peer was set to deny before the upgrade to SGOS 6.2, RCIP for ProxyClient sets to use-local upon upgrade to 6.2; this is consistent with how RCIP for ProxyClient was previously handled.
- If RCIP on the Concentrator peer was set to allow, then the client IP is reflected for ProxyClient peers.

Behavior Changes in SGOS 6.2.1.1

ADN

- A branch peer running a release prior to SGOS 5.5.4.1 cannot form transparent tunnels with a Concentrator peer running SGOS 6.2.x or later. The branch peer must be running SGOS 5.5.4.x or later.

CIFS

- The `show cifs` CLI command does not work if the URL contains spaces, even if you enclose the URL in quotation marks.

SMTP Server Configuration

- A new top-level configuration mode, smtp, is available for configuring the SMTP server that the ProxySG uses for emailing notifications and sending heartbeats. In addition, the server port is now user-configurable; previously, it was hard-coded to port 25. The commands for SMTP server configuration are:

  ```
  #(config smtp) server domain_name | ip-address [port]
  #(config smtp) from from-address
  #(config smtp) no server
  #(config smtp) view
  ```

CPL Deprecations

- In the `ftp.server_data( )` property, the `port` and `pasv` arguments have been deprecated. If you install existing policy with these arguments, the system convertst them to `active` and `passive`.

Command Deprecations

- The following `event-log` CLI commands have been deprecated:

  ```
  #(config event-log) mail smtp-gateway {domain_name | ip_address}
  #(config event-log) mail from from_address
  ```

`#(config event-log)` **`mail no smtp-gateway`**

After upgrading, values defined in the `#(config event-log)` **`mail`** commands are mirrored in the `#(config smtp)` subcommands.

Behavior Changes in SGOS 6.2.4.1

Authentication

- Previously, domain controllers were not discovered if the Computer Browser service was disabled on Windows 2008 machines. The code in SGOS 6.2.4.1 has been changed so that domain controllers can be discovered regardless of the state of the Computer Browser service.

IPv6 Support for ADN

- Support for IPv6 now includes ADN. The Blue Coat ProxySG WAN optimization solution now works in an IPv4, IPv6, or combination IPv4/IPv6 ADN.
- When upgrading managed ADN deployments to a release that supports IPv6 on ADN (SGOS 6.2.4.1 or later), the Blue Coat ProxySG appliance that is functioning as the ADN manager must be upgraded before the managed nodes. The manager should continue to be assigned a reachable IPv4 address until all managed nodes have been upgraded. A managed node that has been upgraded to a release that supports IPv6 on ADN (SGOS 6.2.4.1 or later) can use either IPv4 or IPv6 to connect to the previously upgraded manager.
- In explicit deployments, an IPv6-only Concentrator peer will not be advertised as the Internet gateway for a node that is running an older (pre-6.2.4.x) version of software.
- Only IPv4 routes are advertised to managed nodes running pre-SGOS 6.2.4.1 versions.

Management Console

- Certain commands (server subnets, Internet gateways, VLANs) do not accept a slash in the IP Address field, so you cannot enter a subnet with CIDR notation (for example, 10.10.10.0/24). Because of this limitation, you will need to define a subnet by entering the IP address and subnet mask/prefix length in separate fields (IP address: 10.10.10.0, Subnet Mask: 255.255.255.0).

TCP/IP and General Networking

- The distribution algorithm used for WCCP mask assignment has been changed so that it distributes the remainder across the caches more evenly.

Behavior Changes in SGOS 6.2.5.1

Flash Proxy

- Adobe stream failed to load through RTMP proxy. Adobe Connect sends play requests (for non-audio/non-video streams) with the parameter `Reset=2` or `3`.
  Values 2 and 3 are now supported, which add the additional bit ignore timestamps. (Previously, only true and false values were supported.)

URL Filtering

- The local database filter now allows checks against top-level domains (TLDs). In previous versions of SGOS, the Blue Coat ProxySG appliance restricted top-level domain filters.

Behavior Changes in SGOS 6.2.6.1

ADN

- ADN is now able to retrieve device IDs when IPv6 addresses are used for ADN managers.

CIFS Proxy

- When Remote Storage Optimization is disabled, the CIFS proxy no longer generates a lot of SMB Trans2's Find_ First2 requests, which created high CPU utilization of Windows servers. As part of this fix, the behavior of the CIFS proxy was changed so that it would not attempt to prefetch directories when directory cache time is set to 0.

HTTP Proxy

- After upgrading to SGOS 6.2.6.1, the Blue Coat ProxySG appliance uses the `_RST` suffixes (which indicate a connection reset) for cache-misses in the access log.

Management Console

- You can now specify IPv6 addresses for VIPs (in the Management Console, select **Configuration > Network > Advanced > VIPs > New**).

Real Media

- Previously, the Blue Coat ProxySG appliance rejected any media player that did not identify itself via the `user-agent` header. As a result, streaming using FFmpeg player on Linux didn't work due to the lack of a user agent and the RTSP log displayed the message "No license for vendor 0".
  Currently, any player that does not transmit a `user-agent` header is enabled and communicates with the Blue Coat ProxySG appliance exactly as QuickTime player does.

SNMP

- Capitalization in the Blue Coat ProxySG appliance MIB files has been updated to be compliant with the RFC regarding capitalization. To download the latest MIB, see "Download Files from MySymantec" on page 6.

URL Filtering

- The SmartFilter look-up has been updated to allow for lookups of URLs with the .xxx domain.

Behavior Changes in SGOS 6.2.7.1

Authentication

- The Blue Coat ProxySG appliance now supports up to 200 IWA realms. The appliance continues to support up to 40 realms of all other types.

FTP Proxy

- If the IP address has already been authenticated through some other protocol, the FTP proxy will now serve further requests. Otherwise, it will reject all requests. This method ensures that the client knows that the FTP proxy does not require proxy credentials.

Behavior Changes in SGOS 6.2.8.1

CLI Console

- After upgrading from SGOS 5.5 to 6.2 MACH5 Edition, the Threat-Protection configuration is no longer generated in the configuration archive/SysInfo.

Behavior Changes in SGOS 6.2.9.1

CLI Console

- Previously, the console agent was unable to parse HTTP GET requests if the header was over 512 bytes; this happened when the URL in the GET request was over 512 bytes. The buffer for parsing the URL out of a request has been increased from 512 to 2048 bytes.

HTTP Proxy

- The Blue Coat ProxySG appliance now closes the client connection when the server connection cannot be persisted. Previously, when the server wasn't the one that closed the connection, the appliance didn't implement the client persistence policy. As a result, the client connection stayed open, causing the appliance to reuse the connection it just closed with the server.

Behavior Changes in SGOS 6.2.10.1

HTTP

- Objects are no longer served from the cache after Cache-Control: max-age= value expires.

> As part of this fix, the CLI option `http strict-expiration serve` is always enabled. If you disable the setting, the CLI responds `ok`, indicating the configuration is set; however, the setting is not disabled.

Policy

- Policy traces only show authentication information if it was requested for the current transaction. Previously, traces would share the authentication information from a prior transaction in the session if authentication was not requested for the current transaction.

ProxyClient

- ProxyClient download links now work with clients running Microsoft Security patch KB2585542.

Behavior Changes in SGOS 6.2.11.1

TCP/IP and General Networking

- The Blue Coat ProxySG appliance now treats URLs starting with encoded forward slashes as relative URLs when transforming HTML pages. This occurred after a SAP upgrade, where traffic to SAP servers from reverse_proxy was blocked.
- When the OCS sends a response with `set-cookie` and `Location` headers, the appliance includes a new cookie in the pipeline request.

Behavior Changes Applicable to SGOS 6.3.x Upgrade

The behavior changes below are listed under the SGOS 6.3.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.3.x releases.

Command Deprecations in SGOS 6.3.x

The following CLI commands are deprecated in SGOS 6.3.x.

IWA BCAAA Configuration

- The `security iwa` CLI commands and all associated subcommands are deprecated. They have been replaced by the `security iwa-bcaaa` command and subcommands starting in SGOS 6.3.x.

Web Application Controls

- The following command is being deprecated:

  `#(config content-filter bluecoat)` **`view operations <application_name>`**

  Starting in SGOS 6.3.x the deprecated command is replaced by the following:

  `#(config content-filter bluecoat)`**`view operations application <application_name>`**

Behavior Changes in 6.3.x

Websense and SmartFilter Support

- Support for the Websense and SmartFilter on-box content filtering databases has been removed in 6.3.x. If you had Websense or SmartFilter configured in a previous release, the third-party content filtering database setting changes from Websense/SmartFilter to None when you upgrade to SGOS 6.3.x. The associated Management Console configuration settings and CLI commands are no longer available; however, the configuration settings will be maintained and the feature will be restored upon downgrade.
- Support for Websense as an external service (off-box) has been deprecated. The add/edit Websense external services CLI has been deprecated. You can still add/edit Service Groups with Websense external services and view Websense external services. When you issue the following CLI command, the CLI displays a deprecation message:

  `#(config external-services)`**`create websense new_websense_service`**

  ```
  Warning: Websense off-box support has been deprecated and will be removed in a
  future release

  ok
  ```

  Adding policy to trigger Websense off-box categorization results in a policy deprecation warning:

  ```
  Deprecation warning: "request.filter_service"; Websense off-box support has been
  deprecated.
  ```

  In addition, you can no longer add/configure Websense external services or add Websense external

services to Service Groups through the Management Console. You can still view /edit existing Service Groups containing Websense external services from the Management Console.

Behavior Changes in SGOS 6.3.1.1

ADN

- A Branch peer running a release earlier than SGOS 5.5.4.x cannot form transparent tunnels with a Concentrator peer running SGOS 6.2.x or later. The branch peer must be running SGOS 5.5.4.x or later.

CLI Consoles

- SSH host and client keys are now retained when upgrading from SGOS 5.5.3.1 or 5.5.4.1 to SGOS 6.3.x, which prevents proxies from becoming disconnected from Director.

MIB Changes

- BLUECOAT-MIB
  - Added device IDs for the ProxySG 300 (device 32), ProxySG 900 (device 34), ProxySG 9000 (device 29), ProxyAV 1200 (av 7), and ProxyAV 1400 (av 5).
  - Changed ProxySG 600 device ID to device 31.
- BLUECOAT-SG-PROXY
  - Added the word Core to the table entries in sgProxyCpuCoreTableEntry to match the OID names.
  - Changed the syntax of the sgProxyCPUCoreTable object to be RFC compliant.

Behavior Changes in SGOS 6.3.2.2

- The list of User Agents available as a Web Access Layer source in the Visual Policy Manager includes new agents. For a list of new User Agents, refer to the SGOS 6.3.x *Release Notes*.

Authentication

- To join a Windows domain, the current implementation now requires delegation, which requires the Blue Coat ProxySG appliance to have administrator credentials

Behavior Changes in SGOS 6.3.3.1

New CA Certificates

- Seven new intermediate CA certificates have been added. For a list of new CAs, refer to the *SGOS 6.3.x Release Notes*.

