



## *Blue Coat SGOS 4.2.x Release Notes*

*Version: SGOS 4.2.8.6, build 35252*

*BCAAA Version 120*

*Release Date: 07/21/2008*

*Document Revision: 1.20 on 08/05/2008*

### *Release Note Contents*

This SGOS 4.2.x Release Note document contains the following sections:

- ["Section A: Read Me First"](#)
- ["Section B: Limitations"](#)

## Section A: Read Me First

### Introduction

These release notes apply to Blue Coat® Systems' appliances that are currently running or will be upgraded to the SGOS 4.2.8 release. Before starting the upgrade process, please review these notes.

Blue Coat recommends that you upgrade to the latest patch release listed in these release notes of SGOS 4.2.x.

### Browser Popups

Depending on your browser settings, the VPM module and online help (accessible when you click **Help** at the bottom of any Management Console panel) might not display. If this happens, you must change the browser settings to allow popups.

### Support

Direct support questions regarding this release to Blue Coat Support. For more information, visit: <https://www.bluecoat.com/support/contactsupport>.

### New in this Release

#### *Version SGOS 4.2.8.6, build 35252*

*Release Date: 7/21/08*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1*

*Document Revision: 1.6 on 07/21/2008*

#### **New in this Release**

No new features in this release.

#### **Fixed in this Release**

- ❑ DNS Cache Poisoning Vulnerability (CERT VU#800113).
- ❑ Software restart at 0x4003F in Process "Cache Administrator" in "ce\_admin.dll" at .text+0x8951 after an incomplete object deletion in the RAM cache (97864). This completes the fix for the deadlock situation that caused the HTTP client to build up (B#95795).
- ❑ User-agent was not sent by RTSP proxy when connecting to multicast station's OCS/upstream (B#97091, 2-117077592).
- ❑ Hot-swap HDD was not detected by the SG810 (B#96260).
- ❑ Added support to ttl(0) (B#98109, 2-82029277).
- ❑ Windows Media Proxy: Software restart at 0x4801C in Process "Cache Administrator" in "Kernel.dll" at .text+0xa0d6 (B#96634, 2-115779477).

- ❑ Documentation: The Blue Coat CPL Reference Guide did not include syntaxes for the `request.header.header_name=`, `request.x_header.header_name=`, `response.header.header_name=`, and `response.x_header.header_name=` gestures. The CPL Reference Guide posted for this release (doc version SGOS 4.2.8—07/2008) contains the missing syntaxes.

## Version SGOS 4.2.8.3, build 34781

*Release Date: 06/11/08*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1*

*Document Revision: 1.5 on 06/11/2008*

### New in this Release

This release supports SmartFilter's CGI-based ratings feature: categorization of some URLs now takes into account the URL query string. (B#93933, 2-107888592)

### Fixed in this Release

This release fixes a categorization issue of `youtube.com/verify_age` when using Smartfilter XL. (B#96938, 2-117766481)

## Version: SGOS 4.2.8.2, build 34635

*Release Date: 05/28/2008*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1*

*Document Revision: 1.4 on 06/04/2008*

### New in this Release

- ❑ The SG810 series supports CPU model NE80546EG0721M, 2.8GHz, LV 1M 800FSB.
- ❑ CPL Property: `authenticate.force_307_redirect( )`

Force authentication redirects to use an HTTP 307 response code.

This property only affects authentication redirect modes. i.e. origin-cookie-redirect, origin-ip-redirect, form-cookie-redirect, form-ip-redirect. By default, authentication modes which redirect the browser use an HTTP 307 response code for Internet Explorer and an HTTP 302 response code for all other browsers. If an HTTP POST or PUT request requires authentication, a 307 redirect properly preserves the POST/PUT data, while a 302 redirect will convert the request to a GET and lose the POST/PUT data. The default behavior is to always preserve the POST/PUT data even at the cost of the authentication mode. To avoid losing the POST/PUT data, browsers which would use a 302 redirect are downgraded to a non-redirect authentication mode.

If the POST/PUT contains a multi-part mime type, Internet Explorer will not correctly preserve the data with a 307 redirect. The default behavior is to downgrade all multi-part POST/PUT requests to a non-redirect authentication mode.

Downgrading the authentication mode preserves the data, but means that the user is not authenticated using the virtual URL. This can be an issue if credentials need to be secured by using an SSL virtual url. This property can be used to override the default behavior and force the use of 307 redirects. This will ensure that the user is authenticated using the virtual URL.

Most modern browsers support 307 redirects, but browsers other than Internet Explorer obey the RFC and display a pop-up asking the user if they want to repost the data. This pop-up can be repeated numerous times during authentication.

#### *Syntax*

```
authenticate.force_307_redirect (yes)
```

The default value is no.

#### *Layer and Transaction Notes*

- Valid layers: Proxy
- Applies to: HTTP proxy transactions

#### *Example*

This example enables 307 redirects for FireFox. All other browsers will see the default behavior. Note that request.header.User-Agent condition is a regex and can be used to match any particular browser.

```
<Proxy>
request.header.User-Agent="Firefox"
authenticate.force_307_redirect (yes)
```

## **Fixed in this Release**

- ❑ Blue Coat has provided a workaround in this release to a Microsoft WM server bug that impacts the use of the x-asf-packet RTSP protocol extension. The WM server bug, triggered by Rewind followed by Play actions by end users, can cause corruption of cached data.

To avoid this Microsoft bug, it's important to upgrade to SGOS 4.2.8.2. (B#95117)

- ❑ SSL Proxy now works in presence of clients and servers that are capable of using newer TLS versions (such as TLSv1.1 and TLS v1.2), newer ciphers (like camellia), and SSL-based compression. (B#94922, B#94831)

Previously, you might have had a problem in such cases with the following symptoms:

- The application did not load the page successfully. (The application could be a Web browser or the YellowDog Update Manager running on Red Hat server version 5 updating patches and going through the SSL Proxy); and
- You see any of the following errors appear in the event log
  - error:140920F8:SSL routines:SSL3\_GET\_SERVER\_HELLO:unknown cipher returned
  - error:140770FC:SSL routines:SSL23\_GET\_SERVER\_HELLO:unknown protocol
  - error:14092101:SSL routines:SSL3\_GET\_SERVER\_HELLO:unsupported compression algorithm

Table 1. Fixed in SGOS 4.2.8.2

Issue	Service Request	Description
80473	2-100983900, 2-47996708, 2-53336042, 2-67129522, 2-86465666, 2-89634622, 2-97819112	Page Fault at 0x4 in Process "CAG_Maintenance" in "tcpip.dll".
82341	2-100648981, 2-100649027, 2-102305248, 2-102305295, 2-102305390, 2-103238455, 2-53780151, 2-55023265, 2-94845371, 2-97371361, 2-97654681, 2-97819269, 2-99732778	Watchdog timeout in Process "Cache Administrator" in kernel.dll - Free_address_space_to()
83917	2-110966541	Software restart at 0xffff0001 in Process "PDW t=5470520 for=C6917400 " in "shared_dll.dll" at .tex.
86927	2-103411370, 2-112981051, 2-71417561, 2-83375553	Gigabit passthru card reverts to half duplex even when switch is set to full.
88686	2-82917412, 2-90631046, 2-90631098, 2-90631170	Page fault in Process "tcpip" in "tcpip.dll" at .text+0x1f23f.
91033	2-87963032	Hardware restart (Invalid Opcode) in Process "HTTP CW AF7A6EC0" in "" at .text+0x0.
91333	2-91882965	Software restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897 due to very frequent updates of large central policy file.
92117	2-70189502, 2-73126132, 2-95301260	BCAAA processes not being terminated.
92241	2-92185701, 2-94333751	Origin-cookie-redirect being downgraded to origin challenge with firefox and http post.
92363	2-94586508	Restart at x19 in Process "HTTP CW CC146EC0" in "Kernel.dll" at .text+0x19511.
92527	2-93600442	Policy trace does not show a match for the deny rule when explicit FTP is used.

Table 1. Fixed in SGOS 4.2.8.2 (Continued)

Issue	Service Request	Description
92583	2-93658331	Unlicensed 4.1 Permeo Agent was not working with ProxySG.
92683	2-94864233	Page fault at 0x30F45665 in Process "dns service worker FDFBBE24" in "ce_admin.dll" at .text+0x382F2.
92688	2-94596112	Page Fault in Process "tcpip" in "tcpip.dll" at .text+0x12da7.
92885	2-90651655, 2-96848582	High HTTP worker count (1082) without HTTP requests.
92886	2-91389733, 2-97658491	Yahoo-IM: In some occasions, the client got logged out instantly with the error message "body too big" in debug log.
92900	2-94848932	Software restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897.
93154	2-95341032	Page Fault 0x8 in Process "WCCP_Admin" in "wccp.dll" at .text+0x2C01.
93279	2-100740295, 2-103254112, 2-103928298, 2-104294512, 2-105600242, 2-94295354, 2-94849041, 2-95480902, 2-96032329, 2-96767968, 2-97300502, 2-97414977, 2-99407101, 2-99732422	HTTP CW count remains high with no HTTP traffic.
93310	2-86583042, 2-96156407	Software restart at 0x29 in Process "HTTP CW D7E6AEC0" in "Kernel.dll" at .text+0x96e3.
93324	2-96165341, 2-97667104	High CPU in console agent causing slow HTTP responses.
93485	2-96757682	SG reports the wrong SF categories for HTTPS URLs.
93685	2-96868052, 2-97392792	ICAP request mod: URL containing "#" is expanded by SG to %23. OCS is not expecting %23 and request fails.
93721	2-97718829	Page fault in Process "tcpip" in "tcpip.dll" at .text+0x1480A - Scatter_gather_copy when large ODC2 message (>8k) follows after the initial prompt message.
93775	2-101360738, 2-106144362, 2-96157682, 2-91913351, 2-102994252	Watchdog timeout caused by Websense database download.

Table 1. Fixed in SGOS 4.2.8.2 (Continued)

Issue	Service Request	Description
93837	2-97882765	Page Fault at 0x1E in Process "HTTP CW FD9EDF20" in "authenticator.dll" at .text+0x47563.
93902	2-93882131	The setting of TCP-RTT-USE is lost after rebooting SG.
94068	2-94882286, 2-97856012	Page Fault at 0x43E83000 in Process "HTTP SW 6598BEC0 for 648E1EC0" in "http.dll" at .text+0x5BFEB.
94090	2-93571642, 2-96759912	ProxySG generated http header names (capitalization) do not match the RFC.
94233	NONE	OPP worker count remains high even though number of TCP connections to ICAP server is low.
94300	2-98535322	Long URLs (>2K) are causing high CPU usage when using Websense database.
94387	2-101388001	Page Fault in Process "SSLW ADF04BF4" in "cfssl.dll" at .text+0x2202.
94401	2-102334181	Division fault in Process "MMS HTTP ClntW CC0D25C0" in "mms.dll" at .text+0x1f963 - startPlaying.
94418	2-102710636, 2-106659722	Watchdog timeout in Process "CAG_Worker 5" in "Kernel.dll" at .text+0x11f33.
94491	2-101642496	Page Fault in Process "tcpip" in "tcpip.dll" at .text+0x147EA (scatter_gather_copy).
94734	2-101346582, 2-103245209, 2-103441952, 2-103934822, 2-105200852, 2-105580106, 2-105580193, 2-105902557	Software restart at 0x48018 in Process "Cache Administrator" in "Kernel.dll" at .text+0xa0d6.
94748	2-97657822, 2-97693371	WLM 8.5 Buddy Lists greater than 100 do not load.
94831	2-103353520	SSL Proxy: Get error when trying to get update for Red Hat 5 Linux server: error 14092101:SSL routines:SSL3_GET_SERVER_HELLO:unsupported compression algorithm.
94896	2-104195021	Software exception in Process "PDW t=204819072 for=1A50B80 in "policy_enforcement.dll.
94942	2-103934692	Page Fault in Process "dns service worker A6289E24" in "shared_dll.dll" at .text+0x182E2.
95082	2-100701462	FTP proxy fails FTP requests that contain RCMD "<AS/400 commands>".

Table 1. Fixed in SGOS 4.2.8.2 (Continued)

Issue	Service Request	Description
95145	2-96155862	Enabling force-ntlm returns '407 Proxy Authorization Required' and missing headers when OCS authentication challenge is Basic (it works for NTLM challenge from OCS).
95176	2-105878315	Page fault at 0x8 in Process "Disk 046FA000" in "ce_admin.dll" at .text+0x4d1d0 when Avalanche load is run.
95702	2-108281826	Error=54 output in event log due to communication with BCAA.
95795	2-106880816 2-111058671 2-111322812 2-113162232 2-97414977 2-99407101	The number of open connections increases until the system cannot accept new connections.
95825	2-69914431	Gratuitous arp request made by proxy for non local address, occasionally result into traffic which should be sent to another device getting sent to proxy.

### Known Issues in this Release

- ❑ RealNetworks Helix Player version 11 cannot stream content using UDP transport when the ProxySG is deployed as a transparent proxy, using WCCP, a Layer-4 switch, or placed inline.