Behavior Changes Applicable to SGOS 6.4.x Upgrade

The behavior changes below are listed under the SGOS 6.4.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.4.x releases.

Behavior Changes in SGOS 6.4.x

Authentication

- You can now specify a container in Active Directory for the Blue Coat ProxySG appliance's computer account, as in the following example:

```
#(config security windows-domains)join-container ?

<domain name alias> <DNS domain name> <container DN> <join account name> [<join
account password>]

#(config security windows-domains)join-container auth_saml auth-saml.local ou=-
=sg,dc=auth-saml,dc=local admin admin

ok
```

- After users who are already authenticated by IP surrogate go to a Web site through explicit proxy, the Blue Coat ProxySG appliance now invokes the surrogate for transparent requests. Previously, the appliance did not invoke the IP surrogate and sometimes denied transparent requests.

Policy

- The limit for the `location.id policy` condition has been expanded to the maximum value stored by an unsigned32 value (0..4294967295). Previously, policy failed to compile if the value of the location.id condition was greater than 9999.

Visual Policy Manager

- The list of User Agents in the VPM have been updated to include Internet Explorer, Firefox, and Chrome version options.

MIB Changes in 6.4.x

Failover MIB

- The new BLUECOAT-SG-FAILOVER-MIB has been added to monitor changes in the failover state of the Blue Coat ProxySG appliance. The message sent in the notification describes the state change. The bluecoatSgFailoverTrap is used to send the notification.

Behavior Changes in SGOS 6.4.1.1

Deprecations and Removals

- The ability to disable heartbeats has been removed from the Management Console in SGOS 6.4.1.1.
  You can now manage the customer experience program and monitoring settings (heartbeats) from the CLI only:

  ```
  #(config) diagnostics
  #(config diagnostics) heartbeat disable
  ```

  If you disable automatic heartbeats, you can still manually send a heartbeat message by entering the following commands:

  ```
  #(config) diagnostics
  #(config diagnostics) send-heartbeat
  ```

  When monitoring is enabled (by default), Symantec receives encrypted information over HTTPS whenever the appliance is rebooted. Like the heartbeat, the data sent does not contain any private information; it contains restart summaries and daily heartbeats. This allows the tracking of Blue Coat ProxySG appliance unexpected restarts because of system issues and allows Symantec to address system issues preemptively. To disable monitoring, enter the following commands:

  ```
  #(config) diagnostics
  #(config diagnostics) monitor disable
  ```

  If you have disabled heartbeats and/or monitoring, you can re-enable them by entering the following commands:

  ```
  #(config diagnostics) heartbeat enable
  #(config diagnostics) monitor enable
  ```

Event Logging

- In deployments with a high number of Syslog host servers configured, the Syslog no longer displays a high number of messages about dropped messages due to lack of resources (such as `2711860143 message(s) dropped by Syslog, due to lack of resources`). The Syslog on each server now displays a single notification message that indicates the number of dropped messages for the specific host. If no messages were dropped for the specific host, Syslog does not display the notification.

Flash Proxy

- You can now play Flash video on RTMP/RTMPE streams without having to set policy to bypass caching.

HTTP Proxy

- The appliance now respects the Per-Server clientless limit when running large content distribution jobs from Director. Previously, the appliance set server connections as persistent and did not close the sockets for finished requests, resulting in connections that exceeded the specified limit.

Policy

- Explicit connections to the Blue Coat ProxySG appliance using a port other than port 443 are now denied and the browser displays an exception page.

SSL Proxy

- The appliance can now correctly cache intermediate certificates that have different properties (such as issuers, public key, and authority key) but which share the same subject name. In addition:
- A previously cached certificate without a subjectIdentifierKey is replaced by a certificate that has the same subject field and has a subjectIdentifierKey.
- A previously cached certificate with a subjectIdentifierKey is not replaced by a certificate that has the same subject field but no subjectIdentifierKey.

  Intermediate CA certificates are cached before they are validated using OCSP revocation or the CRL, which causes revoked certificates in the intermediate-certificate cache.

Behavior Changes Applicable to SGOS 6.5.x Upgrade

The behavior changes below are listed under the SGOS 6.5.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.5.x releases.

Behavior Changes in SGOS 6.5.1.1

Access Logging

- Access log facilities now work as expected after restoring a configuration archive that contain them. Previously, you could not assign the facility.

Authentication

- Not all authentication realms are supported in the VPM Admin Access Layer. If an authentication realm that is not supported is referenced in a pre-6.5 release, the following compilation warning occurs.

  ```
  Warning: <Admin> layer authentication requires that the realm support BASIC or Connection credentials. BASIC credentials should be enabled or a new realm should be specified.
  ```

  In SGOS 6.5.x, these warnings now register as policy compilation errors. You must resolve this issue before upgrading to 6.5; otherwise, policy fails to compile upon upgrade, which (depending on your default policy configuration) results in an appliance that either allows all traffic or denies all traffic.

  Prior to SGOS 6.5, a certificate realm in the VPM Admin Access Layer generated a policy compilation warning but would still work correctly. In 6.5, certificate realms compile successfully without warnings or errors.

BCAAA

- BCAAA 6.1 has been released. Note the following changes in BCAAA:
- You cannot run multiple instances of BCAAA on the same machine.
- You must delete all previous BCAAA instances before installing BCAAA 6.1.

HTTP Proxy

- The default Normal acceleration profile has changed. `Never serve after expiration` is now enabled by default.
- HTTP 4xx (except for 401 and 407) and 5xx error codes are treated as failed requests by default. To specify which HTTP responses the ProxySG appliance should treat as failures, you could configure attack detection mode for the client or the server. Refer to the “Preventing Denial of Service Attacks” chapter in the *SGOS Administration Guide* for more information.

MIB

- The new BLUECOAT-SG-ICAP-MIB provides statistics and events related to the Blue Coat ProxySG appliance’s ICAP services.

SSL

- In SGOS 6.5.x, the HTTPS Management Console, HTTPS Reverse Proxy, SSL Device Profiles, and SSL Client Profile services have new default TLS settings. When you upgrade from 6.5.x, the value of the existing SSL protocol for each service is copied to the new registry node. When you downgrade, the previous registry node containing the SSL protocol becomes available, including the previous service values.

Deprecations and Removals

- BCAAA 6.1 no longer supports the COREid realm. In addition, a Solaris version of BCAAA is no longer provided.

Behavior Changes in SGOS 6.5.2.1

Caching

- The maximum object size that the ProxySG appliance can cache has been increased to 4 GB from 1 GB. This affects only new installations.

HTTP Proxy

- The ProxySG appliance now allows HTTP request lines that are over 6 KB in length, up to a maximum of 16 KB.

Policy

- The Effective Client IP object in the Visual Policy Manager has been enhanced to allow multiple substitutions. You can add multiple (pre-set or custom) substitutions and specify the order in which policy should evaluate them; the first valid substitution is used whenever `client.effective_address=` is specified.

Serviceability

- The maximum number of snapshots you can store has been increased to 1000 from 100.

SSL

- Emulated certificate keys will now match the size of the RSA key provided by the server, up to 2 KB. The default is no longer 1 KB. This allows for more secure keys and avoids issues caused by mismatched key sizes. If a DSA certificate is presented by the OCS, the emulated RSA certificate key size remains 1 KB.

Deprecations and Removals

- IM policy gestures have been deprecated. See "Deprecated Policy Constructs" on page 53 for the specific gestures.
- The following gestures are no longer available in the `<Cache>` layer:

  `http.request.apparent_data_type=`

  `http.request.apparent_data_type.allow`

  `http.request.apparent_data_type.deny`

  If these gestures were used in SGOS 6.5.1 in the `<Cache>` layer, policy will not compile.

Behavior Changes in SGOS 6.5.6.1

SSL

- The Blue Coat ProxySG appliance now supports HTTPS interception in forward proxy mode when sites use ECDHE ciphers. The following variants of ECDHE-RSA are available:
  - ECDHE-RSA-AES128-SHA (0xC013)
  - ECDHE-RSA-AES256-SHA (0xC014)
  - ECDHE-RSA-AES128-SHA256 (0xC027)
  - ECDHE-RSA-AES128-GCM-SHA256 (0xC02F)
  - ECDHE-RSA-RC4-SHA (0xC011)

  Users can now access websites that use these ECDHE ciphers.

Behavior Changes in SGOS 6.5.7.1

Authentication

- Upstream 407 challenges are now blocked by default. As a result, users no longer see any upstream 407 challenges; they receive exception pages instead. Depending on your deployment and your organization's requirements, upgrade to SGOS 6.5.7.1 for best security; however, after the upgrade, you might have to perform additional steps to maintain your network behavior.

  The change was made to address a security vulnerability with how the appliance handles 407 authentication challenges. The vulnerability affects only explicit proxy deployments where enterprise credentials are at risk of being forwarded to a malicious upstream origin content server (OCS) that sends a 407 authentication challenge. This issue applies to deployments with:

  - Explicit proxies with IWA/NTLM authentication
  - Appliances running SGOS 6.5.6.x and earlier

  Depending on your deployment and topology, you may have to configure the appliance to allow upstream 407 challenges. Command line interface (CLI) commands have been added to allow and deny 407 challenges. See details in the *Command Line Interface Reference*.

  Refer to ALERT2294 and SA93 for important information on this vulnerability, the behavior change, and instructions for configuring the ProxySG appliance (including if and when to use the new CLI) to maintain current functionality.

SSL

- The Blue Coat ProxySG appliance now includes the following additional ECDHE-ECDSA ciphers between the appliance and the OCS:
  - ECDHE-ECDSA-AES128-SHA256 (0xC023)
  - ECDHE-ECDSA-AES128-GCM-SHA256 (0xC02B)
  - ECDHE-ECDSA-RC4-SHA (0xC007)
  - ECDHE-ECDSA-AES128-SHA (0xC009)
  - ECDHE-ECDSA-AES256-SHA (0xC00A)

Behavior Changes in SGOS 6.5.7.6

Content Filtering

- In April 2015, Google discontinued YouTube Data API v2.0. As a result, Blue Coat categories for YouTube are no longer supported in earlier versions of SGOS 6.5.x. Starting in SGOS 6.5.7.6, you must specify a valid server key for the YouTube API v3 in order to use Blue Coat categories for YouTube. After an upgrade to SGOS 6.5.7.6, you must set the server key and enable YouTube as a provider. To obtain a key, log in to the Google Developers Console to create a project and then generate the key. Refer to TECH245050 for more information.

Behavior Changes in SGOS 6.5.8.1

SSL

- SGOS no longer restricts the size of external certificates imported via the CLI or Management Console. You can now import external certificates larger than 8000 bytes in size; however, if you downgrade to a previous version of SGOS, the certificates must be re-imported and are subject to the 8000-byte size limit. If you import external certificates in SGOS 6.5.8.1 or later releases, and then downgrade to an SGOS version earlier than 6.5.8.1, you must import the certificates again.

Behavior Changes in SGOS 6.5.9.10

Management Console

- The appliance keyring has been updated to a SHA-256 certificate with 2048-bit RSA encryption. If you have a mixed ADN deployment with peers running SGOS 5.5.x, Symantec recommends that you upgrade the peers to 6.2.x or later.

Policy

- Upon an upgrade to this release, ProxySG policy engine disables RDNS lookups by default. Policy gestures that trigger an RDNS lookup may be affected. This change was made to prevent potential misuse of RDNS by malicious third parties. A new CLI command was introduced to control whether an RDNS lookup is used or not:
  `#(config) policy restrict-rdns {all | none}`
  The command is set to `all` by default. If you allow RDNS lookups by changing the setting to `none`, downgrade SGOS, and then upgrade to this release again, RDNS lookups are still allowed (the `none` setting is preserved).

  Using the `restrict rdns` definition block in policy allows RDNS lookups, regardless of the CLI setting.

Behavior Changes in SGOS 6.5.9.14 (Patch Release)

HTTP Proxy

- This release introduces improved handling of HTTP headers that are not RFC-compliant. In SGOS 6.5.9.2, stricter validation rules for HTTP headers were introduced to protect client computers from attacks that rely on headers that are not RFC compliant; however, these stricter validation rules caused the Blue Coat ProxySG appliance to report that legitimate websites that were not RFC-compliant were returning invalid responses. As a result, those websites were blocked. In SGOS 6.5.9.14 and later, Symantec has made enhancements to how the Blue Coat ProxySG appliance validates HTTP headers, to allow users to access legitimate websites that are not RFC-compliant as well as protect client computers from attacks.

  In addition, two new access log fields with policy substitutions (`x-bluecoat-normalized-response-headers` and `x-bluecoat-invalid-response-headers`) have been added. In cases where SGOS still rejects a response, the `x-bluecoat-invalid-response-headers` field reports what made the response invalid. In cases where the Blue Coat ProxySG appliance automatically normalizes the headers and returns the corrected response to the client, the `x-bluecoat-normalized-response-headers` field reports what normalization changes the appliance made.

SSL Proxy

- By default, trust-destination-ip is now set to true for upstream SSL proxy connections in transparent deployments. As a result, when server name indication (SNI) is implemented, the appliance does not perform DNS resolution on the hostname in HTTP headers, and trusts the destination IP in the client hello message instead.

Behavior Changes Applicable to SGOS 6.6.x Upgrade

The behavior changes below are listed under the SGOS 6.6.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.6.x releases.

Behavior Changes in SGOS 6.6.2.1

Access Logging

- The `bcreportermain_v1` log format has changed. The following fields were added to support Web Application Firewall (WAF) in SGOS 6.6.2.1:
  - `x-bluecoat-application-name`
  - `x-bluecoat-waf-attack-family`
  - `x-bluecoat-waf-block-details`
  - `x-bluecoat-waf-monitor-details`

  See the following **Deprecations and Removals** section for details on fields that were removed.

- The `rs-service-latency` field was also added to `bcreportermain_v1`. This field reports the total time taken to connect to the origin content server and receive the first response byte from it. The `rs-service-time-taken` field has been removed from the log format.

Attack Detection

- IPv6 is now supported in Attack Detection, in addition to IPv4. No CLI changes are required; you can simply now specify IPv6 addresses. IPv6 entries are displayed for client/server commands and when viewing statistics.

Content Filtering

- If you were using Blue Coat categories for YouTube prior to upgrading to SGOS 6.5.7.6 or SGOS 6.6.2.1, after the upgrade YouTube is no longer enabled as a provider. The event log also displays a message indicating that you must set a server key to use YouTube for categorization. This behavior is by design; previously, SGOS used the YouTube API v2, but SGOS now uses the YouTube API v3 for categorization.

  To set the server key and enable YouTube in SGOS 6.6.2.1, refer to TECH245050.

- The Blue Coat WebFilter (BCWF) username and password are no longer saved when you archive the configuration (or Director or Management Center backs up the configuration) while the data source is set to Intelligence Services; however, the username and password still exist in the ProxySG configuration and the Management Console displays them in **Configuration > Content Filtering > Blue Coat** when you switch the data source back to Webfilter. To save the BCWF username and password, switch the data source back to **Webfilter** and save a separate configuration file.

Health Monitoring

- The **Subscription Communication Status** metric has been removed from **Maintenance > Health Monitoring > General**. In SGOS 6.6.x, configure thresholds and intervals for each subscription service (including services introduced in this release) individually on **Statistics > Health Monitoring > Licensing**. In addition, you must configure a global notification method for all subscription services on **Maintenance > Health Monitoring > Subscription**.

- The **Subscription Communication Status** metric, which reported the communication status for Application

Protection, CachePulse, and Geolocation in previous SGOS versions, has been removed from **Statistics > Health Monitoring > Status**. In SGOS 6.6.x, the communication status of each subscription service (including services introduced in this release) is reported separately on **Statistics > Health Monitoring > Subscription**.

Management Console

- A read-only Blue Coat appliance CA certificate list (CCL) called `bluecoat-appliance` has been created, which trusts only Blue Coat appliance keys. The ProxySG appliance automatically switches the configuration from using the original `appliance-ccl` to using the new `bluecoat-appliance` CCL if the `appliance-ccl` is unmodified; if `appliance-ccl` was modified, the appliance continues to use the original `appliance-ccl`.
- The Management Console might time out while in use. For security reasons, the timeout period is now based on communication between the Management Console and the Blue Coat ProxySG appliance itself, not on activity in the Management Console interface. For example, actions such as moving between tabs or opening and closing the Help do not prevent a timeout.

Networking

- The Blue Coat ProxySG appliance now supports disabling and enabling specific adapters and VLAN IP addresses. This provides for additional security; you may disable any adapters not specifically in use. If you attempt to disable an interface configured with the IP address currently being used to access the Management Console, you will see a message warning you of potential loss of connectivity.
    - By default, all interfaces are enabled (not shut down).
    - The **Configure Interface x:x** panel now includes an **Enable Interface** selection.
    - If the appliance is downgraded to a version which does not support interface shutdown, no interface will be disabled.

Policy

- Geolocation is now supported for both reverse proxy and forward proxy. Geolocation in SGOS 6.6.2.1 introduces the following behavior changes:
    - When writing policy, country names are case-insensitive. Previously, when geolocation was supported only in reverse proxy, country names were case-sensitive.
    - When geolocation is enabled, connections to all countries are allowed by default until you install geolocation policy to restrict specific countries. These restrictions take effect if the geolocation subscription is valid, the service is enabled, and the database is downloaded.
    - Previously, when geolocation was supported only in reverse proxy, the appliance could not block connections based on country in forward proxy. Now, when the geolocation service is enabled but the subscription is invalid or data is not downloaded, users might experience restricted access.
- In previous versions of SGOS, if you did not specify normalization in policy, the appliance performed URL and HTML entity decoding by default. In SGOS 6.6.2.1, default normalization has been removed; you must now specify normalization in the `http.request.normalization.default()` property. For information, see the *Content Policy Language Reference*.
- The `http.request.data=` condition has been updated. You can now specify a value up to 65536 for the number of bytes to inspect in the body of an HTTP request. Previously, the maximum was 8192.
- If policy includes both the `http.request.data=` condition and the new `http.request.body.inspection_size()` property, WAF advanced engines now use the greatest specified value for the scanning limit.

VOD Pre-Population

- SGOS 6.6.2.1 supports prepopulating Flash content using RTMP. Flash content prepopulated using the CLI `content distribute` command remains in cache after downgrading to a pre-6.6.2 release, and pre-pop commands for Flash VOD fail.

Deprecations and Removals

- Web Application Firewall (WAF) features introduced in SGOS 6.5.x are no longer available in the VPM. In SGOS 6.6.2.1, WAF support is in CPL only. The following VPM elements have been removed:
  - **Web Application Protection** policy layer
  - **Web Application Protection** object
  - **Risk Score** object

  If the Web Application Protection layer still appears in the VPM or CPL, refer to TECH245671.

  In addition, the `x-risk-category` and `x-risk-score` fields have been removed from the `bcreporterwarp_v1` access log format.
- The `http.request.detection.injection.sql()` property has been deprecated. SGOS 6.6.2.1 introduces `define application_protection_set` for detecting SQL injection attacks. For more information, refer to the *Content Policy Language Reference*.
- The **Trace** object in the VPM has been simplified to allow you to either fully disable or fully enable tracing. The intermediate levels (request tracing and rule/request tracing) have been removed. In addition, the corresponding `trace.rules()` property has been deprecated.

  Note that if you specified request, rule/request, or verbose tracing in policy before upgrading to SGOS 6.6.2.1, tracing is enabled after the upgrade.
- The `#show sources policy common` command has been removed. Use the `#show policy source` command instead.
- WebPulse now always uses secure connections. The following have been removed:
  - The **Use secure connections** option in the Management Console (**Configuration > Threat Protection > WebPulse**)
  - The CLI command `#(config bluecoat) service secure {enable | disable}`
- The `#(config bluecoat) view applications` and `#(config bluecoat) view operations` commands have been removed. To view content filtering details, use the `#(config bluecoat) view` command.

Behavior Changes in SGOS 6.6.3.2

Unlimited Users with Web Application Protection License

- In a reverse proxy deployment, if you have an existing valid Web Application Protection subscription and the service is enabled, the system no longer enforces the user limit prescribed by the Blue Coat ProxySG appliance's base license.

  This does not apply to the SG300, SG600, or SG900 platforms. On those appliances, the base license's user limit always applies

  The system enforces the user limit again if the subscription expires or you disable the service, and does not allow unlimited users until you renew the subscription or enable the service again. If you downgrade SGOS, the system enforces the user limit.

Upgrade/downgrade	Both: Valid subscription Enabled service	Either: Invalid subscription Disabled service
Upgrade to SGOS 6.6.3.2	No user limit	Enforced user limit
Downgrade to SGOS 6.6.2.x or 6.5.x	Enforced user limit	Enforced user limit

Deprecations and Removals

- The following conditions have been renamed:

Previous CPL	Current CPL
`url.application.name=`	`request.application.name=`
`url.application.operation=`	`request.application.operation=`

- The `x-bluecoat-transaction-id` field in the bcreporterwarp_v1 access log format has been replaced with the new `x-bluecoat-transaction-uuid` field.

Behavior Changes in SGOS 6.6.4.1

Authentication

When the Blue Coat ProxySG appliance tries to establish a secure channel with the domain controller (DC) in IWA Direct, SMB signing must be enabled on the DC when trying to establish a secure channel. This change of behavior was made to address the Badlock vulnerability (CVE-2016-2115 and CVE-20162118).