The player does not honor the `source` field in the RTSP `transport` header. The player always listens on the server instead of listening and accepting the UDP packets delivered from the proxy in spite of the proxy address being correctly specified in the `source` field. As a result, all UDP packets sent from the proxy to the player are dropped. This is an issue with RealNetworks, not the ProxySG. (B#95460)

- ❑ The default policy evaluation order causes the forwarding file to be evaluated out of the proper order. Note that if the Central policy file is above either the Local or VPM policies, the Forwarding file is correctly evaluated last. (B#95670, SR 2-107467097)

Table 2. Known Issues in SGOS 4.2.8.2

Issue	Service Request	Description
76739	2-41186231, 2-41834886, 2-96005082	Restart in Process "OPP_Worker C418FCB8" in "opp.dll" at .text+0x207B0.
87439	2-74894991	RTSP Content-Base header re-written to original client URL instead of header from OCS.
89117	2-84887362	Encrypted log .enc file is overwritten by .der file when using HTTP Upload client on SGOS 4.2.5.1 and SGOS 4.2.6.1.
89268	2-82276411	Certificate chaining behavior change: If keyring includes server certificate and intermediate certificate and the Certificate Authority (CA) certificate store also includes the intermediate CA public key, then the ProxySG sends two intermediate CA's.

Table 2. Known Issues in SGOS 4.2.8.2 (Continued)

Issue	Service Request	Description
90123	2-103962752, 2-88349861, 2-89646433, 2-90836132, 2-93818662	Software restart at 0x4801c in Process "Cache Administrator" in "Kernel.dll" at .text+0xa0d6.
90941	2-101216673, 2-91117002	When having compliance page (notify user policy) and the safesearch policy defined, the syslog server reports the error "Policy: Action discarded".
93307	2-96638384	3rd Generation Partnership Project (3GPP): Allow unrecognized RTSP traffic to pass through the box without modification.
93409	2-92052041, 2-95141165	Restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897 on low end platforms due to large downloads.
93778	2-97301122	Restart in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897.
93787	2-112215701, 2-97672074	Software restart at 0x40028 (CEA_INVALID_HASH_ENTRY_LINK) in Process "Cache Administrator" in "ce_admin.dll" at .text+0x3a406.
93944	2-93838816	On some occasions, redirect on HTTPS Connect is not executed when forwarding rule is present. Policy workaround available.
94067	2-101360457, 2-97664572	Restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897 due to logging issues.
94298	2-96282181	Software restart at 0x19 in Process "Idler 0" in "Kernel.dll" at .text+0x20f05.
94512	2-99199662	FTP Proxy changes 226 Response Line from OCS.
95321	2-101689301	TCP checksum for RST from SG seems incorrect.
95511	2-103876821	When using "test-url", categories "unlicensed; unavailable" are missing.
95670	2-107467097	Default policy evaluation order causes forwarding file not to be evaluated last. Note: If Central policy file is ordered above either Local or VPM, the Forwarding file is correctly evaluated last.

### Version: SGOS 4.2.7.1 build 32941

Release Date: 02/29/2008

BCAAA Version: 120

Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1

Document Revision: 1.1 on 03/05/2008

#### New in this Release

- ▣ Added support for the SSL Cavium card 1010 for the SG510, SG810, and SG8100 series.

- RTSP Log Forwarding: This feature adds support for forwarding values for several log fields. These values are reported by the ProxySG for the streaming session between the client and the ProxySG and are forwarded to the Origin Content Server (OCS) in the client log record:
  - `cs-uri-stem`: URI stem of the client request is sent in the client log record being forwarded to the server.
  - `s-pkts-sent`: Packets sent by the ProxySG to the client, during the playspurt.
  - `sc-bytes`: Bytes sent by the ProxySG to the client, during the playspurt.
  - `s-totalclients`: Number of clients connected to the ProxySG.
  - `s-proxied`: Set to 1 for proxied sessions.
  - `s-cpu-util`: CPU utilization of the ProxySG.
  - `s-session-id`: A unique id of the streaming session between client and the ProxySG.

This feature is enabled when following configuration options for the windows-media streaming proxy are set to the values specified:

- `log-forwarding`: **enable** (default is enabled). You can change this value through the:
  - Management Console: **Configuration > Proxy Settings > Windows Media** and selecting or de-selecting the **Forward client-generated logs to origin media server** checkbox.
  - CLI:  `#(config) streaming windows-media log-forwarding {enable | disable}`
- `log-compatibility`: **disable** (default is enabled). You can change this value through the CLI with the following command:

```
 #(config) streaming windows-media log-compatibility {enable | disable}
```
- Content Filtering Configurable RAM ceiling: Content filtering databases are becoming larger and can cause CPU spikes, restarts and ProxySG performance issues. If you find this is the case, you can change the amount of RAM (the ceiling) that the content filter service (CFS) is allowed to use.

You can use either the Management Console, by selecting the appropriate Memory Allocation radio button at the bottom of the **Configuration > Content Filtering > General** tab, or the CLI, by going to the (config) prompt and entering:

```
SGOS#(config) content-filter
SGOS#(config content-filter) memory-allocation ?
  high Maximize memory use for filtering
  low Minimize memory use for filtering
  normal Use the default amount of memory for filtering
```

The command causes a reload of all enabled content filter providers, with the new effective ceiling in place.

On a downgrade, memory allocation reverts to normal for the platform . The selected setting is reinstated when the device is re-upgraded.

**Important: Changing the memory allocation might have significant impacts on performance of the appliance. Be sure that the setting you choose is appropriate for the deployment.**

## Fixed in this Release

- Reverse Proxies: Blue Coat no longer use the `mms://localhost/file.wmv` syntax for caching objects. Now, upon upgrade, new client requests are cached under a name such as `mms://<host or ip>/file.wmv`, where `<host or ip>` is based on the server URL returned by policy and can be same as the client's request URL.

Objects that were previously cached under a name such as `mms://localhost/file.wmv` are not usable on an upgrade.

This optimization was only useful when (multiple) hostname or IP in the request URL would all resolve to one of the ProxySG IP addresses. (B#87537)

Table 3. Fixes for SGOS 4.2.7.1

Issue	Service Request	Description
55356	NONE	SSL Statistics: The field "Currently active sessions" under SSL Origination on the SSL/Statistics page displays an invalid counter value.
76322	2-41451941, 2-65937201, 2-69918811, 2-84114717, 2-89338012, 2-89529812, 2-90637491, 2-91124706, 2-91148740, 2-91401682, 2-91701727, 2-91838372, 2-93833332, 2-93957570, 2-93967182, 2-93967968, 2-93995473, 2-94732171, 2-94759415	"REG: File_target::create returned error 0X00000009 (9). " 0 70000:1 ../Reg_logging.cpp:119. The error is reported if the registry file cannot be opened for create.
78980	2-44184471, 2-94314731	Software error (CK_Fatal_error) code 0xFFFF registered to 'CF_KERNEL'.
85329	2-66657495, 2-69877725, 2-75734082, 2-90998542	Restart in Process "RTSP_WM_Dispatcher" in "Kernel.dll" at .text+0xA32.
86435	NONE	Services Panel does not generate delta CLI on single service change
86927	2-71417561, 2-83375553	Gigabit passthru card reverting to half duplex even when switch is set to full
87258	2-68036475	Referrer header containing authenticator cookie is being chopped with icap req mode and origin-cookie-redirect leading to http 400 response from proxy
87458	2-73500158, 2-81512124, 2-82224173, 2-85220459, 2-91039214	CPU spike and restart apparently caused by increase in Websense database size.
87609	2-76053041	Hardware watchdog timeout in CMsshd CLIworker.

Table 3. Fixes for SGOS 4.2.7.1 (Continued)

Issue	Service Request	Description
87798	2-74471201	HTTP HEAD response with no content-length header causes subsequent request on the same connection to fail.
88164	2-80180172, 2-80185632, 2-87210042	DSAT returned unexpected error: File open error.
88344	2-72585382	MC test-url does not find URL with query string in iwfbuff file.
88507	2-82863713, 2-83085692, 2-83206172, 2-83235122, 2-83706051, 2-83825744, 2-83825787, 2-83825840, 2-83825899	Unexpected restart (watchdog timeout) after running for over 497. days.
88685	2-83381799, 2-84097871, 2-90812612	In some rare occasions, the core is not being generated after tcp related page fault.
89445	2-86420851, 2-86516251, 2-87180721	Page Fault in Process "MMS File Worker 69D1B620" in "mms.dll" at .text+0x15175.
89467	NONE	Kernel faults when trying to write a core image during the initial process set.
89606	2-86602501	Resources statistics show cache available as 170% of disk use.
89629	2-82090802	Yahoo-IM: Yahoo sometimes disconnects over HTTP because of server response timeout.
89668	2-63825131	Server persistence is not working when policy is set but the global setting is off on the proxy. The policy action would only change the settings for server persistence if the connection was over HTTP.
89791	2-86775083	SGRP announcement (multicast) traffic is not processed after bringing up a gigabit interface.
89855	2-87463678	FTP does not check policy termination during upload.
89967	2-85886202	Software restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897 due to high count of SSLW (clientless workers).
90340	2-88548772, 2-92052412	ASN.1 encoding/decoding failure from Entrust when submitting CSR.

Table 3. Fixes for SGOS 4.2.7.1 (Continued)

Issue	Service Request	Description
90508	2-82099602, 2-92337021	When editing services table, the Management Console resets CLI created cipher suite. Added the "attribute cipher-suite" command to CLI for HTTPS Reverse Proxy and HTTPS Console services.
90688	2-90224712	Page Fault in Process "AOL IM Worker 75AA783C" in "im.dll" at .text+0x28d43 - Send_icbm_ack.
90692	2-83876056	When running load the access log drop down is missing items.
90751	2-90095602	MC display issue: when service name has capital letters, the combo box next to a label of icap service: is defaulted to "no service selected".
90838	2-87734602, 2-90339733, 2-91710911, 2-92356922, 2-93988401	SG rejecting server hello from gmail ("error:14092073:SSL routines:SSL3_GET_SERVER_HELLO:bad packet length").
90897	2-90392601	XML Realm: High CPU when XML authentication server is unreachable.
90929	2-69854919	Access logs showing invalid number (4294967296) bytes downloaded: sc-bytes=2^32 on random 403 responses.
91310	2-90390651, 2-93692592, 2-93840552	Page Fault at 0x1f1df4b8 in Process "tcpip" in "tcpip.dll" at .text+0x140fc.
91344	2-91909551	Page Fault in Process "Yahoo IM Worker 7381A010" in "im.dll" at .text+0x47338.
91357	2-91857271, 2-92997892 2-93833602, 2-94332062	In ICAP request mode, The ProxySG substitutes char % or ~ in URLs, with encoded characters, ie. "%25" hex value. This breaks the Web server, as the server is expecting the character, ie "%", in the URL string.
91447	2-90224686, 2-94777346	Software Restart at 0x19 in Process "Disk 03F02000" in "ce_admin.dll" at .text+0x4bc32.
91485	2-92399631	Restart in Process "HTTP CW FC7A3EC0" in "authenticator.dll" at .text+0x2211F.
91545	2-84393172, 2-90124298 2-90631046, 2-90631098 2-90631133, 2-90631170 2-94758442, 2-95472677	Page fault in Process "tcpip" in "tcpip.dll" at .text+0x14257
91782	2-93118956	In some occasions, MC GUI shows that IP forwarding is enabled when it's not.

Table 3. Fixes for SGOS 4.2.7.1 (Continued)

Issue	Service Request	Description
92175	2-93677646	CLI: bandwidth-management configuration is missing in post setup configuration. Added display of bandwidth management configuration information in "show conf post-setup" output.

## Known Issues in this Release

Table 4. Known Issues for SGOS 4.2.7.1

Issue	Service Request	Description
81835	2-52811796	Page fault at 0x3C "HTTP CW 92B27F20" in "ce_admin.dll" at .text+0x15251
83010	NONE	Without the LDAP realm in the sequence the Windows SSO realm will not correctly authorize against its LDAP realm. Adding LDAP Realm to the sequence enable Windows SSO authorization.
84783	2-64192190	ICAP X-Authenticated-User is reporting realm "unknown" for sequence realms.
84871	NONE	SG had (CK_Fatal_error) code 0x20005, registered to 'CF_SCSI_SERVER'. after downloading SG5.2 image.
85097	2-65747233	Page fault in HTTP SW C9DADEC0 for C9FF0EC0" in "http.dll"
87037	2-72604404, 2-76626252	Restart: Process "HTTP CW FE169EC0" in "transformer_dll.dll" at .text+0x8B13
87256	2-74491716	if policy decision is to "DENY" the request, socks closes the connection without sending socks reply message
87270	NONE	http.response.data test causes a denied socks transaction to succeed
87439	2-74894991	RTSP Content-Base header re-written to original client URL instead of header from OCS.
88686	2-82917412, 2-90631046, 2-90631098, 2-90631170	In some cases, the proxySG doesn't produce a full core at restart.
89117	2-84887362	Encrypted log .enc file is overwritten by .der file when using HTTP Upload client.
89268	2-82276411	CERT chaining behavior change: If keyring includes server cert and intermediate ca and ca store also includes the intermediate ca public key then sg sends two intermediate CA's.