Content Filtering

When an enabled valid content filtering provider cannot categorize a test URL, it now returns a result of “none”; previously, it did not return a result. If the provider's Lookup mode is set to Uncategorized, the "none" result is not visible; however, if the Lookup mode is set to Always, the "none" result is visible. Refer to the following examples of the current behavior:

Lookup Mode set to Always	Lookup Mode set to Uncategorized
If a URL matches a custom category in policy and a Blue Coat WebFilter category, testing it yields the following responses:	

Current and previous behavior:
`Policy: Policy-Shopping`
`Blue Coat: Shopping`
	Current and previous behavior:
	`Policy: Policy-Shopping`
	`Blue Coat: Shopping`

If a URL does not match any custom category in policy but matches a Blue Coat WebFilter category, testing it yields the following responses:	

Current behavior:
`Policy: none`
`Blue Coat: News/Media`
Previous behavior:
`Blue Coat: News/Media`
	Current and previous behavior:
	`Blue Coat: News/Media`

If a URL matches a custom category in policy but not a Blue Coat WebFilter category, testing it yields the following responses:	

Current behavior:
`Policy: Policy-Shopping`
`Blue Coat: none`
Previous behavior:
`Policy: Policy-Shopping`
	Current and previous behavior:
	`Policy: Policy-Shopping`

If a URL does not match any custom category in policy or a Blue Coat WebFilter category, testing it yields the following responses:	

Current and previous behavior:
`Policy: none`
`Blue Coat: none`
	Current and previous behavior:
	`Policy: none`
	`Blue Coat: none`

Hardware

- The Blue Coat ProxySG Virtual Appliance MACH 5 Edition now supports increased VM memory sizes; however, you *must* do the following before upgrading to this release on the SGVA-5-M5 platform:
  1. Update the license key using the CLI command:
     `#licensing update-key`
  2. Set the VM memory to 2048 MB (2 GB).

Symantec recommends increasing the memory sizes for other platforms, but doing so is not a requirement in order to upgrade to this release.

ProxySG VA MACH5 Platform	Supported Memory Size (MB)	VM Memory Increase
SGVA-5-M5	2048	Required
SGVA-10-M5	2560	Recommended
SGVA-15-M5	3072	Recommended
SGVA-20-M5	4096	Recommended

- The ProxySG Secure Web Gateway Virtual Appliance (SWG VA) now supports increased VM memory sizes; however, you must do the following before upgrading to this release on the V-100 platform:
  1. Update the license key using the CLI command:
     `#licensing update-key`
  2. Set the VM memory to 8192 MB (8 GB). For instructions on how to configure the VM memory, refer to TECH245936.

  Symantecincreasing the memory size to 8 GB for all user limits; however, user limits up to and including 1000 users are only required to have 4 GB of memory. User limits above 1000 users are required to have 8 GB of memory.

User Limit for SWG VA V100	Minimum VM Memory Requirements (GB)	Recommended VM Memory (GB)
25	4	8
50	4	8
250	4	8
500	4	8
1000	4	8
1500	8	8
2000	8	8
2500	8	8

MAPI Proxy

- The MAPI over HTTP proxy is enabled by default. If Blue Coat ProxySG policy includes rules that intercept Office 365 traffic and sends that traffic to Content Analysis, Content Analysis scans attachments in messages from Outlook 2013 or Outlook 2010 (with hotfix) clients.

SSL/TLS and PKI

- On an initial upgrade to version 6.6.4.x, if the default protocols (TLS 1.0, 1.1, and 1.2) for the HTTPS Console service were selected previously, only TLS 1.1 and 1.2 are selected by default now. If the HTTPS Console service's protocols were changed from the defaults previously, the selections do not change.

  Note: Any subsequent upgrades to 6.6.4.x, for example after a downgrade, do not change the protocol selections; the protocols selected prior to the subsequent upgrade are retained.

  On a downgrade to version 6.6.4.x, your selections do not change (whether you kept the default selections or changed them).

- Weak ciphers and HMAC algorithms are no longer offered as defaults. If you have upgraded to this release from a previous 6.6.x version, issue the `#(config ssh-console)` **`ciphers reset`** and `#(config ssh-console)` **`hmacs reset`** commands to reset the default list.

  Note: Although these weak ciphers and HMACs are still available for selection (they appear in the `choices` lists in CLI output), Symantec recommends that you issue the `reset` commands after an upgrade and use only strong ciphers and HMACs.

- Keyrings with certificates and/or CSRs over 8k created in this SGOS release are not backward-compatible with previous 6.6.x releases; keys over 8k cannot be used in older SGOS versions. Symantec recommends backing up your current configuration before upgrading and importing and using larger keys, so you can restore your previous configuration if you downgrade. On downgrade, if you can correctly view the Keyring/External Certificate/CSR properties, then that item is usable.

Deprecations and Removals

- The `s-icap-status` access log field is deprecated and has been replaced with the following unique status fields:
  - `cs-icap-status`: request modification
  - `rs-icap-status`: response modification

Behavior Changes in SGOS 6.6.5.1

Improved WAF Command Injection Engine

- By default, the command injection engine detects a wider set of attacks, including non-chained command injection payloads. The existing `define application_protection_set` definition has been updated with a new keyword/property to support this new version of the engine.

  Although you can change the command injection engine version in CPL, Symantec recommends that you keep the default setting to use the current version of the engine.

  To use the previous version of the engine, specify the `version=2` keyword/property, as follows:

```
define application_protection_set mySet
   engine=injection.command version=2
end
<proxy>
 http.requestion.detection.mySet(block)
```

  To return to the default setting, specify `version=3`, as follows:

```
define application_protection_set mySet
  engine=injection.command version=3
end
<proxy>
 http.requestion.detection.mySet(block)
```

Policy

- Upon an upgrade to this release, ProxySG policy engine disables RDNS lookups by default. Policy gestures that trigger an RDNS lookup may be affected. This change was made to prevent potential misuse of RDNS by malicious third parties. A new CLI command was introduced to control whether an RDNS lookup is used or not:
  `#(config) policy restrict-rdns {all | none}`
  The command is set to `all` by default. If you allow RDNS lookups by changing the setting to `none`, downgrade SGOS, and then upgrade to this release again, RDNS lookups are still allowed (the `none` setting is preserved).

  
  Using the `restrict rdns` definition block in policy allows RDNS lookups, regardless of the CLI setting.

Behavior Changes in SGOS 6.6.5.10

Networking

- The maximum bandwidth has been increased to 10 Gb. Set maximum bandwidth using the following CLI command:

  `#(config bw-class` *`class_name`*`)` **`max-bandwidth`** *`maximum_in_kbps`*

Behavior Changes Applicable to SGOS 6.7.x Upgrade/Downgrade

The behavior changes below are listed under the SGOS 6.7.x version in which they were introduced. After a change is introduced, it is included in all subsequent 6.7.x releases.

Be aware of deprecations, removals, and downgrade notes before attempting to downgrade from version 6.7.x.

Behavior Changes in SGOS 6.7.1.1

Authentication

- In previous versions of SGOS, the appliance sent LDAP pings for domain controller discovery over the TCP protocol. In SGOS 6.7.1.1, you can specify UDP or TCP as the protocol using the following command:

  ```
  #(config security windows-domains)ldap-ping-protocol {tcp | udp}
  ```

  When upgrading to this release, the TCP setting is preserved for existing Windows domains and the default for new domains is UDP.

- By default, the appliance now uses the SMB2 protocol for connecting to the Active Directory server. If the server only supports the SMB1 protocol, you can change the default using the following command:

  ```
  #(config security windows-domains)smb2 disable
  ```

  For best security, Symantec strongly recommends that you use the SMB2 protocol.

Emulated Server Certificate Keyring Sizes

- When the ProxySG appliance emulates RSA server certificates, it will match the key size up to a maximum of 4096 bits. When the appliance emulates DSA/ECDSA server certificates, it will emulate an RSA certificate up to 2048 bits.
- On downgrade, keyrings exceeding 2k for RSA certificates and 1k for DSA and ECDSA certificates created in this SGOS release will be lost.

ECDSA Certificate Support

- This release includes support for ECDSA signed certificates. The ProxySG appliance can now verify ECDSA certificates during the SSL handshake, as well as DSA and RSA signed certificates.

HSM Failover

- If the ProxySG appliance encounters an error when attempting to use an hsm-keyring, it is flagged as failed. The signing operations will be tried on another member of the HSM key group, if applicable. The ProxySG appliance will periodically attempt to see if the error has been corrected. Once it has been, the signing key will be put back into service.

HTTP Proxy

- After an initial upgrade to this release, the following pipeline settings (in the Management Console, **Configuration > Proxy Settings > HTTP Proxy**) are disabled by default in the **Normal** profile:

- Pipeline embedded objects in client request
- Pipeline redirects for client request
- Pipeline embedded objects in prefetch request
- Pipeline redirects for prefetch request

Any of these options that were enabled previously are disabled after the upgrade; however, if you enable them again, the setting persists through subsequent upgrades.

Policy

- In this release, `exception.all` includes the transaction ID by default. As a result, by default all exception pages include text such as the following:

  "Transaction ID: c27001ec614d1217-00000000000002d1-0000000058238d68"

  Because this is an update to all existing exceptions, you must manually update the current exceptions definition. See "Update Exceptions Manually" on page 79 for instructions.

- Auto-complete is now disabled for all password fields in forms on policy exception pages. After an upgrade, the system does not pick up the changes automatically; must edit your current exceptions manually to get the changes. See "Update Exceptions Manually" on page 79 for instructions.

Secure Web Gateway Virtual Appliance

- The default network adapter for the Secure Web Gateway Virtual Appliance (SWG VA) in SGOS 6.7.x is VMXNET3. To downgrade the SWG VA from version 6.7.x to 6.6.x or 6.5.x, first change the network adapters to E1000.

  For example, to change the adapters in VMware vSphere Client:

  1. Power off the VM.
  2. Right-click the VM and select **Edit Settings**.
  3. The **Hardware** tab should display four VMXNET3-type adapters; remove each one.
  4. Add four new ethernet adapters, specifying **E1000** as the type.

SSH

- After an upgrade or downgrade, the current list of ciphers and the current list of HMACs—as shown in `view` subcommand output—may change. If you modify the current list using the `add`, `remove`, and `set` subcommands, the changes persist after system upgrades, downgrades, and reboots; however, the current list will not be identical to the list prior to upgrade/downgrade if the SGOS version must consider deprecated ciphers and HMACs.

  To understand the behavior after upgrade/downgrade, refer to `#(config ssh-console)` **`ciphers`** and `#(config ssh-console)` **`hmacs`** in the "Privileged Mode Configure Commands" chapter in the *Command Line Interface Reference*.

SSL Proxy

- By default, trust-destination-ip is now set to true for upstream SSL proxy connections in transparent deployments. As a result, when server name indication (SNI) is implemented, the appliance does not perform DNS resolution on the hostname in HTTP headers, and trusts the destination IP in the client hello message instead.

TLS and Cipher Defaults

- TLS 1.1 and 1.2 are the default protocols for Management Console connections to Symantec, and for the default SSL device profile, once TLS 1.2 support has been verified. TLS v1.1 will be used if 1.2 is not available.