Table 4. Known Issues for SGOS 4.2.7.1 (Continued)

Issue	Service Request	Description
90123	2-88349861, 2-89646433, 2-90836132, 2-93818662	Software restart at 0x4801c in Process "Cache Administrator" in "Kernel.dll" at .text+0xa0d6.
90941	2-91117002	When having compliance page (notify user policy) and the safesearch policy defined, the syslog server reports the error "Policy: Action discarded".
91033	2-87963032	Hardware restart (Invalid Opcode) in Process "HTTP CW AF7A6EC0" in "" at .text+0x0.
91466	2-91913351	TCP Livelock after smartfilter download and possibly higher user counts.
92117	2-73126132	BCAAA processes not being terminated.
92241	2-92185701	origin-cookie-redirect being downgraded to origin challenge with firefox and http post.
92363	2-94586508	Restart at x19 in Process "HTTP CW CC146EC0" in "Kernel.dll" at .text+0x19511.
92583	NONE	Unlicensed 4.1 PA not working with Proxy SG
92683	2-94864233	Page fault at 0x30F45665 in Process "dns service worker FDFBBE24" in "ce_admin.dll" at .text+0x382F2.

## Doc Errata

- ❑ *Configuration and Management Guide*, SSL Proxy, Intercepting HTTPS Requests to Specific Sites through VPM:

This section mistakenly says to use the Access Layer to intercept HTTPS requests. The correct procedure to intercept HTTPS requests follows.

**Procedure:** To intercept HTTPS requests to specific sites through VPM

1. Go to **Configuration > Policy > Visual Policy Manager** and launch VPM.
2. From the **Policy** drop-down menu, select **Add SSL Intercept Layer**.
3. In the **Destination** column, right-click **Set**; the **Set Destination Object** displays.
4. Click **New** and select **Server Certificate**.
5. Fill in the fields as described below. Note that you can only choose one field:

- a. **Hostname:** This is the hostname of the server whose traffic you want to intercept. After entering the hostname, use the drop-down menu to specify **Exact Match, Contains, At Beginning, At End, Domain, or Regex**.
  - b. **Subject:** This is the subject field in the server's certificate. After you enter the subject, use the drop-down menu to specify **Exact Match, Contains, At Beginning, At End, Domain, or Regex**.
- ❑ *Configuration and Management Guide, Static Bypass:*
- This section does not make it clear that static bypass lists are used only in transparent proxy environments. The local bypass list contains a list of IP addresses, subnet masks, and gateways. It can also define the default bypass gateway to be used by both the local bypass list and central bypass list. The gateways specified in the bypass list must be on the same subnet as the ProxySG.
- Used only in a transparent proxy environment, the bypass list allows the SG appliance to skip processing requests sent from specific clients to specific servers.
- ❑ *Content Policy Language (CPL) Guide:* Table C-1 indicates that range headers can be deleted. This is not the case. In this release of SGOS, range headers cannot be deleted.

## Version: SGOS 4.2.6.4, build 31840

*Release Date: 12/13/2007*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1*

*Document Revision: 1.0 on 12/13/2007*

### New in this Release

- ❑ Large downloads: Blue Coat now supports HTTP content-length headers greater than 32-bits.
- ❑ Hard disk drives 73 GB, model Seagate ST373455LC, and 300GB, model Seagate ST3300655LC, are supported on the SG810 platform.
- ❑ Instant Messaging: WLM 8.1 is now supported.
- ❑ Content Filtering, SmartFilter: During configuration from either the Management Console or the CLI, you can select the SmartFilter database edition to use: XL or SL. The XL edition is the default, and is compatible with SmartFilter 4.2 or later. There are a number of category additions and changes in the XL edition.

If you select a different database edition than was previously set, examine your policy compilation listing after the download. The set of available categories will be different, and you might need to modify the existing policy.

To select the database version, go to **Configuration > Content Filtering > SmartFilter, Database edition**, and select either the **XL** or **SL** radio button.

## Fixes in this Release

Table 5. Fixes for SGOS 4.2.6.4 Since SGOS 4.2.6.1

Issue	Service Request	Description
55642	NONE	MSN-IM: Version 7.5 - Messaging may not work when Reflection is enabled.
84779	2-64104541, 2-84629101	In certain conditions SNMP doesn't send trap when SG restarts.
86988	2-70787922	FTP upload client username and path do not allow a "\".
87586	2-77097598, 2-84730061	RTSP: Streaming stats and TCP connection stats show a steady increase of the Windows media client count (WM_RTSP workers) while the TCP connections remain fairly static, causing memory pressure to keep increasing.
87593	2-70456439, 2-72336059, 2-77146467	Software restart at 0x230000, Process "RTSP_WM_Dispatcher" in "rtsp.dll" at .text+0x63BDA. Temporary workaround: disable log-forwarding.
87806	2-80591051	Software restart at 0x19 in Process "CMsshd CliWorker" in "Kernel.dll" at .text+0x106A0.
87881	2-78652638	Management Console: After a restore-defaults factory-defaults, setting non-speed related interface settings causes speed setting to be added and applied. The "speed" CLI command is generated only when "Manually configure link settings" option is selected.
88024	2-81305482	Management Console includes "xxx-client no filename" when changing other attribute of an access log facility if the filename is "SG_%f_%l%m%d%H%M%S.log"
88075	2-76918841, 2-83794711	ISP-GW: under certain conditions, page-fault in TCP/IP when re-enabling return to sender.
88122	2-81816340, 2-82097972	The dual processor 810 models do not show/reference the second CPU in sysinfo after downgrading to 4.2.x from 5.2.x.
88227	2-72711902	WLM 8.1: On some occasions files transfers are not blocked.
88258	NONE	Streaming: After upgrading to 4.2.6.1, the default streaming format contains the field s-session-id. It should be possible to update the access log format in order to go back to the pre-upgrade format.
88446	2-81543838	POST request without Content-Length header get 411 response.
88510	2-81967157	Streaming: WMV files with multi-language audio tracks: when a language changes occurs during the stream the full file is requested.
88780	2-83739314	VPM-XML does not accurately reflect upgraded VPM-CPL policy
88948	2-72320031	LDAP authentication fails after cancelling VPM browsing.

Table 5. Fixes for SGOS 4.2.6.4 Since SGOS 4.2.6.1 (Continued)

Issue	Service Request	Description
89011	2-81816792, 2-82865702, 2-83374462, 2-84583771, 2-86041014	Certificate Signing Request (CSR) format corruption on SGOS 4.2.5.1 and later releases.

## Known Issues in this Release

Table 6. Known Issues for SGOS 4.2.6.4

Issue	Service Request	Description
85329	2-66657495, 2-69877725, 2-75734082	Restart in Process "RTSP_WM_Dispatcher" in "Kernel.dll" at .text+0xA32.
86435	NONE	Services Panel does not generate delta CLI on single service change.
86927	2-71417561, 2-83375553	Gigabit passthru card reverting to half duplex even when switch is set to full.
87037	2-72604404, 2-76626252	Restart: Process "HTTP CW FE169EC0" in "transformer_dll.dll" at .text+0x8B13.
87256	2-74491716	If policy decision is to "DENY" the request, SOCKS closes the connection without sending SOCKS reply message.
87258	2-68036475	Referrer header containing authenticator cookie is being chopped with ICAP req mode and origin-cookie-redirect leading to http 400 response from proxy.
87270	2-72794712, 2-84990885	http.response.data test causes a denied SOCKS transaction to succeed
87439	2-74894991	RTSP Content-Base header re-written to original client URL instead of header from OCS.
87458	2-73500158, 2-81512124, 2-85220459	CPU spike and restart apparently caused by increase in Websense database size.
87609	2-76053041	Hardware watchdog timeout in CMsshd CLIworker.
88164	2-80180172, 2-80185632	DSAT returned unexpected error: File open error.
88280	2-78227542	X-Virus-Id and X-Virus-Details are missing for cache hits. As a consequence, the number of viruses reported is less than number of viruses that are found.
88344	2-72585382	MC test-url does not find URL with query string in iwf buff file.
88507	2-82863713, 2-83235122, 2-83706051	Unexpected restart (watchdog timeout) after running for more than 497 days.

Table 6. Known Issues for SGOS 4.2.6.4 (Continued)

Issue	Service Request	Description
88685	2-83381799, 2-84097871	On some rare occasions, the core is not being generated after TCP-related page fault.
89117	2-84887362	Encrypted log .enc file is overwritten by .der file when using HTTP Upload client on SGOS 4.2.5.1 and SGOS 4.2.6.1.
89268	2-82276411	CERT chaining behavior change: If keyring includes server cert and intermediate ca and ca store also includes the intermediate ca public key then the ProxySG sends two intermediate CAs.
89396	2-86420851	Software restart at 0x19 in Process "MMS File Worker 721E5620" in "mms.dll" at .text+0x15227.
89404	2-82090802	Yahoo Messenger logs out after period of inactivity going through the ProxySG.

## Doc Errata

- ❑ Content Filtering (Internet Watch Foundation): The *Blue Coat ProxySG Configuration and Management Guide* does not indicate that it is optional to use a username/password when downloading the Internet Watch Foundation database. (B#89063, SR 2-83647191).
- ❑ CRLs: The *Blue Coat ProxySG Command Line Reference* does not list proper syntax for the edit CRL list name. The proper syntax is (B#42866):

```
SGOS#(config ssl crl crl_list_name)
option 1: exit
option 2: inline
option 3: load
option 4: path
option 5: view
```

## Version: SGOS 4.2.6.1, build 31079

*Release Date: 10/23/2007*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1*

*Document Revision: 1.1 on 10/29/2007*

## New in this Release

- ❑ Streaming Access Logging: The default access logging format has been changed to support the `s-session-id`. This field logs the session identifier the SG appliance uses to track a streaming session. This is important for tracking multiple log entries to the same session. For more information about access logging formats, refer to *Blue Coat ProxySG Configuration and Management Guide*.
- ❑ Hardware: A new SSL accelerator card is now shipping with SG210 systems.

- SmartFilter: SGOS 4.2.6 now downloads and uses the SmartFilter "XL" database. This version of the database contains a number of additional categories that can be used in policy. For more details about the database, including descriptions of the new categories, please visit:

<http://www.securecomputing.com/filteringdb.cfm?db=XL>

The SmartFilter database previously in use cannot be incrementally upgraded to the "XL" database. The first SmartFilter download after you upgrade to SGOS 4.2.6 fetches the full database (approximately 200Mb). Subsequent downloads are incremental as usual. This process is automatic and requires no user intervention.

## Fixes in this Release

Table 7. Fixes in this Release Since SGOS 4.2.5.1

Issue	Service Request	Description
78844	2-44405695	Management Console: doesn't accept a preview size value of 0 once set to a non 0 value.
64277	NONE	AOL 5.1 : Japanese characters not being recognized by the SG for IM File Transfer traffic.
81003	2-51338368	Changing core settings deletes restart entry in Core_image page.
83818	2-60244221	Page fault at 004BA8B6 in MMS File Worker FBC9C640" in "mms.dll" at .text+0x178B6.
84779	2-64104541	In certain conditions SNMP doesn't send trap when SG restarts.
85094	2-65123331	Restart in Process "DNS Service worker" in "ce_admin.dll" at .text+0x38072.
85551	2-66257633	Novell SSO: Delay needed after logon/logout event before querying edirectory.
85581	2-61959911	Double interface bandwidth shown on 8000-x.
85601	2-65572781	Management Console advanced URL links do not work with IE.
85602	2-67236276	Restart in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897.
85721	2-64103801	Siteminder sharing of credentials during a user request causes an authentication loop.
85848	2-68075716	SSL: Disabled SSL service still activates TCP listener for the specified port.
85960	2-65747111	Wrong disposition for category 153 when sending logs to Websense reporter.
85967	2-69720101	Invalid response to PWD by FTP server causes connection to fail
86003	NONE	Siteminder 6: Off box redirects do not work.