Deprecations and Removals

- For better security, the SSLv2 and SSLv3 protocols are no longer available for device profiles and the HTTPS-Console service.
- The following CLI commands are removed in SGOS 6.7.x:
  - `#(config ssh-console) ciphers demote`
  - `#(config ssh-console) ciphers promote`
  - `#(config ssh-console) hmacs demote`
  - `#(config ssh-console) hmacs promote`

Behavior Changes in SGOS 6.7.4

Deprecations and Removals

- For better security, the following hidden CLI commands are deprecated:

  `#(config) show config with-keyrings`

  `#(config) show config with-keyrings unencrypted`

  To specify how `show config` output displays keyrings, use the new CLI:

  `#(config) security private-key-display` *subcommands*

  The settings apply only to the current terminal session.

  Refer to the *Command Line Interface Reference* for details.

Important Consideration for Downgrades to Versions Prior to SGOS 6.7.4

If you intend to downgrade to a version prior to SGOS 6.7.4, you must first take additional steps to roll back the implicit FTPS configuration. Failure to do so can result in dropped explicit and implicit FTPS connections.

Before downgrading to SGOS 6.7.3 and earlier, perform the following steps:

1. Set existing FTPS proxy listeners to Bypass:
   a. From the Management Console, select **Configuration > Services > Proxy Services**.
   b. Expand the **Standard** list to locate the FTPS service.
   c. Select the service and click **Edit Service**.
   d. On the Edit Service dialog, beside Service Group, select **Bypass Recommended**.
   e. Click **OK** to save the settings.
   f. In the Bypass Recommended list, beside the FTPS service, select **Bypass** from the drop-down menu.
   g. Click **Apply**.
2. Remove any instances of the following FTPS method CPL from policy:
   - `ftp.method=AUTH`
   - `ftp.method=PBSZ`
   - `ftp.method=PROT`

About Deprecated Content Policy Language

Symantec periodically eliminates or replaces CPL constructs with new constructs that are more flexible or powerful. Symantec does not immediately remove these constructs; they are in a deprecated to give you advance notice of these changes.

When a policy construct is deprecated, you can still use it in policy, but you should replace it with the new construct before upgrading to the next major release (for example, from SGOS 5.x to 6.x). Deprecated policy constructs may be removed in the next major release and can cause policy load failures.

The VPM automatically generates up-to-date CPL syntax for VPM-generated CPL. If the VPM issues deprecation warnings, you should reinstall the policy though the VPM to regenerate the CPL. For policy that wasn't installed in the VPM, you must manually edit the local, central, and/or forward policy files to replace deprecated constructs with new constructs.

As part of policy migration strategy, deprecation warnings are issued for CPL syntax that is going to be removed in a future release. If the currently installed policy contains deprecated CPL, you receive an error message when you attempt to install it. In the Management Console, the error is as follows:

```
Policy deprecation warnings exist. Please resolve them prior to upgrading to the
next major release of system software.
```

When you use the #**load upgrade command** in the CLI, the error is as follows:

```
WARNING: The installed policy contains deprecation warnings. Please fix these warn-
ings prior to upgrading to the next major release, or use load upgrade ignore-warn-
ings at your own risk. Upgrading to the next major release with deprecation
warnings will cause the policy compilation to fail on boot.
```

In general, when you load policy in the CLI or the Management Console, warnings indicate that there is deprecated policy, for example:

```
Deprecation warning: 'category.dynamic.mode' has been replaced by 'webpulse.c-
ategorize.mode'

cpl.local:47: category.dynamic.mode(realtime)
```

The line following the warning also indicates where the deprecated policy is in use. For example, `cpl.local:47` indicates that it is line 47 in the local policy file.

Review the list of deprecated CPL for your target release. See "Deprecated Policy Constructs" on the facing page.

Under special circumstances, you can force an upgrade of SGOS if deprecation errors exist. See "Force an Upgrade" on page 57.

Deprecated Policy Constructs

The following tables list the policy constructs that were deprecated in the specified versions and indicates whether the construct has been abandoned in the next major release. Even if the construct has not been abandoned, the best practice is to always replace the deprecated construct with the new syntax.

CPL Triggers and Properties Deprecated in SGOS 6.6.3.x

Deprecated Construct	Replacement Construct	Abandoned in 7.x?
`url.application.name=`	`request.application.name=`	
`url.application.operation=`	`request.application.operation=`	

CPL Triggers and Properties Deprecated in SGOS 6.6.2.x

Deprecated Construct	Replacement Construct	Abandoned in 7.x?
`http.request.detection.injection.sql()`	`define application_protection_set`	
`proxy.card=`	`client.interface=`	
`trace.rules()`	None; functionality removed.	

CPL Triggers and Properties Deprecated in SGOS 6.5.x

Deprecated Construct	Replacement Construct	Abandoned in 7.x?
im.buddy_id= im.chat_room.conference= im.chat_room.id= im.chat_room.invite_only= im.chat_room.type= im.chat_room.member= im.chat_room.voice_enabled= im.file.extension=im.file.name= im.file.path= im.file.size= im.message.opcode=im.message.reflected= im.message.route= im.message.size= im.message.text= im.message.type= im.method= im.user_id=	None; features removed.	

CPL Triggers and Properties Deprecated in SGOS 5.x

Deprecated Construct	Replacement Construct	Abandoned in 6.x?
category.dynamic.mode(none | realtime | background | default)	webpulse.categorize.mode (none | realtime | background | default)	No
force_patience_page(yes)	response.icap_feedback.force_interactive(yes)	No
force_patience_page.useragent(yes)	response.icap_feedback.force_interactive.user-agent(yes)	No
force_patience_page[useragent, extension, contenttype](yes)	response.icap_feedback.force_interactive [user-agent, extension, contenttype](yes)	No

Deprecated Construct	Replacement Construct	Abandoned in 6.x?
`force_patience_page(useragent, extension)`	`response.icap_feedback.force_interactive (user-agent, extension)`	No
`icp(yes|no)`	None; feature removed.	No
`patience_page(no)`	`response.icap_feedback.interactive(no)`	No
`patience_page(delay)`	`reponse.icap_feedback (patience_page, delay)`	No

`socks.allow_compression()`	`adn.server.optimize()`
	`adn.server.optimize.inbound()`
	`adn.server.optimize.outbound()`
		No

`socks.gateway.request_compression()`	`adn.server.optimize()`
	`adn.server.optimize.inbound()`
	`adn.server.optimize.outbound()`
		No

`$(session.username)` exception page substitution	`$(session-monitor.attribute.calling-station-id)`	No
`ttl(0)`	`ttl(auto)`	Yes

CPL Triggers and Properties Deprecated in SGOS 4.x

Deprecated Construct	Replacement Construct	Abandoned in 5.x?
`attribute.name=ServiceType`	`attribute.name=Service-Type`	No
`client.connection.negotiated_cipher=` deprecated in `<Proxy>` and `<Exception>` layers	`client.connection.negotiated_cipher=` can be used only in `<SSL>` layer	No
`client.connection.negotiated_cipher. strength=` deprecated in `<Proxy>` and `<Exception>` layers	`client.connection.negotiated_cipher. strength=` can be used only in `<SSL>` layer	No
`content_admin=yes|no`	`content_management=yes|no`	Yes
`http.x_method=`	`http.method.custom=`	Yes
`transform active_content`	`define active_content`	Yes

Deprecated Construct	Replacement Construct	Abandoned in 5.x?
`transform url_rewrite`	`define url_rewrite`	Yes

Force an Upgrade

You can force an upgrade even if policy contains deprecate constructs; however, after the upgrade, policy compilation will fail and the Blue Coat ProxySG appliance will revert to the default policy of ALLOW or DENY. You must take corrective action to restore normal operation.

For this reason, you should only force and upgrade in special situations. For example, it could be appropriate when you are upgrading an appliance on which you will later install a new version of policy. You might do this in the following cases:

- You are upgrading a number of appliances from Director.
- After having upgraded policy on one appliance, upgraded the software, and tested new features in that release, you are preparing to roll out the upgrade. You could force an upgrade and immediately replace the policy before bringing the appliance online.

To force an upgrade, issue the CLI command in enabled mode:

```
#load upgrade ignore warnings
```

Upgrade or Downgrade SGOS on the Same Appliance

Perform the following steps to upgrade or downgrade SGOS.

1. Determine whether to change the HTB format.
2. (If you are upgrading from SGOS 5.x to 6.x) Resolve CPL deprecations.
3. (If you are upgrading from SGOS 5.x to 6.x) Migrate policy.
4. Archive the current configuration.
5. (If you are not running in Trial Mode) Download the SGOS license.
6. (If you use SWG or MACH5 with SWG authentication (Direct to Net)) Upgrade the BCAAA service.
   This is only necessary if the next release uses a different BCAAA version.
7. Install the SGOS software release.
   This is either the target release or an intermediate release, depending on the upgrade path. Consult the upgrade path diagram and repeat this step as needed until you reach the target release.
8. (If you are upgrading from SGOS 5.x to 6.x, and a previous 6.x configuration that is not the intended target configuration exists) Convert SGOS configuration settings.
9. Verify license validity.
10. (If you are running a licensed appliance and did not download the license in step 5) Manually upgrade the license.
11. Access the Management Console and clear the browser cache.
12. Check for errors in policy compilation and exception pages.
13. Update exceptions manually.
14. (If you use MACH5 with SWG and are upgrading to SGOS 6.x from a version older than 5.5.1.1) Enable regular transparent tunnels.
15. (If you decided to change it in step 2) Change the HTB format.
16. Remove older SGOS images.
    This should avert an accidental downgrade to an incompatible release.
17. (If you use MACH5 with SWG) Once all platforms are upgraded to 6.x, enable fast transparent tunnels.
18. (If applicable) Correct the ProxyClient version.

Determine Whether to Change HTB Format

This step is **recommended** if you are upgrading:
- SGOS 6.2 or later in an ADN
- SGOS 6.2 or later on SG900 or SG9000 models in a non-ADN
- SGOS 5.x or 6.1 to SGOS 6.2 or later in a non-ADN

Skip this step if you are migrating to a new appliance.

SGOS 6.2 and later includes an object store HTB format called HTBv2. The HTBv2 format supports a higher limit on the maximum number of objects that each disk can store.

When determining which HTB format to use, consider the following:

- Releases prior to SGOS 6.2 use HTBv1; SGOS 6.2 and later can use either HTBv1 or HTBv2.
- When upgrading from SGOS 5.x or 6.1.x to 6.2 and later, the appliance preserves the HTBv1 format.

Considerations

If you are upgrading SGOS 6.2 or later (for example, from 6.2.x to 6.4.x) in an ADN, you may want to use HTBv1 because that format benefits ADN performance. To determine the HTB version you are running, see "Verify the Current HTB Format" on the next page.

If you are upgrading from SGOS 5.x or 6.1.x to 6.2 and later in a non-ADN, you may want to use HTBv2 because that format benefits object caching capacity. In addition, converting an SG900 or SG9000 model to HTBv2 allows it to store a much larger number of objects.

Refer to the following table to determine if you should change the HTB format after upgrading.

Network	Current HTB format	Should you consider changing the format after upgrading?	Next step
ADN	HTBv1	No. HTBv1 is optimal for ADN.	"Clear the Byte Cache" on page 61
	HTBv2	Yes. HTBv1 benefits ADN performance on a multi-disk ProxySG appliance.*	"Reinitialize Disks" on page 62
SWG	HTBv1	Yes. HTBv2 benefits object caching, and also allows for more object storage on SG900 and SG9000.*	You will change the HTB format later in the upgrade process.
	HTBv2	Not applicable.	"Clear the Byte Cache" on page 61

* If you use a single-disk appliance, there is no benefit in changing the HTB format and you would not be able to reinitialize disks. Proceed to "Resolve CPL Deprecations" on page 63.

Verify the Current HTB Format

If you are running SGOS 6.1 or earlier, the disks are formatted with HTBv1 and you do not have to verify the format.

If you are running SGOS 6.2 or later, the disks could be formatted with either HTBv1 or HTBv2. You should verify your current HTB format to determine your next step.

1. In the CLI, enter enable mode.
2. Type the following command:
   `#show disk 1`
3. In the command output, look for the value of Pre 6.2 compatible:

   ```
   Disk in slot 1
   Vendor: TOSHIBA
   Product: MK2001TRKB
   Revision: 0105
   Disk serial number: 8130A06WFM13
   Capacity: 2000398933504 bytes
   Pre 6.2 compatible: no
   Status: present
   ```

   If the value is `yes`, the disks are currently formatted with HTBv1.

   If the value is `no`, the disks are currently formatted with HTBv2.

   Consult the table in "Determine Whether to Change HTB Format" on the previous page to determine your next step.

Clear the Byte Cache

If the byte cache dictionary contains a large amount of data, it can take hours to resynchronize the dictionary with all peers after a restart. During this resynchronization period, byte caching is disabled and you do not have the option to clear the byte cache. To prevent this delay after upgrade, Symantec recommends clearing the byte cache before upgrading.

1. In the Management Console, select **Maintenance > System and Disks > Tasks**.
2. Click **Clear the byte cache**.

Reinitialize Disks

If you plan to change the HTB format, reinitialize disks before proceeding to "Resolve CPL Deprecations" on the facing page. If you do not reinitialize disks prior to upgrading, it can take a substantial amount of time on high-capacity platforms for SGOS to restore all the old HTBs and execute the command to change the HTB format.

Before you reinitialize disks, refer to the appropriate article to back up data:
- For a single-disk system, see TECH242136
- For a multi-disk system, see TECH242581

Reinitializing the disks clears all the HTBs and reduces the time needed to restore the disks after an `upgrade-restart` to 5 to 10 minutes.

1. In the CLI, enter enable mode.
2. Enter the following command for each disk:

   `#disk reinitialize <disk_number>`

   Type `y` to confirm the action.

   If you specify any disks that are not present, the commands terminate with a message.

You can execute a series of commands quickly by entering a series of CLI commands, such as the `#disk reinitialize` commands for each disk, into a text file. Then, copy and paste all of the commands into the CLI. For example, after you enter enable mode, you can copy and paste a list of commands like the following:

```
disk reinitialize 1
y
disk reinitialize 2
y
disk reinitialize 3
y
disk reinitialize 4
y
```

Resolve CPL Deprecations

This step is **mandatory** if one or more of the following applies to you:
- You are upgrading SGOS from 5.x to 6.x on the same appliance
- You are upgrading from 5.x to 6.x and migrating to a new appliance
- You use authentication realms

You must resolve all deprecated CPL before upgrading or migrating to a new appliance.

In the CLI, run the following command to view the deprecations:

```
#(config) show policy listing
```

If your policy contains deprecated commands, the CLI displays a line similar to the following:

```
'request.icap_service(no)'. In the next major release this will be an error
```

You must then replace all instances of the deprecated command(s) in your policy.

If you do not resolve CPL deprecations, policy will not compile after upgrade or appliance migration. For more information, see "Deprecated Policy Constructs" on page 53.

If you use authentication realms for administrator access and are upgrading to SGOS 6.5.x, a policy compilation error occurs if an authentication realm that is referenced in policy is not supported.

Migrate Policy

This step is **mandatory** before an upgrade from SGOS 5.x to 6.x on the same appliance.

If you are migrating a configuration from a ProxySG appliance running SGOS 5.x to a new appliance that runs SGOS 6.x, perform these steps on the previous appliance. For information, refer to *Migrating to a New Blue Coat ProxySG Appliance*:
http://www.symantec.com/docs/DOC10323

The upgrade path must include a version that shows all possible deprecation warnings so that you can correct them and avoid policy compilation failures after upgrading. The appropriate versions are indicated in the procedure that follows.

1. (If necessary) Upgrade to SGOS 5.5.10.1 or later.

   SGOS 5.5.10.1 contains all pre-6.x deprecation warnings.

   a. Download the image file. See "Download Files from MySymantec" on page 6.
   b. In the Management Console, select **Maintenance > Upgrade**.
   c. In the 'Upgrade actions' section, click **Upload**.
   d. On the dialog that opens, click **Choose File** and browse to where you downloaded the SGOS image.
   e. Select the file and click **Install**. Wait for the file to install and then close the dialog.
   f. Click **Restart** to boot the appliance with the new system.
2. Load the VPM to upgrade VPM-generated syntax.
   a. In the Management Console, select **Configuration > Policy > VPM > Launch**.
   b. Click **Install policy**.
3. Display deprecation warnings in policy.
   a. Select **Configuration > Policy > Policy Files**.
   b. From the View File menu, select **Results of Policy Load**, and click **View**.
4. Identify deprecation warnings.

   Deprecation warnings look similar to the following:

   ```
   Deprecation warning: 'category.dynamic.mode' has been replaced by
   'webpulse.categorize.mode'cpl.local:25: category.dynamic.mode(default)
   ```

   The previous deprecation warning indicates that deprecated code is in the local policy file. Other messages could indicate the CPL is in the central or forward file.

5. Replace deprecated syntax with the new syntax.
   a. Select **Configuration > Policy > Policy Files**.
   b. Go to the **Install Local File from** line, select **Text Editor** from the menu, and click **Install**. The Edit and Install the Local File dialog opens.
      If the deprecated code is in the central or forward policy file, choose the corresponding options.
   c. For each deprecation warning, copy or type the suggested replacement syntax.
   d. Click **Install**.

   Proceed to the next step if you receive error messages.

   See "Deprecated Policy Constructs" on page 53 for a list of deprecated constructs and the replacement syntax.

6. (If applicable) Identify errors.

   Identify any errors that occurred when you installed policy. If there were no errors, proceed to the next step.

   If your policy contains any syntax errors, the 'Error Installing File' message appears. Error messages look similar to the following:

   ```
   Error: Invalid value: '0' for tag 'response.icap_feedback'

   cpl.forward:2: response.icap_feedback(0)
   ```

   Repeat step 5 to fix any typing errors or syntax errors.

7. Check for deprecation warnings in exception pages.

   Exception pages are error messages that are sent in response to certain Blue Coat ProxySG appliance client requests, such as denial by policy, failure to handle the request, and authentication failure. Exception pages display in the browser.

   a. Select **Configuration > Policy > Exceptions**.
   b. From the View File list, select **Results of Exceptions Load**, and click **View**.

   You will check for deprecation warnings in exception pages again, after you upgrade to SGOS 6.x.

8. Replace deprecated syntax in exception pages with the new syntax.
   a. Select **Configuration > Policy > Exceptions**.
   b. From the Install Exceptions Definitions from list, select **Text Editor**, and click **Install**.
   c. Replace the deprecated syntax with the new syntax.
   d. Click **Install** to install the revised exception definitions.
   e. Fix any errors you may have introduced, and then reinstall the definitions.

Archive the Configuration

This step is **highly recommended** before any upgrade or downgrade of SGOS.

Before upgrading or downgrading SGOS, you should archive your current configuration. Creating a configuration archive ensures that a backup is available should any issues occur as a result of the upgrade/downgrade. If you encounter an issue after an upgrade/downgrade, you can restore the previous SGOS version and then restore the configuration.

If you are archiving the configuration from an appliance running SGOS 5.x and plan to restore it to an appliance running 6.x,you must perform additional steps. Refer to *Migrating to a New ProxySG Appliance* ay MySymantec.

1. In a web browser, access the Management Console of the Blue Coat ProxySG appliance you want to back up: https://<*ProxySG_IP_address*>:8082
2. Select **Configuration > General > Archive**.
3. In the View Current Configuration area, from the View File menu, select **Configuration - expanded**.
4. In the Install Configuration area, clear the **Enforce installation of signed archives** option.
5. Click **View**. A browser window opens and displays the configuration. You can also view the file by selecting **Text Editor** in the Install Configuration panel and clicking **Install**.
6. Copy the configuration to a text file and save it in a secure location.

To restore an archived configuration file, refer to “Restoring a Configuration Archive” in the *SGOS Administration Guide*. You should restore configuration files only on appliances running the same SGOS release version. For example, restore configuration files from SGOS 5.5.6.x only to appliances running SGOS 5.5.6.x.

Download the License

This step is:
- **Recommended** if you are upgrading from SGOS 5.x to 6.x on the same appliance and plan to run the appliance in licensed mode (not in Trial Mode).
- **Mandatory** if you are upgrading SGOS and migrating to a new appliance.

If you do not download the license in this step, you will have to manually upgrade the license in "Manually Update the License" on page 76.

The Blue Coat ProxySG appliance can automatically check for license updates upon reboot or once daily for a month before the currently installed license expires.

Verify that the appliance is set to automatically check for license updates. In the Management Console, select **Maintenance > Licensing > Install**. If the Use Auto-Update option is selected, the appliance is set to automatically check for license updates.

A current, valid license is required to configure the Use Auto-Update option.

If the Use Auto-Update option is selected, the appliance retrieves and installs the SGOS 6.x license if all of the following conditions are true:

- The appliance running the previous version also supports SGOS 6.x (refer to the *Release Notes* for the previous version to verify if this is true).
- Your enterprise has a valid entitlement/service contract from Symantec.
- The appliance can connect to the Internet.

If you do not select the Use Auto-Update option, you can click the **Update** button to manually update the license at any time (as long as the appliance can connect to the Internet).

Note that the **Maintenance > Licensing > View tab > Licensed Components** area does not contain the new SGOS 6.x license or display the line until the SGOS 6.x software is installed.

If you do not retrieve an upgraded license before you download and install SGOS 6.5.x, the appliance runs in Trial Mode and you must upgrade the license manually; see "Manually Update the License" on page 76 for instructions. Alternatively, you can downgrade to the previous release and retrieve the license as described previously.