Table 7. Fixes in this Release Since SGOS 4.2.5.1 (Continued)

Issue	Service Request	Description
86034	NONE	Cross-site scripting (XSS) vulnerability in the handling of the URL that loads Certificate Revocation Lists into the appliance via the management console. If the URL is malformed in certain ways, the malformed text is treated as HTML and displayed to the user, instead of an error message being generated. A workaround is for administrators to never visit any untrusted site while logged into the ProxySG management console.
86052	NONE	Switch to the SmartFilter XL database, which has 91 categories (the full set).
86124	NONE	Timezones: machines upgraded to timezone-supporting versions can not be persistently set to UTC.
86164	NONE	Add support in SG for launching VPM independently of MC in Director.
86247	2-70249062	RIP: gateway error on install of rip config due to "trust_gateway" parameter.
86258	2-70456207	RIP: passwd in rip config is not working as expected
86307	2-70249682	Hardware restart at 0xE in Process "MSN IM Worker 1934E7CC" in "im.dll" at .text+0x2B011.
86330	2-69166231	Hardware restart in Process "MSN IM Worker 174F4B30" in "im.dll" at .text+0x37A64.
86353	2-70776242, 2-71421279	FTP Proxy: RNT0 command not being passed through causing SG to send "530 access denied".
86359	2-70891902	Page Fault at 0x3C in Process "HTTP RW C3EF9EC0" in "ce_admin.dll" at .text+0xD95.
86368	2-70324472	Retransmission packets are sent to default gateway when inbound return-to-sender is enabled.
86369	2-70710181, 2-70874552, 2-71394303, 2-71993519	ICAP: URL encoding issue with certain characters breaking REQMOD and RESPMOD.
86417	2-71529042	RIP: rip routes for an interface that is down do not get removed from the ip route table.
86556	2-71519791, 2-73158122, 2-74815572	Page fault in Process "tcpip" in "tcpip.dll" at .text+0x14247
86583	2-71342234, 2-71544102	Page Fault 0xE in Page Fault Process "HTTP CW C7921EC0" in "http.dll" at .text+0x2B913.
86656	NONE	SG 810: restart code 0x4801F, registered to 'CF_CACHE_ADMIN'
86680	2-71993403	SG Responds 200 OK to invalid range RTSP request

Table 7. Fixes in this Release Since SGOS 4.2.5.1 (Continued)

Issue	Service Request	Description
86857	2-69720691	FIXED: Daylight Savings Time extension needed for New Zealand
86788	2-72611221	Novell SSO: Workstation Logins are masking User Logins.
86976	NONE	WM-RTSP: Access log entries corruption.
86981	2-72369352	Windows SSO authorization fail when moving user to a different container
87005	2-69930343	SG sends CWD command for FTP upload even though path is empty
87026	2-72896981	WM-RTSP: Extra '/' is added into SETUP request when "a=control:" SDP attribute has trailing '/'.
87123	2-73573497	Occasional high CPU is seen with little traffic.
87137	2-72479455	After restore-defaults, the full SmartFilter database download is needed to use already downloaded categories
87146	2-72342665	BCAAA agent unexpectedly closes connection with ProxySG on port 16101 and stops with event id 1403.
87192	2-74324166	DNS service admin appears to not process some requests.
87221	2-74826685, 2-74826699	Page fault in MMS File Worker CD7DC240" in "mms.dll" at .text+0x17ca7.
87246	2-73080292	Page fault in IM_Admin" in "im.dll" at .text+0x4401.
87493	2-76214945	<p>Occasional slowness under load due to MMS Admin doing blocking DNS lookups on server urls returned by policy, in order to create a url of the form mms://localhost/file.wmv if the hostname/IP in the server url resolved to one of SG's local IPs.</p> <p>Reverse proxy limitation: The ProxySG no longer uses the mms://localhost/file.wmv syntax for caching objects. This optimization was only useful on reverse proxies, when (multiple) hostname or IP address in the request URL would all resolve to one of the ProxySG appliance's IP addresses.</p> <p>On upgrade, previously cached objects under a name such as mms://localhost/file.wmv are not usable. New client requests that would have previously used the cached copy now cause the appliance to fetch file.wmv and cache it under a name such as mms://host_or_ip&gt;/file.wmv, where host or ip is based on the server URL returned by policy; it might be the same as the client's request URL.</p>

## Known Issues in this Release

Table 8. Known Issues in this Release

Issue	Service Request	Description
58663	NONE	Policy: Delete action doesn't work on request.header.Range.
76322	2-41451941, 2-65937201, 2-69918811	"REG: File_target::create returned error 0X00000009 (9). " 070000:1 ../Reg_logging.cpp:119. The error is reported if the registry file cannot be opened for create.
80473	2-47996708, 2-53336042, 2-67129522	Page fault HeC:0xe,SeC:0x0,PFLA:0x4,PFE:0x0,Process "CAG_Maintenance" in "tcpip.dll"
84783	2-64192190	ICAP X-Authenticated-User is reporting realm "unknown" for sequence realms.
84871	NONE	SG had (CK_Fatal_error) code 0x20005, registered to 'CF_SCSI_SERVER'. after downloading SG5.2 image.
85097	2-65747233	Page fault in HTTP SW C9DADEC0 for C9FF0EC0" in "http.dll"
85329	2-66657495, 2-69877725, 2-75734082	Restart in Process "RTSP_WM_Dispatcher" in "Kernel.dll" at .text+0xA32.
85668	NONE	Page fault at 0x4B8 in Process "RTSP_CDN_Client" in "rtsp.dll" at .text+0xBB18 while doing content pre-population.
86135	2-70458020	SG dropping packets outgoing and ignoring incoming packets.
86435	NONE	Services Panel does not generate delta CLI on single service change
86611	2-70456439, 2-72336059	Restart in process "RTSP_WM_Dispatcher" in "rtsp.dll" at .text+0x62F60
86927	2-71417561	Gigabit passthru card reverting to half duplex even when switch is set to full duplex.
86988	2-70787922	FTP upload client username and path do not allow a "\"
87005	2-69930343	SG sends CWD command for FTP upload even though path is empty
87037	2-72604404	Restart: Process "HTTP CW FE169EC0" in "transformer_dll.dll" at .text+0x8B13
87146	2-72342665	BCAAA crashing with event id 1403 in Novell SSO realm.
87246	2-73080292	page fault in IM_Admin" in "im.dll" at .text+0x4401
87256	2-74491716	If policy decision is to "DENY" the request, socks closes the connection without sending socks reply message.
87258	2-68036475	Referrer header containing authenticator cookie is being chopped with icap req mode and origin-cookie-redirect leading to http 400 response from proxy.

Table 8. Known Issues in this Release (Continued)

Issue	Service Request	Description
87270	2-72794712	http.response.data test causes a denied socks
87418	2-75683445	Hardware restart at 0x19 in Process "MMS Administrator" in "mms.dll" at .text+0x2e47.
87439	2-74894991	RTSP Content-Base header re-written to original client URL instead of header from OCS.
87458	2-73500158	CPU spike and restart apparently caused by increase in Websense database size.
87593	2-77146467	Software restart at 0x230000, Process "RTSP_WM_Dispatcher" in "rtsp.dll" at .text+0x63BDA. Temporary workaround: disable log-forwarding.

## Version: SGOS 4.2.5.1, build 29951

Release Date: 8/15/2007

BCAAA Version: 120

Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.3.1, ProxyAV 3.1

Document Revision: 1.2 on 08/20/2007

### New in this Release

- ❑ The SG210 platform is supported.
- ❑ Yahoo 8.1 is supported.
- ❑ The following CPL conditions are now supported in the <forwarding> layer:
  - request.header.header\_name
  - request.header.header\_name.count
  - request.header.header\_name.length
  - client.host.has\_name
- ❑ The Blue Coat Reporter Client is available as an access log custom client. Designed for the Reporter administrator, the custom client improves the reliability of the communication channel.

You can access and edit the client by going to the **Management Console > Access Logging > Logs > Upload Client**, and selecting Bluecoat Reporter Client from the **Client type** drop-down list.

CLI Syntax:

```
SG#(config) access-log
SG#(config access-log) edit log main
SG#(config log main) bluecoat-client {alternate hostname [port] | no
{alternate | primary}| primary hostname [port]}
```

### Fixes in this Release

- ❑ Fixed OpenSSL vulnerability VU#724968

- ❑ In certain cases, DNS lookups were not occurring, but rather being blocked forever. HTTP requests attempting DNS lookup would similarly become blocked, ultimately exhausting the SG Appliance's HTTP proxy service (B#82706, 2-53711556, 2-56416061)
- ❑ Under certain conditions, the `content revalidate` CLI command deletes objects when retrieval is interrupted. (B#83185, 2-51769421)

Table 9. Changes for SG 4.2.5.1 since SG 4.2.4.1, Limited to milestone SG 4.2.5

Issue	Service Requests	Description
61411	2-24323961, 2-28640147, 2-40723116, 2-42220333	MMS via http does not handle 302 HTTP responses correctly.
62218	NONE	MC: Service Ports New/Edit Dialog has graphic corruption when navigating through proxies using up/down keys.
64873	2-29880838	Stream does not play when going to this site <a href="http://www.ndr2.de/pages_special_lib/0,,SPM7454_CONndr2_TYPreal_LOCint,00.html">http://www.ndr2.de/pages_special_lib/0,,SPM7454_CONndr2_TYPreal_LOCint,00.html</a> due to format in new Helix players.
75656	2-40719281, 2-62296041	Page fault in "TCPIP_stats_server" in "Kernel.dll" at .text+0x1127 while printing TCP conn table.
76237	2-29982820	Gig interface does not re-establish link after being disconnected for 90 minutes.
76709	2-41483546	Specific order of executing deletion of failover group and VIP as batch apply/commit causes errors.
77862	2-42391570	Page Fault in "CE's DNS Service" in "ce_admin.dll" at .text+0x34536 - Initialize@CEA_DNS_Entry.
77988	2-43312459	MSN 7.5 hangs at login when using HTTP explicit proxy.
78844	2-44405695	SG doesn't accept Preview size value 0 once user set non 0 value on GUI
78874	2-44654501, 2-61961443, 2-62169745, 2-62965198, 2-63003271, 2-63516011, 2-64231201, 2-64941181, 2-65352951, 2-65687463, 2-66214603	ICAP Respmoed adds "25" to %20 for URLs containing spaces.
79107	2-45583421	CLI and MC: issue creating an ICAP req mode Service containing "?".
79760	2-42419595	Using a certificate with an umlaut prevents new certificates from being created.
79849	2-45236672	Surfcontrol log has the same timestamp at the beginning and at the end in the logs.

Table 9. Changes for SG 4.2.5.1 since SG 4.2.4.1, Limited to milestone SG 4.2.5 (Continued)

Issue	Service Requests	Description
79899	2-43922811, 2-65352891, 2-65733091	Software restart at 0x19, in Process "Cache Administrator" in "ce_admin.dll" at .text+0x3d300.
80226	2-46407415	Proxy doesn't use server side persistent connection when reflect_ip is configured.
80297	SR#2-45411515	MSN IM can't transfer file.
80592	2-48411928, 2-63605603	RSTP: Page Fault at 0xFC in RTSP_WM_Client" in "rtsp.dll" at .text+0x47032.
80791	2-42223071	Unchunk compressed response fails when the response data is separated from the header packet.
80871	2-44030453, 2-52090001, 2-61744133	Padding error when connect using SSH to SG.
81702	2-48167834, 2-61401061	In certain conditions, accepted-NotifyUser1 Notify URLs is leaked to the OCS.
81758	2-53120076	The Proxy restarts when the netbios responder is disabled.
81950	2-53334221, 2-60132606	When OCS sends 0 byte chunk immediately after the end of 200 ok response and if the ICAP service is enabled, SG doesn't send 0 byte chunk or last chunk to the client.
82002	2-61182821	Hardware restart at 0xe in Process "tcpip" in "tcpip.dll" at .text+0x96F0
82008	2-53779501	Local user-list not deletable after restore-defaults.
82073	2-53797481	Kerberos credentials configuration in IWA realm is not shown in "show configuration".
82473	2-62278641, 2-64923381	Sequence Realms With Policy Substitution fall back.
82505	2-53339751	The agent address in SNMP trap is different from the source-ip of the trap.
82666	2-55753799	Page Fault at 0xdfc6ff0 in Process "LDAP Worker" in "tcpip.dll" at .text+0x10fd9.
82737	2-54486262	IM Proxy increases content-length when receiving extra bytes from client.
82887	2-55738061, 2-57291481, 2-64675371	Watchdog timeouts caused by large number of "time=" policy re-evaluation.
83059	2-55748680	MC Maintenance > Licensing > View: It is unclear when trial component is disabled.
83208	2-54773895, 2-59511735, 2-59580118, 2-59580201	Restart at Process "Idler 0" in "Kernel.dll" at .text+0x20ED5.

Table 9. Changes for SG 4.2.5.1 since SG 4.2.4.1, Limited to milestone SG 4.2.5 (Continued)

Issue	Service Requests	Description
83241	2-54527505	In upload FTP client, "Error encountered while committing changes to the proxySG" prompt when password starts with an "!".
83358	2-58949931	Proxy sends 503 responses to the client when persistent connections are closed.
83533	2-59407211	Page Fault at 0x70656363 in Process "Agent-Admin-coreid_www2_form_de" in "authenticator.dll" at .text+0x30E0E.
83575	2-59605290, 2-60244061, 2-61204641, 2-62321671	SG reports high worker count and high CPU when using Smartfilter.
83673	2-57488701	BCAAA Solaris: SG closes connection to BCAA when authenticating a user.
83717	2-60666821	SG sends out ARP request instead of forwarding to default gateway when destination IP is in bypass list in WCCP setup.
83899	2-60595744, 2-63798611	Software restart at 0x5B0000 in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897.
83900	2-60966901	Client Negotiated and Server Negotiated objects cannot be negated in VPM.
83981	2-58429256	In rare occasions, the BCAA faults (memory exception: 0xc0000005).
84009	2-59770981	Specific IPs on client and SG VIP cause TCP checksum errors.
84024	2-61804941	Software restart at 0xFFFF0001 in Process "PDW t=157424186 for=10D8380 " in "transactions.dll".
84152	2-62321031	FTP through HTTP proxy ignores reflect_ip(vip) policy.
84158	2-61960283	IM: MSG messages larger than 4096 bytes are not supported.
84311	2-62146651	SSH deadlock with high volume sessions.
84424	2-57126527, 2-63829151	Category objects can't be renamed in VPM.
84506	2-64186439	Certification with wildcard domain *.telindus.com fails with certification domain invalid.
84575	2-62722281	In transparent deployments, if packets are redirected to SG by a layer 4 switch, IP fragments get dropped.
84649	2-61537566	Primary weight configuration only works on interface 0:0.

Table 9. Changes for SG 4.2.5.1 since SG 4.2.4.1, Limited to milestone SG 4.2.5 (Continued)

Issue	Service Requests	Description
84712	2-64386380	Proxy SG strips off the response headers when OCS sends http/1.02 version.
84777	2-64943721	Time object and "only between the following times of day" changes to "00:00".
84868	2-64086501	Page fault in Process "CLI_Worker_1" in "registry.dll" at .text+0x1643F when deleting a local realm.
84873	2-65116383	If an empty alt-text statement is defined within an html image tag in a Notify-User definition, the 2nd quote mark is moved to after the closing bracket of the tag.
84883	2-65355291	Restart in Process "AOL IM Worker 84EB83C" in "im.dll" at .text+0x11be5.
84946	2-65437475	Software restart at 0x230000 in Process "RTSP_Recorder" in "rtsp.dll" at .text+0x1F0EE.
84962	2-65256120	Watchdog timer expired on reboot after running heavy load.
84976	2-65794651, 2-66452914	Seeing hardware registration page even though the hardware is registered.
85105	2-61034391	MC Display issue - Licensing page is unreadable if browser window is resized too small.
85377	2-65572621	DNS Proxy intermittently not responding to DNS request.
85549	2-64862223	The network adapter LED color is not shown on Web Console.
85603	2-66671506	XML Realm can not be deleted if unresolvable URL entered for Primary & Alternate responders.
85728	2-66349421	WM-RTSP: "a=control:" SDP attribute is not properly rewritten when the url path has a trailing '/'.

## Known Issues in this Release

Table 10. Known Issues for SGOS 4.2.5.1

Issue	Service Request	Description
84458	2-62287610	Restart in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897.
84779	2-64104541	In certain conditions SNMP doesn't send trap when SG restart.
84783	2-64192190	ICAP X-Authenticated-User is reporting realm "unknown" for sequence realms.

Table 10. Known Issues for SGOS 4.2.5.1 (Continued)

Issue	Service Request	Description
84815	2-64217521	SSL proxy: Connect request to port 8613 returns 200 ok with specific policy instead of 403.
85094	2-65123331	Restart in Process "DNS Service worker" in "ce_admin.dll" at .text+0x38072.
85329	2-66657495	Restart in Process "RTSP_WM_Dispatcher" in "Kernel.dll" at .text+0xA32.
85601	2-65572781	Management Console advanced URL links do not work with IE.
85721	2-64103801	Siteminder sharing of credentials during a user request loop.

### Version: SGOS 4.2.4.1, build 29063

Release Date: 5/21/2007

BCAAA Version: 120

Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2 and Reporter 8.3.1, ProxyAV 2.4 or ProxyAV 2.5

Document Revision: 1.12 on 05/21/2007

#### New Features in this Release

- ❑ Two new hard drives—80GB model SEAGATE ST380215A-3.AAC and 250GB model SEAGATE ST3250820A-3.AAE—are supported on the 200 platform.
- ❑ Vista support.
- ❑ “XML Realms” on page 48.
- ❑ MSN/Windows Live Messenger supports HTTP explicit proxy authentication. Note that the SG appliance must be configured to use HTTP ProxyAuth code 407, not HTTP auth code 401.
- ❑ The Management Console behavior for enabling or disabling the trial period has changed. Now, if the trial period is enabled and you click **Maintenance > Licensing > View**, the Management Console displays a check box to disable the trial period. If the trial period is disabled, the Management Console displays a check box to enable the trial period.

#### Fixed in this Release

- ❑ Open SSH security vulnerability (SA22091)

Table 11. Fixes in SG 4.2.4.1 since SG 4.2.3.26

Issue	Service Request	Description
54041	2-29385111, 2-40673545, 2-41925015, 2-45114850, 2-50877469, 2-51209059, 2-57161599	In some conditions, the proxy closes the server side connection abruptly.
64604	2-22626101	SGRP packets are not being sent on the correct interface.

Table 11. Fixes in SG 4.2.4.1 since SG 4.2.3.26 (Continued)

Issue	Service Request	Description
65022	2-41319326, 2-41647529, 2-43986259	WCCP interface setting: "sho wccp config" does not reflect correct settings.
77553	2-42892256, 2-43291481, 2-47601911, 2-48162031, 2-48332918, 2-48577190, 2-51354572, 2-52086872, 2-53333421	Getting HTTP 500 errors for certain URLs when performing ICAP Respmod.
78145	2-44243521, 2-51653181	Notify User - Compliance page does not show authenticated username.
78746	2-43629103	In some rare occasions, the proxy closes the connection when the client has not sent all data.
80166	2-47044731, 2-48165121, 2-50824423	Yahoo IM: Page Fault at 0x2 in "tcpip.dll" at .text+0x129AB.
80355	2-47031521, 2-47166591	Page fault at 0x44 Process "CLI_Worker_2" in "registry.dll" at .text+0x1642F when deleting sequence realm.
80637	2-47409170	MC: Cannot create more than 100 services.
81011	2-44015441	Page fault at 0xC3CCB824 n "MSN IM Worker 4E3AE374" in "shared_dll.dll" at .text+0x12E73 - _Internal_write().
81759	2-53011334	DOC: Incorrect example on page 517 of 4.2.3 CMG (replaced 'proxy' with 'cache').
82059	2-53676686	Page fault at 0x1E0 in Process "RSTP_WM_Dispatcher" in "rtsp.dll" at .text+0x4B174.
82091	2-53867755, 2-54773823, 2-57806712	Page fault in Process "DNS Service worker" in "tcpip.dll" - dn_skipname().

## Known issues in this Release

See the following table for information on known issues.

Table 12. Known issues for SG 4.2.4.1

Issue	Service Request	Description
77862	2-42391570	Page fault in "CE's DNS Service" in "ce_admin.dll" at .text+0x34536 - Initialize@CEA_DNS_Entry.
78844	2-44405695	MC: does not accept a preview size value of 0 once set to a non 0 value.
78874	2-44654501	ICAP Respmod adds "25" to %20 for URLs containing spaces.

Table 12. Known issues for SG 4.2.4.1 (Continued)

Issue	Service Request	Description
80592	2-48411928	RSTP: Page fault at 0xFC in RTSP_WM_Client" in "rtsp.dll" at .text+0x47032.
81758	2-53120076	The proxy restarts when the netbios responder is disabled.
81759	2-53011334	DOC: Incorrect example on page 517 of 4.2.3 CMG (replaced 'proxy' with 'cached').
82008	2-53779501	Local user-list not removable after restore-defaults.
83185	2-51769421	In some cases and under certain conditions, the content revalidate command deletes objects when retrieval is interrupted.
83208	2-54773895	Restart at Process "Idler 0" in "Kernel.dll" at .text+0x20ED5.
83358	2-58949931	Proxy sends 503 responses to the client when persistent connections are closed.

### Version: SGOS 4.2.3.26, build 28839

Release Date: 4/23/2007

BCAAA Version: 120

Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2, ProxyAV 2.4 or ProxyAV 2.5

Document Revision: 1.11 on 04/20/2007

#### Fixed in this Release

- ❑ Fixed a known issue that may occur under certain conditions where an SG appliance with AV configured, with the system under high load and experiencing client to SG network disconnects, with either bandwidth gain enabled or a high proportion of non-cacheable objects, the SG may restart or hang with the SG unable to transfer data to the AV.
- ❑ WM-RTSP: Bad Request responses for streaming requests due to the modification of the "a=control" attribute in the RTSP response (B#81666, SR 2-48931681, SR2-50624468, SR2-54103181).
- ❑ If you're getting HTTP 500 errors for certain URLs when doing ICAP Respmod, you must reinitialize the SG appliance drives. Back up the system configuration before proceeding. (B#77553 SR 2-42892256, 2-43291481, 2-47601911, 2-48162031, 2-48332918, 2-48577190, 2-51354572, 2-52086872, 2-53333421)

#### Limitations

For a list of limitations with SGOS 4.2.3.x, see "[Section B: Limitations](#)" on page 56.

## Version: SGOS 4.2.3.21, build 28657

Release Date: 3/29/2007

BCAAA Version: 120

Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2, ProxyAV 2.4 or ProxyAV 2.5

Document Revision: 1.10 on 03/26/2007

### New in this Release

- Streaming-Speed Pre-population. SGOS 4.2.3.x supports Windows Media (WM) RTSP streaming, including live splitting and VoD caching. With SGOS 4.2.3.20, Blue Coat adds support for using RTSP to pre-populate WM streaming files from origin WM servers. This allows later RTSP requests from WM clients for the pre-populated content to be served from the cache as long as the file does not change on the origin WM server.

The existing content CLI command set for content pre-population is also used for WM pre-population. Use appropriate `rtsp:// url` to specify the content to be cached. For example:

```
# (config) content distribute rtsp://domain.com/file.wmv.wmv
```

### Limitations

- Pre-population of WM streaming files from HTTP web servers is not yet supported.
- Pre-population of authenticated content is not supported.

### Fixes in this Release

---

**Note:** Because of fixes to the BCAA service, Blue Coat recommends that you upgrade to the latest version of BCAA.

---

Table 13. Changes Since SGOS 4.2.3.12

Issue	Service Request	Description
59694	2-41723362	BCAAA: Failure to spawn connection child terminates parent listener
60810	2-26278610, 2-39850120, 2-41663382	Page Fault in "tcpip" in "tcpip.dll" at .text+0x14A8A - Scatter_gather_copy().
61832	2-27573631, 2-30875653, 2-42809161, 2-44453421, 2-45812481	ProxySG goes into acceptance regulation due to leakage of transactions when using Yahoo IM.
63621	2-30763523	Software restart at 0x4001C in Process "HTTP CW EE9D2F20" in "ce_admin.dll" at .text+0xAB2.
64756	2-38946121, 2-41631071, 2-41684897	BCAAA sporadically restarts when using Novell SSO.
64920	NONE	MC-IE7.0: in Statistics-->Advanced page second Java pop up asking for username and password.

Table 13. Changes Since SGOS 4.2.3.12 (Continued)

Issue	Service Request	Description
65077	2-40154607	ProxySG does not send 307 for origin redirect for IE7.
75830	NONE	Delay installing VPM under load when "time" under web access layer is selected.
75934	2-40824681	Data retransmitted after connection with client already closed.
76185	2-47471888	810 Internal nics sometimes get corrupted data.
76520	2-41639451	Problems logging on to msn 7.5 when pac file configured to be served from a vip.
76523	2-41257009	notify-NotifiedUser cookie is sent to the OCS along with the request.
76678	2-30315287, 2-30325015	Authentication cookie not being set when ICAP reqmod is processed.
76693	2-30010071	Site can't be accessed after hex-encoded strings are decoded.
76920	2-38633231	Restart in Process "HTTP CW C4B2AF20" in "cfssl.dll" at .text+0x1F3CD
77622	2-42696481	Page Fault in Cag_worker in "shared_dll.dll" at .text+0x5D1B when uploading system image.
77649	2-42779391, 2-43632041, 2-43632605	snmp get for ifnumber.0 only returns 1 interface.
77681	2-42419581, 2-43162349, 2-43220623, 2-43414074, 2-44655841, 2-44970450, 2-45133211, 2-46190771, 2-47326320, 2-48206615, 2-48326750, 2-48339871, 2-48463781, 2-48471891, 2-48902531, 2-48902861	Software restart in Process "Threshold_Monitor" in "Threshold_monitor.dll" at .text+0x897 - due to Cache Block leakage.
77903	2-42696621	Page Fault at 0x492791A0 - "DNS Service worker" in "Kernel.dll" at .text+0x4590.
77904	NONE	HTTP proxy drops "WWW-Authenticate: Negotiate" in an HTTP response when OCS requires Kerberos authentication.
77937	2-41761670, 2-43365531, 2-44099571, 2-44120532, 2-46770581, 2-47072494	Page Fault in "tcpip" in "" at .text+0x0 - rtalloc1().
77996	2-42424921	Page fault at 0x1472C000 in Process "Policy Import Worker - AFL" in "shared_dll.dll" at .text+0x1EEA7 (policy enforcement).
78037	2-43483977	VPM: Individual LDAP realms cannot be selected in "Add Attribute Object".

Table 13. Changes Since SGOS 4.2.3.12 (Continued)

Issue	Service Request	Description
78350	2-42425828	BCAAA : software exception at c0000005 after upgrading to 4.2.3.4.
78569	NONE	Page fault due to malformed DNS query over TCP .
78599	2-43922321	Server-side keep-alive (OPTIONS *) packet causes the proxy to stop serving traffic to the client.
79183	2-45450651, 2-45529848, 2-45829171, 2-46133943, 2-47468207, 2-48165041	MC unresponsive due to problems opening object.
79204	2-48314240	Page fault at add_host@af_neighbour_manager in af_neighbours.cpp.
79710	2-45413286	PF in Process "Yahoo IM Worker 95C993A0" in "im.dll" - Remove_active_session_id()
80259	2-40375564, 2-44184345, 2-46921446	Page fault at 0x5 in Process "tcpip" in "tcpip.dll" at .text+0x60E2A .
80340	2-46647694, 2-46648861, 2-46859481, 2-47749131, 2-47996751, 2-48007528	Software restart at 0x19 in Process "SCSI Disk 6712:0:6" in "Kernel.dll" at .text+0xdec1.
80545	2-47124655	"Show Me" button in SG4 Maintenance -> Upgrade page point to SG5 download site.
80810	2-48745999	SG8100 hangs with certain interface configuration and SNMP enabled.
80870	2-48914082	Hardware restart in Process "MSN IM Worker 8A104A3C" in "im.dll" at .text+0x3BC07.

### Known Issues in this Release

A known issue may occur under certain conditions where an SG appliance with AV configured, with the system under high load and experiencing client to SG network disconnects, with either bandwidth gain enabled or a high proportion of non-cacheable objects, the SG may restart or hang with the SG unable to transfer data to the AV. This issue is fixed in SG 4.2.3.26.