Upgrade the BCAAA Service

This step is **mandatory** if your target SGOS version uses a BCAAA version different from your current BCAAA version, and you use any of the following authentication realms:
- IWA
- CA eTrust SiteMinder 5.5/6.0
- Windows SSO
- Novell SSO

Prerequisite: Review *BCAAA Service Requirements* at MySymantec:
For BCAAA 6.1: http://www.symantec.com/docs/DOC10043

This step applies to you if use the BCAAA service. If you do not use BCAAA, proceed to "Install the SGOS Software Release" on page 70.

BCAAA Upgrade Notes

Before installing SGOS, always ensure you are running a BCAAA version that includes support for the BCAAA version required by the SGOS release. You must install the compatible BCAAA service before upgrading or downgrading SGOS.

To install or upgrade BCAAA, you must stop the service while files are copied during the installation process. If you have configured a backup BCAAA server, the Blue Coat ProxySG appliance will fail over to that server when BCAAA is stopped. If you have not configured a backup BCAAA server, you must schedule downtime to perform the installation.

Download and install BCAAA 6.1

Determine the version of BCAAA you want to install. Consult the *BCAAA Service Requirements* to ensure that your version is compatible with the SGOS version and for information on installing BCAAA, including how to install multiple versions.

Windows Server 2008 or later is required for BCAAA 6.1.

1. (If you are currently running BCAAA 5.x or earlier) Uninstall the current version of BCAAA.
   If you do not uninstall BCAAA 5.x or earlier, you will not be able to install BCAAA 6.1.
2. Download BCAAA 6.1 from the following URL: http://appliance.bluecoat.com/sgos/bcaaa/v6/bcaaa_windows.zip
3. When prompted, save the ZIP file to the server where you plan to install BCAAA (or save it to a location that you can access from that server).
4. Locate the ZIP file you downloaded.
5. Extract the EXE file and double click it. The BCAAA setup wizard opens.
6. Follow the steps in the installation wizard.

Download and install BCAAA (pre-version 6.1)

1. (If you are currently running BCAAA version 110) Determine the upgrade path for BCAAA.

   a. Identify all BCAAA versions required for your upgrade or downgrade.
   b. Examine your SGOS upgrade or downgrade path; see "Determine the Upgrade/Downgrade Path" on page 10.
   c. Record the BCAAA versions required for all interim SGOS releases. You must install the correct BCAAA version before installing the SGOS upgrade.

2. Download and install the BCAAA version for the target SGOS release. See "Download Files from MySymantec" on page 6.

3. Determine the current version of BCAAA on the authentication server:

   a. Go to the folder where the bcaaa-setup.exe resides, for example: C:\Program Files\Blue Coat Systems\BCAAA
   b. Right click the bcaaa-setup.exe file, select **Properties**, and click the **Version** tab. (In Windows 2008, click the **Properties and Details** tab.)

4. Locate the ZIP file you downloaded.

5. Extract the EXE file and double click it. The BCAAA setup wizard opens.

6. Follow the steps in the installation wizard.

7. (To install another SGOS version) Check whether the installed BCAAA version includes support for the BCAAA version required by the next SGOS release.
   If it does not support the BCAAA version, repeat the previous step before you install each SGOS release until you arrive at the target version.

Install the SGOS Software Release

This step is **mandatory** before every upgrade or downgrade of SGOS.

To install the SGOS software release, you must obtain the image, and then install it on your appliance. If you must install one or more interim releases before you reach the target release, you must download and install those releases in succession. You must reboot the appliance after installing each interim release.

If you use BCAAA, download and install a compatible BCAAA version before installing each version of SGOS in your upgrade/downgrade path. See "Upgrade the BCAAA Service" on page 68.

Components in Trial Mode

If the appliance is running in Trial Mode, or if you want to use the appliance for evaluation purposes, select **Maintenance > Licensing > View**. In the Licensed Components area, select Trial Components are Enabled. Then, perform the steps in "Manually Update the License" on page 76.

If the appliance is not running in Trial Mode and it automatically downloaded an SGOS 6.x license (or you manually retrieved one by clicking **Update**), proceed to install the SGOS software. After upgrading to SGOS 6.5.x, the Blue Coat ProxySG appliance continues to intercept traffic as configured.

Step 1 - Obtain the release image.

If you can upgrade directly to 6.x, download that image. If your upgrade/downgrade path contains one or more interim releases, download the next one in the path.

"Download Files from MySymantec" on page 6

Step 2 - Install SGOS.

a. Access the appliance Management Console: https://*<ProxySG_IP_address>*:8082
b. Enter your login credentials.
c. Select **Maintenance > Upgrade**.
d. Click **Upload**.
e. In the browser window that opens, click **Choose File** and browse to the location of the image you downloaded in Step 1.
f. Select the image and click **Install**. Wait for the system to upload the file.
g. When the upload is complete, close the browser window.
h. (If you are running SGOS 5.x and want to upgrade to 6.x) Convert configuration settings. See "Convert SGOS Configuration Settings" on page 72. The procedure will return you to this section after you convert configuration settings.
i. (If you are not upgrading SGOS 5.x to 6.x) Click **Restart**. The Blue Coat ProxySG appliance reboots. This might take several minutes. When the reboot is complete, the appliance logs you out.

Symantec recommends that you install and load an image that is one minor release earlier or later than your target release, if one is not already present on the appliance. Keep this image as a backup in case the primary image becomes corrupted.

Step 3 - Verify the installation.

a. Log in to the Management Console.
b. Click the **HOME** link (in the upper right corner). Check the version in the banner to verify that the appliance is running the correct SGOS release.
c. If the version is correct and you do not have to install any interim releases, proceed to "Manually Update the License" on page 76.
   If the version is not correct or if you have to install interim releases, proceed to the next step in this procedure.
d. Select **Maintenance > Upgrade > Systems**.
e. Identify the correct system release and select **Default** for that version.
f. Click **Apply**.
g. Select the **Upgrade** tab and click **Restart**. The appliance reboots.
h. (If necessary) If you must install another release to reach the target version, download and install the appropriate releases. See "Download Files from MySymantec" on page 6.
i. After you have installed and verified your target SGOS version, proceed to "Verify License Validity " on page 75.

Convert SGOS Configuration Settings

This step is mandatory if you are upgrading SGOS from 5.x to 6.x.

The SGOS software includes upgrade handlers designed to convert configuration settings between major release upgrades, such as upgrades from 4.x to 5.x, or from 5.x to 6.x. SGOS creates a new configuration file automatically the first time it boots to a new major version and retains a separate configuration file for each major release on the system.

When you boot up a major release for which a configuration already exists on the system, the SGOS upgrade handler does not create a new configuration; the existing one is used. If you want SGOS to create a new configuration instead, you must convert settings to migrate the configuration from the current release to the target release.

See "How the Appliance Saves Configurations" on page 74 to determine how the appliance saves configurations during an upgrade.

If you are upgrading to SGOS 6.x from 5.x and want to migrate the configuration from version 5.x to 6.x, consult the following table to identify the method you should use to automatically convert the configuration settings.

Version of SGOS 5.x you are upgrading to 6.x	How to convert configuration settings	What the CLI command does
Any 5.x version	a. After you download the SGOS 6.x image, click **Restart**. The appliance will boot up with 6.x as the new default image. b. After the appliance boots up, log into the CLI. c. In enable mode, run `restore-sgos5- config`. d. Enter **y** to proceed. Symantec recommends this method because you can use this command for all 5.x versions.	Restores the ProxySG to settings last used with SGOS 5.x. The ProxySG retains the network settings. For more information on the command, refer to a 6.x edition of the *Command Line Interface Reference*.
SGOS 5.5.4.x and later	a. To start the 6.x upgrade image after loading it, log into the CLI. b. In enable mode, run `restart upgrade keep-sgos5-config`. The CLI logs you out as the system reboots.	Boots the 6.x system image and selects the SGOS 5.x configuration to be migrated to the SGOS 6.x configuration. For more information on the command, refer to a 6.x edition of the *Command Line Interface Reference*.
SGOS 5.5.4.x and later	a. Prior to starting the 6.x upgrade image, log into the CLI. b. In enable mode, run `remove-sgos6- config`. c. In the Management Console, click **Restart** to boot up SGOS 6.x.	Removes any SGOS 6.x configuration file so that when upgrading from SGOS 5.x to 6.x, the configuration settings for 6.x will be based on the current 5.x configuration. For more information on the command, refer to a 5.x edition of the *Command Line Interface Reference*.

After you install the required release(s) and convert configuration settings, verify that you are using the correct SGOS version. See Step 3 in "Install the SGOS Software Release" on page 70.

How the Appliance Saves Configurations

Every time you upgrade or downgrade SGOS, the most recent configuration is saved (where “most recent” is the configuration of the version previous to the target release).

For example, the first time you upgrade from 5.x to 6.x:

- the 5.x version is saved
- a new 6.x configuration is created

You then downgrade to 5.x again:

- the 6.x configuration is saved
- the saved 5.x configuration is used

If you then upgrade to 6.x again:

- the saved 6.x configuration is used
- the 5.x configuration is saved but not converted to the 6.x configuration but any new changes to the 5.x configuration are not converted to the 6.x config.

Which Configuration is the Appliance Using?

You can quickly determine which configuration the appliance is using when you restart the appliance in SGOS 6.x. Look for lines similar to the following in the CLI:

```
Booting Version: SGOS 6.2.12.1, Release id: 104304

Completed major version system upgrade
```

If you see the second line indicating that the system was upgraded, the 5.x configuration was migrated to 6.x. If the second line is not present after you boot into 6.x, an existing 6.x configuration was used. If the 6.x configuration was used but you want to use the 5.x one, you can use the restore-sgso5-config command to replace the 6.x config with the converted 5.x config. See "Convert SGOS Configuration Settings" on page 72 for more information on this command.

Verify License Validity

This step is **mandatory** after an upgrade or downgrade of SGOS.

1. Select the **Maintenance > License > View**.
   The Licensed Components area displays the SGOS 6.x license information.
2. Verify that the license information is correct.
   For example, the Component should display “SGOS 6 Proxy Edition” or “SGOS 6 MACH5” and Valid should display “Yes”.
3. Confirm that the license is valid.
   Select the component and click **View Details**. The Component Name line displays the license type, and the Product Description field displays the version that was shipped on the Blue Coat ProxySG hardware platform, which would differ from the version that you installed. For example, if you had received a new appliance that shipped with SGOS 5.x installed, the Product Description field would display SGOS 5.x information even if you upgrade to SGOS 6.x.

   If the license does not appear to be valid, proceed to "Manually Update the License" on the next page to update the license manually.

   If the license is valid, go to "Access the Management Console" on page 77.

Manually Update the License

This step is **mandatory** if you plan to run a licensed appliance (not in Trial Mode) and one or more of the following applies to you:
- You are upgrading from one major version to another major version, such as SGOS 5.x to 6.x
- You did not download the license in "Download the License" on page 67

If you did not update the license before upgrading SGOS, you must update it now.

1. In the Management Console, select **Maintenance > Licensing > Install**.
2. Click **Update**.

If you receive an 'error' stating that the license is already up to date, your license is current and does not need updating.