Table 14. Known Issues

Issue	Service Request	Description
76097	2-29385111, 2-40673545, 2-41925015, 2-45114850	Software restart at 0x19 in "HTTP CW" in "Kernel.dll" at .text+0x925C.
76707	2-40684441	Purge-dns-cache not reflected in CE/DNS/Info/URLs.
76739	2-41186231, 2-41834886	Page Fault in Process "OPP_Worker C418FCB8" in "opp.dll" at .text+0x207B0.
77553	2-42892256, 2-43291481, 2-48162031, 2-48332918	Getting HTTP 500 errors for certain URLs when performing ICAP RespmoD.

Table 14. Known Issues (Continued)

77862	2-42391570	Page Fault in "CE's DNS Service" in "ce_admin.dll" at .text+0x34536 - Initialize@CEA_DNS_Entry.
78145	2-44243521	Notify User - Compliance page does not show authenticated username.
78844	2-44405695	MC: doesn't accept a preview size value of 0 once set to a non 0 value.
78874	2-44654501	ICAP Respmo adds "25" to %20 for URLs containing spaces.
79404	2-44961061	When enabling RESPMOD, cached JPG files are not refreshed when a PNC header is received.
79849	2-45236672	Surfcontrol log has the same timestamp at the beginning and at the end in the logs.
80166	2-47044731	Yahoo IM: Page Fault at 0x2 in "tcpip.dll" at .text+0x129AB.
80226	2-46407415	Proxy doesn't use server side persistent connection when reflect_ip is configured.
80480	2-47393631	Software restart at 0x19 MMS File Worker" in "mms.dll" at .text+0x177ed -- Unblock_clients_on_error().
80637	2-47409170	MC: Cannot create more than 100 Services.
80724	2-47031521	Cannot clear/remove realm in sequence realm after upgraded to SGOS 4.2.3.
80789	2-48165121	Yahoo IM Page Fault at 0x50 in Process "tcpip" in "tcpip.dll" at text+0x12a4a
80791	2-42223071	Unchunk compressed response fails when the response data is separated from the header packet.
80871	2-44030453	Padding error when connect using SSH to SG.
61411	2-24323961, 2-28640147, 2-40723116, 2-42220333	MMS via HTTP does not handle 302 HTTP responses correctly.
64873	2-29880838	Stream does not play when going to this site http://www.ndr2.de/pages_special_lib/0,,SPM7454_CONndr2_TYPreal_LOCint,00.html
65022	2-41319326, 2-43986259	"show wccp config" does not reflect correct settings.
75656	2-40719281	Page fault in "TCPIP_stats_server" in "Kernel.dll" at .text+0x1127 while printing TCP conn table.
76237	2-29982820	Gig interface does not re-establish link after being disconnected for 90 minutes.
76709	2-41483546	Specific order of executing deletion of failover group and VIP as batch apply/commit causes errors.

Table 14. Known Issues (Continued)

79899	2-43922811	Software restart at 0x19, in Process "Cache Administrator" in "ce_admin.dll" at .text+0x3d300.
-------	------------	--

## Doc Errata in this Release

### *Configuration and Management Guide*

SNMP Traps: The documentation states that failed attempts to login to the SG appliance are logged. In actuality, this trap is used with SNMPv2 only when an SNMP packet is received with an invalid community name. (B#79575, 2-42751311)

### *Content Policy Language Guide and Configuration Management Guide*

IM: Policy condition `im_method=` indicates it has values of `send_unknown` and `receive_unknown`. This is incorrect. The values are `unknown_send` and `unknown_receive`. (B#79863)

## Version: SGOS 4.2.3.12, build 28131

*Release Date: 2/08/2007*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2, ProxyAV 2.4 or ProxyAV 2.5*

*Document Revision: 1.09 on 02/08/2007*

## New in this Release

- ❑ Daylight Savings Time change (DST). The appliance software has been modified to include new rules for DST. Additionally, all timestamps, which are recorded in Coordinated Universal Time (UTC), are processed differently so that local time displays correctly. The Management Console has been modified to include a more comprehensive time zone selection. To enable flexibility, time zone selection can be associated with an open source time zone database that can be updated at your discretion. The time zone database is not required to set the appliance to UTC.

## Fixes in this Release

- ❑ Blue Coat appliance is hanging due to registry write lock (B#64009, 2-29712361).
- ❑ Restart in Process MSN IM Worker 5D678374 in `im.dll` at `.text+0x2AF71` (B#75691, 2-40189417, 2-40606401, 2-41134166, 2-41301688, 2-41445974, 2-42530691).
- ❑ Page Fault in "IM\_Admin" in "im.dll" at `.text+0x4451` (#75904, 2-40836381).
- ❑ Page Fault in Process in "AOL IM Worker 13CF8DC0" in "im.dll" at `.text+0x226E7` (B#76168, 2-41448021, 2-41448401, 2-42121041).
- ❑ In certain conditions, proxy notify requests are being sent to the OCS causing an access error (B#76462, 2-41623641, 2-41631551, 2-42015053).
- ❑ Relative paths in URLs are incorrectly re-written (as part of the URL normalization process) (B#76637, 2-41452001).
- ❑ Bypass list entries missing from text editor, present through CLI or Management Console view button (B#76910, 2-41852453, 2-42189871, 2-42590242, 2-42601647).

- ❑ Restart in process "HTTP SW C3EDDF20 for C41B1F20" in "shared\_dll.dll" at .text+0x1BE94 (B#77254, 2-42092317, 2-42092366, 2-43038791, 2-43461021).
- ❑ CAG: MC post CLI interface fails due to object open failures (B#75744, 2-42765975, 2-42809501, 2-43291921, 2-43444902, 2-43461583, 2-43485043, 2-43537741, 2-44040032, 2-44284210, 2-44490471).

## Doc Errata

### *Configuration and Management Guide*

- ❑ Page 505, Chapter 11: *External Services*, Section A: ICAP states:  
"The number of seconds the ProxySG waits for replies from the ICAP server. The range is 60 to 65536. The default timeout is 70 seconds."  
The actual range is 1 to 65536.
- ❑ Page 728, Chapter 16: *Streaming*, Section A: About Streaming Media, states:  
"Using the `content pull` CLI command, content is downloaded from the HTTP server and renamed with a given URL argument."  
The `content pull` command has been replaced with `content distribute`.
- ❑ Page 869, Chapter 20: *Access Logging*, Section H: Configuring the Upload Schedule, states:  
"If the remote server is unavailable to receive continuous upload log entries, the ProxySG saves the log information on the ProxySG disk. When the remote server is available again, the appliance resumes continuous uploading."  
This is misleading. When the data stream is interrupted, the log files are held on the proxy's hard disk. When the stream is restarted, logs held on the hard disk drive are not sent.
- ❑ *Content Policy Language*: Page 305: Syntax is incorrect. In the `ssl.forward_proxy()` property, the reference should be to HTTPS rather than HTTP.

```
ssl.forward_proxy(no)
ssl.forward_proxy(https)
ssl.forward_proxy(https, always) ; synonym for
ssl.forward_proxy(https)
ssl.forward_proxy(https, on_exception)
```

## Version: SGOS 4.2.3.7, build 27640

*Release Date: 12/07/2006*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2, ProxyAV 2.4 or ProxyAV 2.5*

*Document Revision: 1.08 on 01/25/2007*

## Enhancements

- ❑ Support has been added for Japanese MSN 7.5 IM.

## Fixes in this Release

- ❑ Openssl vulnerability fix regarding `SSL_get_shared_ciphers()` and buffer overflow. (B#75441, 2-40317861, 2-40800251)
- ❑ Management Console: SNMP default value misinterpreted by Management Console: SNMP displays as enabled when it is actually disabled (B#76084, 2-41320375)
- ❑ Page corruption when using the strip active content rule. (B#64947, 2-39845481, 2-39852501, 2-40007276, 2-41186476, 2-41322098)
- ❑ The use of rarely used four-bytes in the ASF packet header causes the proxy to restart when running audio live streams. (B#75915, 2-40193586)

See Page 34 for other fixes.

## Version: SGOS 4.2.3.4, build 27548

*Release Date: 11/27/2006*

*BCAAA Version: 120*

*Compatible with: Director SGME 4.2.x or SGME 5.1.3.x, Reporter 8.2.2, ProxyAV 2.4 or ProxyAV 2.5*

*Document Revision: 1.04 on 11/27/2006*

### New Features in SGOS 4.2.3.4

- ❑ Authentication:
  - "Novell SSO"
  - "Policy Substitution Realm Enhancements"
  - "Windows SSO SGOS 4.2.3.4 Enhancements"
- ❑ Content Filtering:
  - "Content Filtering Enhancements"
  - "BCWF Dynamic Categorization Proxy Chaining"
- ❑ "Director Support for Health Monitoring"
- ❑ "Health Monitoring"
- ❑ "Management Console/VPM Design Changes"
- ❑ "Permeo SOCKS Client"
- ❑ "Platform Support for SG510, SG810, and SG8100"
- ❑ "Windows Media RTSP Support"

### Known Issues in this Release

- ❑ "Known Issues with Management Console and VPM Design Changes" on page 69
- ❑ See Page 32 for other known issues.

### Fixes in this Release

- ❑ CLI: `Show interface all` output now displays the correct information when the interface is set for full duplex and 10Mbps. Numerous changes have been made to the CLI; this bug no longer is an issue. (B#57104)
- ❑ See Page 31 for Fixes regarding the Management Console and VPM Design Changes.

- ❑ See Page 34 for other fixes.

## **Version: SGOS 4.2.2.2, build 26403**

*Release Date: 07/07/2006*

*BCAAA Version: 110*

*Compatible with: Director SGME 4.x/Reporter 8.2.2/ProxyAV 2.4 or ProxyAV 2.5*

*Document Revision: 1.01 on 07/07/2006*

### **New Features in SGOS 4.2.2.2**

- ❑ "Access Logging Enhancements"
- ❑ Authentication: "Windows Single Sign-on"
- ❑ Content Filtering:
  - "Internet Watch Foundation"
  - "Partial Lookup"
- ❑ Policy: "SGOS 4.2.2 Enhancements"
- ❑ SSL Proxy:
  - "SSL Proxy Default Mode of Operation"
  - "SSL Detection"
  - "SSL Interaction with Reporter"

## **Version: SGOS 4.2.1.2, build 24604**

*Release Date: 01/18/2006*

*BCAAA Version: 100*

*Compatible with: Director SGME 4.2/Reporter 8.2.2/ ProxyAV2.4 or ProxyAV 2.5*

*Document Revision: 1.00 on 01/18/2006*

### **New Features in SGOS 4.2.1.2**

- ❑ "Apparent Data Type"
- ❑ Authentication:
  - "RADIUS Enhancements"
  - "IWA/Kerberos Support"
- ❑ "Certificate Revocation Lists"
- ❑ "Health Checks Timeout"
- ❑ "HTTP Changes"
- ❑ "ICAP Performance Enhancements"
- ❑ "Internationalization--General Support"
- ❑ "Licensing Behavior Changes"
- ❑ "Policy Enhancements"
- ❑ "Protocol Detection"

- ❑ "Root CA Certificates"
- ❑ "SSL Proxy"

## New Features in SGOS 4.2.x

### Access Logging Enhancements

Two new formats —`bcreportermain_v1` and `bcreporterssl_v1`--have been added to supported interaction with Reporter. If you are using SSL, you should use the `bcreporterssl_v1` format, which does not reveal private or sensitive information.

### Apparent Data Type

This feature, used through policy, identifies data content associated with Microsoft DOS and Windows executable files. When used in a deny policy, drive-by installation of spyware is blocked. File types that are blocked include:

- ❑ \*.exe
- ❑ \*.dll
- ❑ \*.OCX
- ❑ \*.CAB

### Certificate Revocation Lists

Certificate Revocation Lists (CRLs) allow checking server certificates against lists provided and maintained by Certificate Signing Authorities that show certificates that are no longer valid. Only CRLs that are issued by a trusted issuer can be verified by the ProxySG successfully. The CRL can be imported only when the CRL issuer certificate exists as CA certificate on the ProxySG.

### Content Filtering Enhancements

- ❑ Internet Watch Foundation

(New in SGOS 4.2.2) The Internet Watch Foundation (IWF) is a non-profit organization that provides to enterprises lists of known child pornography URLs. The IWF provider features a single category called IWF-Restricted, which is susceptible to policy checks. During content filtering configuration, you can select this option; then create policy to block this category.

- ❑ Partial Lookup

(New in SGOS 4.2.2) You can disable dynamic categorization of content filtering vendors. The default is Always, which indicates that any installed database should be consulted on every categorization attempt. Uncategorized indicates that installed data should be skipped if the URL already has categories assigned.

- ❑ BCWF Dynamic Categorization Proxy Chaining

(New in SGOS 4.2.3) The ProxySG allows you to forward Dynamic Categorization requests through upstream proxies and SOCKS gateways, which eliminates the requirement for the ProxySG to have direct connection to back-end servers.

## Director Support for Health Monitoring

Platforms running SGOS 4.2.3.4 can be monitored for health status by Director 5.1.x. Each individual health monitored statistic maintains a `last transition time` that is set whenever that statistic changes state. The most recent time represents the last time a state transition occurred on the appliance. Note that this is not the same as the last time the SG's overall state changed.

## Health Checks Timeout

Fail-over times in many circumstances have been reduced.

## Health Monitoring

The health monitoring feature enhances the remote monitoring capabilities of the ProxySG. By monitoring key hardware and software metrics, Director (and other third-party network management tools) can provide administrators with a remote view of the health of the ProxySG system.

To facilitate prompt corrective action, notification can be configured for threshold "events." For example, an administrator can configure a threshold so that an e-mail or SNMP trap is generated when the threshold state changes. Additionally, many of the threshold levels are configurable so that you can adjust the thresholds to meet your specific requirements.

## HTTP Changes

SGOS 4.2.2 contains better HTTP response header parsing support.

This enhancement eliminates the limitations of previous releases:

- ❑ Response headers that are larger than approximately 8 KB were not parsed.
- ❑ Length of any individual header cannot be larger than 8 KB.
- ❑ Only up to 125 response headers were parsed.
- ❑ Response header continuation was not supported.
- ❑ HTTP compression level can now be controlled by policy.

## ICAP Performance Enhancements

The max-cache-size dependency for scanning has been removed, resolving a number of issues surrounding patience pages and improving performance. Among them:

- ❑ When the HTTPS proxy was enabled, the patience page did not show the progress correctly.
- ❑ If a cached object contained a virus and was sent for a rescan, ProxySG still served it.
- ❑ Requests to some HTTPS sites were resulting in a 400 BAD request.
- ❑ The ProxySG gave a "Connection failure" error page for ICAP 500 Server error responses.
- ❑ The ProxySG crashed when ICAP worker creation failed while scanning cached content.
- ❑ Certain non-cacheable file sizes were not served when the patience page was enabled.
- ❑ The ProxySG was not maintaining persistent connections to the ICAP server.
- ❑ ICAP health checks were always failing with response timeout.

- ❑ FAIL\_OPEN for scan\_cached\_object case did not work.
- ❑ A patience-page loop existed as expires headers set in the past overrode the four-hour expiration on non-cacheable objects.

## Internationalization--General Support

For management interfaces, the only character encodings supported are ASCII and UTF-8. (ASCII is a subset of UTF-8.) This affects the CLI, the encoding of CPL source files, exception pages, and access logs. Libraries such as Shift-JIS and Big5 (Chinese) are not supported.

For proxy network traffic (such as HTTP requests from a client workstation and instant messaging), a variety of different character encodings are supported, including Shift-JIS and Big5 (Chinese).

Generally speaking, the Blue Coat internationalization feature provides support for:

- ❑ Non-ASCII user names, group names and passwords (in the most common cases only).
- ❑ Exception pages.
- ❑ Non-ASCII instant messaging (in the common cases only).
- ❑ Director.
- ❑ Reporter (Reporter v7.1.3 and higher).

SGOS 4.2.2.1 supports general international character support for non-English AOL and MSN IM clients. Yahoo non-English clients are not supported.

Features:

- ❑ General messaging using non-ASCII characters.
- ❑ CPL/VPM policy specified with non-ASCII text field names are supported, with exception that VPM-CPL and VPM-XML files must be encoded for UTF-8.
- ❑ CPL/VPM policy with non-ASCII text matching and replacement is expected to work.
- ❑ CPL/VPM policy with non-ASCII text triggers for file transfer file names and chat/conference rooms are not supported with SGOS 4.2.2.x for AOL and Yahoo.
- ❑ CPL/VPM policy with non-ASCII text triggers for file transfer file names and chat/conference rooms are expected to work with MSN.
- ❑ Non-ASCII text fields are supported for Access Log outputs.

## IWA/Kerberos Support

Support for Kerberos and Integrated Windows Authentication (IWA), replacing NTLM as an authentication realm where appropriate.

### *Limitations*

- ❑ Do not set cache credentials to 0. This does not work properly in NTLM/IWA realms.

## Licensing Behavior Changes

You can now disable the trial period through either the Management Console or the CLI. Disabling the trial period causes unlicensed ProxySG features to stop working.

## Management Console/VPM Design Changes

### *General*

As a result of design changes among Blue Coat products, you can now:

- ❑ Change all panels on the Management Console before applying changes.
- ❑ Preview pending changes.

Other changes include:

- ❑ Installable lists are done using a Java editor within the Management Console..
- ❑ Advanced URL are displayed using Java editor within the Management Console.
- ❑ The Management Console logs out when connectivity lost with the ProxySG.

The Management Console depends upon the CLI for validation failure. If something failed during the **Apply** operation, a window displays with the CLI command output including any error or informational messages.

The VPM module is no longer an independent application, but is an integral part of the Management Console. For example, when creating User/Group objects, VPM previously would fetch realms directly from the ProxySG; now that information comes from the Management Console. For a list of known issues and workarounds, see [“Known Issues with Management Console and VPM Design Changes”](#) on page 69.

### *VPM*

The VPM *shares* information in various lists from the current configuration in the Management Console, *not* the saved ProxySG configurations. When the VPM is launched from the Management Console, it inherits the state of the Management Console and remains synchronous with that Management Console. This state includes configuration changes that have not yet been applied or reverted. This does not include any changes made through the CLI. When you click Apply in the Management Console, the configurations are sent to the ProxySG; the Management Console and the VPM then become synchronized with the ProxySG.

For example, the ProxySG has two ICAP response services installed, A and B. In the Management Console, you remove service B, but do not click Apply. You then start the VPM and view the ICAP Response Services object. Only service A is viewable and selectable.

Another consequence of this new behavior is that VPM does not fetch forwarding host information after the initial application load. Clicking **Revert** in the Management Console synchronizes the Management Console with the current state in the Blue Coat SG.

Following are the lists the VPM obtains from the Management Console:

- ❑ Access Log fields.
- ❑ Authentication character sets.
- ❑ Authentication realms.
- ❑ Bandwidth gain classes.
- ❑ Categories.
- ❑ Exceptions.
- ❑ Forwarding hosts. Note that the VPM does not fetch forwarding host information after being launched.

- ❑ ICAP request and response services.
- ❑ Keyrings.
- ❑ SOCKS gateways.
- ❑ Websense filter services.

For a list of known issues and workarounds, see [“Known Issues with Management Console and VPM Design Changes”](#) on page 69.

## Novell SSO

The Novell® Single Sign-on (SSO) realm is an authentication mechanism that provides single sign-on authentication for users that authenticate against a Novell eDirectory® server. The mechanism uses the Novell eDirectory Network Address attribute to map the user's IP address to an LDAP FQDN. Since the mechanism is based on the user's IP address, it only works in environments where an IP address can be mapped to a unique user.

### Notes

- ❑ The Novell SSO realm works reliably only in environments where one IP address maps to one user. NAT environments are not supported.
- ❑ Novell SSO realms are not supported in IPX environments.
- ❑ Upgrade to Novell client 4.91 SP1 or later if you experience issues with the Network Address attribute not being updated during login.
- ❑ Novell SSO realms do not use user credentials so they cannot spoof authentication information to an upstream server.
- ❑ If an upstream proxy is doing Novell SSO authentication, all downstream proxies must send the client IP address.
- ❑ There can be response time issues between the BCAA service and the eDirectory servers during searches; configure the timeout for LDAP searches to allow the eDirectory server adequate time to reply.
- ❑ The BCAA service that supports Novell SSO is version 120.

## Permeo SOCKS Client

The Blue Coat ProxySG can be used as a SOCKS gateway by the Permeo Premium Agent (PA), with full licensing support and Dynamic Port Management (DPM) functionality.

The ProxySG supports the Windows Permeo PA SOCKS client version 5.12a, including those that require the special probe license protocol and corresponding customer ID. Note that each ProxySG can only support PA clients with the same customer ID.

## Platform Support for SG510, SG810, and SG8100

Three new platforms are supported: The SG510 the SG810, and the SG8100.

System image management has been changed on these platforms to enable future upgrades to our next generation operating system.

Along with a number of engineering improvements, visible changes include:

- ❑ True system view—Starter displays the set of images that exist across all installed drives. In the legacy Starter only the images on the boot drive are displayed.

- ❑ Fault tolerance—Failure to load a particular image from one disk triggers an attempt to load the same image from a different disk. If all instances of the image fail to load, the next most recent image is loaded.
- ❑ Dynamic slot assignments— Instead of images being loaded into fixed slots, images are now sorted by their creation date. The newest image always appears in slot one. Existing images can still be replaced, but the new image will not necessarily exist in the same slot as the replaced image; instead it is slotted according to its creation date.
- ❑ Versioning—The boot chain now versions itself. If at anytime an image includes a newer boot chain, the boot chain updates itself and reboots the system to activate the newer boot chain. The boot chain is also placed on all installed drives to ensure that if one drive fails any other drive can still boot the system.

## Policy Enhancements

For SGOS 4.2, the following conditions are supported in the SSL layer. They previously were supported in the <Proxy> and <Exception> layers. Both conditions can still be used in the Proxy and Exception layers, but you will receive a deprecation message.

- ❑ `client.connection.negotiated_cipher=`
- ❑ `client.connection.negotiated_cipher.strength=`

### SGOS 4.2.2 Enhancements

In releases subsequent to SGOS 4.2.1, two new policy properties—`HTTP.client.persistence` and `HTTP.server.persistence`—have been added to control the persistence of individual client and server connections. Control is based on any policy conditions available in the <Proxy> or <Exception> layers.

## Policy Substitution Realm Enhancements

Policy Substitution Realms are not new in this release, but have been enhanced to support searching an LDAP realm to determine a user's identity. This functionality is useful when the policy substitutions cannot map directly to the user's username and/or full username.

A new policy substitution has been created, as well as several string modifiers, for SGOS 4.2.3:

- ❑ `$(ident.username)`: This results in an Ident query to the client machine for the port that the client has connected to on the ProxySG. The substitution returns the username as specified by the client machine. A Policy Substitution realm can use the `$(ident.username)` substitution to identify users and provide a single sign-on mechanism for clients that run an identd server.
- ❑ `binary_address`—This string modifier can be used to convert a dotted IP address into 4 bytes (one byte for each octet on any substitution that resolves to a dotted IP address. The resulting string is of the format `\xx\xx\xx\xx` where `xx` is an address byte. This modifier does not take arguments.
- ❑ `escape_ldap_filter`—This string modifier allows administrators to specify that a policy substitution value should be escaped using the LDAP search filter syntax as specified in RFC 2254. This modifier does not take arguments.

## Protocol Detection

Protocol detection has been added that identifies HTTP, SSL, and various P2P protocols carried within HTTP CONNECT requests, SOCKS CONNECT requests, and TCP tunnels. Because of this new behavior, if protocol detection is enabled, any protocols recognized inside tunnels will be processed as if they were received by the corresponding proxy. So, for example, an HTTP request recognized in this manner has full HTTP policy applied to it, rather than just simple TCP tunnel policy. In particular, this means that:

- ❑ The request shows up as client protocol "HTTP" rather than "TCP Tunnel".
- ❑ The URL used while evaluating policy is an "http://" URL of whatever shows up in the tunneled HTTP request, not a "tcp://" URL of where the tunnel was connecting to.
- ❑ Forwarding policy is applied based on the new HTTP request and not the original tunnel, so the forwarding host selected must support HTTP. A forwarding host of type TCP cannot handle the request and causes the request to be blocked.

To carry this traffic over a TCP tunnel without applying this additional policy, protocol detection should be disabled.

## RADIUS Enhancements

- ❑ Support for RADIUS servers that use challenge/response as part of the authentication process as well as support for RADIUS groups and the ability to fine-tune RADIUS realms with a number of new attributes.
- ❑ New authentication forms to support RSA SecurID Authentication Manager Version 6.0 and earlier. RSA SecurID Authentication Manager 6.1 does not require the new forms.

## Root CA Certificates

The ProxySG trusts all root CA certificates that are trusted by Internet Explorer and Firefox. This list is updated periodically to be in sync with the latest versions of IE and Firefox.

## SSL Proxy

The SSL proxy allows you to intercept HTTPS traffic (in explicit and transparent modes) so that security measures such as authentication, virus scanning and URL filtering, and performance enhancements such as HTTP caching can be applied to HTTPS content. Additionally, the SSL proxy allows you to validate server certificates presented by various HTTPS sites at the gateway and offers rich information about the HTTPS traffic in the access log.

When using the SSL Proxy software, use of the SSL hardware accelerator card is strongly recommended. For best performance, your system should also have 512MB RAM or higher.

In releases subsequent to SGOS 4.2.1, other SSL enhancements have been made. They include:

- ❑ SSL Detection

You can now control SSL detection for HTTP, SOCKS, and TCP tunnels through both the Management Console and the CLI. Note that if you are using the Management Console, the SSL proxy Intercept pane has been moved from the Management Console>Configuration>SSL pane to the Management Console>Configuration>Services>SSL Proxy pane.

#### ❑ SSL Proxy Default Mode of Operation

With SGOS 4.2.2.1, the SSL proxy intercepts an SSL connection in its default mode if it encounters some error, allowing it to send an HTML error page to the user. If no error is detected, the SSL proxy tunnels SSL connections by default. So the default mode is intercept only on exception, tunnel otherwise. Note that this is a change from SGOS 4.2.1, where the default behavior was to tunnel always.

#### ❑ SSL Interaction with Reporter

A reserved access logging format has been added `--bcreporterssl_v1--` that should be used with SSL. This is a reserved format that cannot be edited. It only contains fields that do not reveal private or sensitive information, unlike the `bcreportermain_v1` format.