If There is No Internet Connection

If you cannot directly access the Internet, contact Symantec Support Services for assistance. Support Services will ask you to provide the hardware serial numbers of the appliances to be upgraded and account details, such as contact name, email address, and BTO account name. If you do not have a BTO account or if you have lost the password, contact Symantec Customer Care.

Access the Management Console

This step is **recommended** after every upgrade or downgrade of SGOS.

After you install the image on the Blue Coat ProxySG appliance, Symantec recommends clearing your web browser cache. Clearing the browser cache triggers a reload of the JAR files. This reloading prevents Java exception errors in the Web browser when you access the Management Console.

If the Management Console displays some elements incorrectly, make sure that a supported version of Java is installed. Refer to TECH245893 for the supported Java versions for your SGOS release.

1. Close all Web browser windows.
2. Clear your Web browser cache. The instructions for clearing the cache varies by browser.
3. Clear the Java cache on your computer:
    a. Go to **Start > Control Panel**.
    b. Double click **Java**. Windows displays the Java Control Panel window.
    c. In the General tab, click **Settings** under Temporary Internet Files.
    d. Click **Delete Files**.
    e. Close the Control Panel windows.
4. Launch the Management Console and enter your credentials to log in.

Check for Policy Errors

This step is **recommended** if you performed the steps in Migrate Policy to migrate policy from SGOS 5.x to 6.x.

If you migrated policy from SGOS 5.x to 6.x, make sure that there are no errors in policy compilation or exception pages.

Perform the following steps in the Management Console.

Display deprecation warnings in policy.

a. Select **Configuration > Policy > Policy Files**.
b. From the View File menu, select **Results of Policy Load**, and click **View**.

Check for deprecation warnings in exception pages.

Exception pages are browser error messages that are sent in response to certain Blue Coat ProxySG client requests, such as denial by policy, failure to handle the request, and authentication failure.

a. Select **Configuration > Policy > Exceptions**.
b. From the View File list, select **Results of Exceptions Load**, and then click **View**.

Update Exceptions Manually

This step is **recommended** after an upgrade of SGOS.

After an SGOS upgrade, the default exceptions definitions are updated but the current exceptions with the same name are unchanged; this is expected behavior. If you upgraded to a version that introduces changes to existing exceptions, the set of default exceptions includes them; however, the set of current exceptions does not include them. If the upgraded version introduces new exceptions, the current exceptions are updated to include the new exceptions and you need not take additional steps to use them.

For the ProxySG appliance to pick up default changes to existing exceptions, you must copy the changes from the default exceptions to your current exception definitions.

Step 1: (Optional) Verify that current exceptions do not match the default exceptions

1. In the Management Console, select **Configuration > Policy > Exceptions**.
2. In the View Exceptions section, select **View File: Current Exceptions** and click **View**. The console opens the current exceptions in a new browser tab.
3. Select **View File: Default Exceptions Source** and click **View**. The console opens the default exceptions in a new browser tab.
4. Compare the current exceptions with the default exceptions. Make note of exception changes that you want to install.

Step 2: Insert changed content from default exceptions into current exceptions

1. In the Management Console, select **Configuration > Policy > Exceptions**.
2. In the Installed Exceptions section, select **Install Exceptions Definitions from: Text Editor** and click **Install**. The console opens an edit window.
3. Copy and paste any changed or new code into the text field and customize the exception definitions as required.
4. Click **Install**. If the code contains errors, the exceptions are not installed and the console provides you with the details regarding the error. Fix the errors and install the exceptions.
5. When the exceptions are installed, click **OK** to dismiss the confirmation message and click **Close** to close the edit window.
6. (Optional) Verify that the current exceptions are updated. Select **View File: Current Exceptions** and clickg **View** again, or refresh the tab if it is still open.
7. (If needed) Review how the updated exception pages appear to users. Select **View File: Exceptions Configuration** and click **View**. The console displays a list of exceptions in a new browser tab.

Example: Updating the exceptions after an upgrade to SGOS 6.7.x

Starting in SGOS 6.7.x, `exception.all` includes the transaction ID by default. As a result, by default all exception pages include text such as the following:

"Transaction ID: c27001ec614d1217-00000000000002d1-0000000058238d68"

Because this is an update to all existing exceptions, you must manually update the current exceptions definition. In the default definition, locate the following HTML under `$(exception.help)`:

```
<TR><TD>

<BR>

<FONT face="Helvetica">

Transaction ID: $(x-bluecoat-transaction-uuid)

</FONT>

</TD></TR>
```

Copy and paste the text or the table row into the current exceptions, and edit the HTML as required. Your exact steps depend on whether or not you modified `exceptions.all` previously as well as the extent of those changes.

Enable Regular Transparent Tunnels

This step is **recommended** if your ADN uses transparent tunnels and you are upgrading to SGOS 6.x from a version older than 5.5.1.1.
Symantec recommends that you do this until you upgrade all appliances to a version that supports fast transparent tunnels.

If your ADN uses transparent tunnels and you are upgrading to SGOS 6.x from a version older than 5.5.1.1, you must enable 'regular' transparent tunnels after the upgrade. Doing so ensures that transparent tunnels between the upgraded appliances and appliances running older versions continue to work correctly.

After all appliances that need to communicate with one another are upgraded to one of these 6.x versions, you can re-enable 'fast' transparent tunnels on them all; see "Enable Fast Transparent Tunnels" on page 86.

1. Log in to the CLI.
2. Enter enable mode.
3. Enter configuration mode.
4. Enter the following commands:

```
#(config) adn
#(config adn) tunnel
#(config adn tunnel) connect-transparent enable regular
```

The CLI support for enabling regular transparent tunnels is not included in SGOS 5.5; thus, an upgrade from 5.4.x or earlier to 5.5.x can still create incompatibility between platforms upgraded to 5.5.x and those not yet upgraded.

Determine if you use transparent tunnels

To determine if you use transparent tunnels, issue the following commands in the CLI:

```
#(config)adn

#(config adn)tunnel

#(config adn tunnel)view
```

Look for the `connect-transparent` value in the output:

- `enabled fast` means use fast transparent tunnels
- `enabled regular` means you use regular transparent tunnels
- `disabled` means you do not use transparent tunnels

Change the HTB Format

Perform this step if you decided to change the HTB format in "Determine Whether to Change HTB Format" on page 59.

When you change the HTB format, the configurations, registry settings, policy, licensing files, and appliance birth certificate are preserved. Cached content, access logs, event log, SysInfo, and snapshot files are lost.

1. Log in to the CLI.
2. Enter enable mode.
3. To change the HTB format to HTBv1, type:
   #**disk decrease-object-limit force**
   To change the HTB format to HTBv2, type:
   #**disk increase-object-limit force**

Remove Older SGOS Images

This step is **recommended** after every upgrade or downgrade of SGOS.

After confirming that the upgraded software runs correctly in your network, remove all release images except the target release and one compatible backup.

Symantec recommends that the backup image be one minor release earlier or later than the target release. Removing older releases protects against an unintended downgrade to an SGOS version that does not support the running features or the upgraded licensing subsystem described in ALERT2285.

Refer to TFA109 for a list of SGOS versions that have the license subsystem upgrade. You should remove any versions that are older than the ones listed.

1. Log in to the CLI.
2. Enter configuration mode.
3. Enter the installed-systems node:
   `#(config)installed-systems`
4. Display the images installed on the appliance:
   `#(config installed-systems)view`
5. From the list of images, determine which ones you can remove.
6. Delete the images:
   `#(config installed-systems)delete <system_number>`
7. The CLI prompts you to confirm the deletion. Enter **y**. When the image is deleted, the CLI responds `ok`.

You can remove unused system images only through the CLI (you cannot remove them in the Management Console). See the following Example to see how you can view all installed system images and identify the ones that can be safely removed.

Example

```
#(config installed-systems)view

ProxySG Appliance Systems

1. Version: SGOS 6.2.12.3, Release ID: 104304

     Thursday January 24 2013 21:54:50 UTC,

     Attributes: FIPS capable

     Boot Status: Last boot succeeded, Last Successful Boot: Tuesday February 12 2013
     21:43:43 UTC

     Disk Layout: Compatible

2. Version: SGOS 6.2.12.2, Release ID: 102777

     Tuesday January 8 2013 06:33:41 UTC,

     Attributes: FIPS capable
```

```
     Boot Status: Last boot succeeded, Last Successful Boot: Friday January 11 2013
     20:42:07 UTC

     Disk Layout: Compatible

3. Version: SGOS 5.5.10.3, Release ID: 95906

     Thursday October 18 2012 01:51:40 UTC,

     Attributes: FIPS capable

     Boot Status: Last boot succeeded, Last Successful Boot: Thursday December 27 2012
     19:53:41 UTC

     Disk Layout: Compatible

4. Version: SGOS 6.2.10.6, Release ID: 93869

     Saturday September 22 2012 00:16:10 UTC,

     Attributes: FIPS capable

     Boot Status: Last boot succeeded, Last Successful Boot: Friday January 11 2013
     18:59:14 UTC

     Disk Layout: Compatible

5. Version: SGOS 5.5.3.31, Release ID: 51877

     Tuesday November 9 2010 11:45:07 UTC,

     Attributes: Locked, FIPS capable

     Boot Status: Last boot succeeded, Last Successful Boot: Thursday January 3 2013
     22:18:24 UTC

     Disk Layout: Compatible

     Default system to run on next hardware restart: 1

     System to replace next: 4

     Current running system: 1

#(config installed-systems)delete <system_number>

Are you sure you want to delete system <system_number>? (y or n)y

     ok
```

In this example, the `#(config installed-systems)` **view** command displays information for five installed system images.

To eliminate the risk of accidental downgrade in this scenario, you should remove images 3 through 5 because they do not have the license subsystem upgrade. You can leave image 2 as a backup for the target release (image 1) because it is the second-most-recent installed release.

Each time you delete an image, the images below it move up one slot. In the preceding example, after you delete image 3, images 4 and 5 become images 3 and 4, respectively. In this case, you could issue a delete 3 command three consecutive times to delete the images, or delete the images in descending order (5, 4, 3).

Enable Fast Transparent Tunnels

This step is **optional**. You can do this after all appliances in the ADN are upgraded to SGOS 6.x with regular transparent tunnels enabled.

1. Log in to the CLI.
2. Enter enable mode.
3. Enter configuration mode.
4. Type the following commands:

```
#(config)adn
#(config adn)tunnel
#(config adn tunnel)connect-transparent enable fast
```

Correct the ProxyClient Version

This step is **mandatory** if the ProxyClient version appears to be incorrect after an initial upgrade to an SGOS version of 6.2.12.1 or later.

After the first upgrade to an SGOS version of 6.2.12.1 and later, the ProxyClient software on the ProxyClient manager might change to the default ProxyClient version for the new SGOS version. This happens if the ProxyClient software has also been upgraded.

To work around this issue, reinstall the required ProxyClient software. For instructions, refer to https://support.symantec.com/en_US/Documentation.html.