#### *Limitations*

- ❑ The field **Currently active sessions** under SSL Origination on the SSL/Statistics page displays an invalid counter value.

### Statistics

A new CLI command `--clear-statistics efficiency--` has been added to Configure mode to clear efficiency statistics counters that are visible in the **Management Console>Statistics>Efficiency** or CLI `show efficiency`.

### WCCP Masking

The assignment-type and mask-scheme commands are now supported in SGOS 4.2.2. Note that this feature is not backwards compatible; if you downgrade to a version that does not support WCCP masking, you must reconfigure WCCP. The same is true if the interface 1:0 was specified as opposed to older configurations where interface 0 or 1 could be specified.

### Windows Media RTSP Support

The ProxySG now supports Windows Media content streamed over RTSP in SGOS 4.2.3.

The following Windows Media RTSP transports are supported:

- ❑ Client-side traffic:
  - RTP over unicast UDP (RTSP over TCP, RTP over unicast UDP)
  - Interleaved RTSP (RTSP over TCP, RTP over TCP on the same connection)
  - Multicast UDP (for live content only)
- ❑ Server-side traffic:
  - Interleaved RTSP

Server-side RTP over UDP is not supported. If policy directs the RTSP proxy to use HTTP as server-side transport, the proxy will deny the client request. The client then rolls over to MMS or HTTP.

The Windows Media RTSP functionality is included in the existing Windows Media license.

Note that the following CLI commands are used only by the Windows Media MMS proxy. They are not used for RTSP support.

```
SGOS#(config) streaming windows-media log-compatibility
```

```
SGOS#(config) streaming windows-media live-retransmit
SGOS#(config) streaming windows-media server-thinning
SGOS#(config) streaming windows-media asx-rewrite
SGOS#(config) streaming windows-media multicast-alias
SGOS#(config) streaming windows-media unicast-alias
SGOS#(config) streaming windows-media broadcast-alias
```

### *Limitations*

#### ❑ RTSP Client Errors

In some cases the ProxySG disconnects the client (for example **access server denied**) and the client can choose to attempt a reconnection.

In other cases, when the ProxySG returns an AdministrativeDisconnect error, no attempt to reconnect is made by the client.

#### ❑ Live Stream Sourced from an Encoder

Sometimes when a live stream is sourced from a encoder, the Windows Media server marks the content as not splittable by the proxy. In such cases, the ProxySG treats the stream as pass-through traffic.

#### ❑ Thinning

Thinning might not work when the client is using TCP Transport. (B#62453)

#### ❑ Buffering State

Windows Media player can sometimes enter a buffering state near the end of the stream when using a rtsp:// URL. (B#64430)

## **Windows Single Sign-on**

The Windows Single Sign-on (SSO) realm is an authentication mechanism available on Windows networks.

### *Windows SSO SGOS 4.2.3.4 Enhancements*

- ❑ FQDN: The Fully Qualified Domain Name (FQDN) of the user is now determined by the Windows SSO realm. This can be used to determine the groups and attributes of the user through the associated authorization realm.
- ❑ BCAA Synchronization: When using Domain Controller Querying, you can configure a BCAA service to use another BCAA service as a synchronization server. Whenever a BCAA service restarts it will contact its synchronization server and update its logon state. Two given BCAA services can use each other as their synchronization server. Thus, each BCAA service can act as a synchronization server to provide logon state to other BCAA services, as well as acting as a synchronization client to update its logon state from another BCAA service.

## **XML Realms**

If you use an authentication or authorization protocol that is not natively supported by Blue Coat, you can use the XML realm to integrate SGOS with the authentication/ authorization protocol.

An XML realm uses XML messages to request authentication and authorization information from an HTTP XML service (the XML *responder* that runs on an external server). The XML realm (the XML *requestor*) supports both HTTP GET and HTTP POST methods to request an XML response. The XML messages are based on SOAP 1.2.

## System Requirements For Upgrades

This section lists the system component requirements for this release and which vendor components are supported.

### ProxySG Platform (Software and Hardware)

- ❑ Software: If you are upgrading from a previous Blue Coat release, the ProxySG must be running SGOS 4.2.1.6 or higher. See the Supported Upgrade Path section below.
- ❑ Hardware: Blue Coat appliance models SG200-x, SG400-x, SG510, SG800-x, SG810, SG8000-x, and SG8100 can be upgraded to SGOS 4.2.3.

**Note:** Due to RAM limitations on the Blue Coat SG 200-0 and SG 400-0 (256MB), very low throughput is to be expected on these platforms, with a maximum at 20 mbps. For sizing information, talk to your Blue Coat sales representative.

Older Blue Coat appliance models 6xx, 5xx, 7xx, 3xxx, 5xxx, 6xxx, 7xxx, 2xxx, 1xxx, and 1xx cannot be upgraded to this release. To upgrade the hardware to a newer model, contact your local reseller or Blue Coat Sales (at [sales@bluecoat.com](mailto:sales@bluecoat.com)).

### Supported Upgrade Path

Refer to the table below for the correct upgrade path.

Table 15. Upgrade Paths

Current OS (Range)	Direct Upgrade to Latest Version?	Next OS version required
SGOS 2.1.x, where x >= 07	No	SGOS 3.2.6
SGOS 3.1.x	No	SGOS 3.2.6
SGOS 3.2.x, where x <= 3	No	SGOS 3.2.6
SGOS 3.2.x, where x >= 4	No	SGOS 4.2.1.6
SGOS 4.1.x	No	SGOS 4.2.1.6
SGOS 4.2.1.x, where x <= 5	No	SGOS 4.2.5
SGOS 4.2.1.x, where x >= 6	Yes	SGOS 4.2.5
SGOS 4.2.2.x	Yes	SGOS 4.2.5

## Upgrading Licenses

### To upgrade the license:

1. In the Management Console, select **Maintenance>Licensing>Install>License Key Automatic Installation** field.
2. Do one of the following:
  - If the **Update** button is enabled, click **Update**.
  - If the **Update** button is not enabled and you have a valid WebPower account login (the same WebPower credentials that the appliance is registered to), click **Retrieve**. A Request License Key dialog appears. Enter your WebPower credentials and click **Send Request**. The Blue Coat license server receives the request, automatically upgrades the SGOS 4.x license, and returns the new license to the appliance.

### Alternate Methods

- If you cannot directly access the Internet, contact Blue Coat Support Services for assistance. You will be asked to provide the hardware serial numbers of the appliances to be upgraded and account details, such as contact name, e-mail address, and WebPower account name.
- If you do not have a WebPower account or lost the password, contact Blue Coat Support Services.

## Upgrading the BCAA Authentication Service

If you use one of the following authentication realms, you should upgrade to the latest release of the Blue Coat Authentication and Authorization Agent (BCAAA) service.

- Integrated Windows Authentication
- Oracle COREid
- Netegrity Siteminder
- Novell SSO
- Windows SSO

BCAAA is distributed as a zip file or UNIX shell script, to be installed on a Microsoft® Windows® system or a Solaris™ system. The zip file to download the BCAA service is posted on the SGOS 4 Software Download Page at <http://download.bluecoat.com/release/SGOS4/index.html>.

---

**Note:** Because of fixes to the BCAA service, Blue Coat recommends that you upgrade to the latest version of BCAA.

---

## Using Multiple Versions of the BCAA Service

You can run multiple versions of the BCAA service. Depending on the versions of BCAA that you want to run, you might have to install different versions of the service. Each version of the BCAA service that you want to run must reside on your system.

---

**Note:** You cannot use an older version or a newer version than your proxy expects. For example, you must install BCAA version 100 for SGOS 4.2.1 or BCAA version 110 for SGOS 4.2.2.

---

Table 16. Supported Versions of the BCAA Service

SGOS Version	BCAA Version Supported
SGOS 3.2.6	Upgrade to BCAA version 99 <a href="http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaa.zip">http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaa.zip</a> or higher <a href="http://download.bluecoat.com/release/SGOS4/index.html">http://download.bluecoat.com/release/SGOS4/index.html</a>
SGOS 4.1.x	Upgrade to BCAA version 99: <a href="http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaa.zip">http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaa.zip</a> or higher <a href="http://download.bluecoat.com/release/SGOS4/index.html">http://download.bluecoat.com/release/SGOS4/index.html</a>
SGOS 4.2.1	100—Download from: <a href="http://download.bluecoat.com/release/SGOS4/index.html">http://download.bluecoat.com/release/SGOS4/index.html</a>
SGOS 4.2.2	110—Download from <a href="http://download.bluecoat.com/release/SGOS4/index.html">http://download.bluecoat.com/release/SGOS4/index.html</a>
SGOS 4.2.3	120—Download from <a href="http://download.bluecoat.com/release/SGOS4/index.html">http://download.bluecoat.com/release/SGOS4/index.html</a>

Install the lowest version of the BCAA service first and the highest version of BCAA last, allowing each version to uninstall the previous version. This leaves behind the `bcaa.ini` and `bcaa-nn.exe` files for that version.

## Notes

- ❑ Only one listening port is used, no matter how many versions you have installed. The BCAA service hands off the connection to the appropriate BCAA version.
- ❑ Installation instructions for BCAA are located in Appendix A of the *Blue Coat ProxySG Configuration and Management Guide* that is accessible through WebPower account access.
- ❑ The BCAA service cannot be installed on Windows NT.

## Clients and Browsers

The Web-based Management Console (MC) and the Visual Policy Manager (VPM) Java application should be used only under the following recommended combinations of OS, Browser and Sun Java Runtime Environment (JRE) versions.

- ❑ OS for MC and VPM: Microsoft 2000 Pro (SP4 or later), XP (SP2 or later).
- ❑ Browser for MC and VPM: Internet Explorer 7.0, Internet Explorer 6.0 (SP1 or later), Firefox 1.5, Netscape 7.2, Windows Vista. Later versions might work, but they have not been tested.
- ❑ JRE: 1.5.0, 1.4.1\_07.

### Notes

- ❑ Only JRE 1.4.1\_07 and 1.5.0 are supported. Because of a Sun-published security issue regarding JRE 1.4.1\_07, only use this version for administrative access to the ProxySG, not for access to external Internet sites. Blue Coat recommends upgrading to JRE 1.5.0.
- ❑ On the Sun download page, Sun naming conventions refer to J2SE 1.5.0 and J2SE 5.0 interchangeably. J2SE 5.0 is the new name for JRE 1.5.
- ❑ Before you download JRE 1.5, verify you have the correct file. Select **Related Links>Popular Downloads>J2SE 5.0** to access the JRE 1.5 download page. Select the desired file.
- ❑ If you experience a problem downloading the latest supported JRE through the Management Console because:
  - The browser does not support automatic download (for example, Netscape), or
  - The automatic download hangs.Enter the following URL to get to the Sun download page (if the automatic download hangs, first terminate the download):  
`http://java.sun.com/products/plugin/index.jsp`
- ❑ Network slowness or slower processor speeds might affect JRE 1.5 performance. The delay decreases the ability to click between Management Console menu selections and options.
- ❑ The Management Console Java applet cannot retrieve data from behind a reverse proxy; it displays the error **unable to obtain session secret from ProxySG**. (B#60652)
- ❑ Enable the auto-detect encoding feature on your browser so that it uses the encoding specified in the console URLs. The browser does not use the auto-detect encoding feature by default. If auto-detect encoding is not enabled, the browser ignores the charset header and uses the native OS language encoding for its display

## Support for Other Products

### *Blue Coat Director and Reporter*

- ❑ This release is compatible with the following Blue Coat Director releases: SGME 4.2.x (if using content management) or SGME 5.1.3.x (without content management).  
Note that SGME 5.1.3.x lacks the content management features present in SGME 4.2.x. Also note that neither SGME release monitors the health state of a SG running this version of SGOS.

- ❑ This release is compatible with the following Blue Coat Reporter releases: Reporter 8.1.1 and higher.

## *Anti-Virus*

The Blue Coat ProxySG with ProxyAV™ integration is a high-performance Web anti-virus (AV) solution. For more information, refer to the Blue Coat Web site.

This release is compatible with ProxyAV versions 2.4 or 2.5.

In this release, SGOS is certified with the following third-party implementations of ICAP:

- ❑ Symantec AntiVirus Scan Engine (SAVSE) 4.3, version 4.3.0.15; ICAP 1.0.
- ❑ WebWasher 5.3, build 1953; ICAP 1.0.
- ❑ Finjan Vital Security 7.0, Service Pack 3a; build 573; ICAP 1.0.

## *Instant Messaging*

Instant Messaging proxy support includes

- ❑ English language versions
- ❑ Japanese language versions

Also, some versions of AOL and Windows Live Messenger (WLM) are not officially supported but work in most situations.

### **English Language Versions Supported**

- ❑ AOL: v5.1 to 5.9.
- ❑ MSN: v4.6, 5.x, 6.0, 6.1, 6.2, 7.0, 7.5.
- ❑ WLM: v8.1, 8.5
- ❑ Yahoo: v5.5, 5.6, 6.0, 7.0, 8.1.

### **Japanese Language Versions Supported**

- ❑ AIM 5.1
- ❑ Yahoo 7.0
- ❑ WLM 8.0

### **Partially Supported IM Protocol Versions**

#### *AOL*

The ProxySG does not recognize AOL v6.x as AIM (IM) traffic. In some ProxySG configurations, however, client login and chat do succeed.

- ❑ AOL: v6.1
  - If a SOCKS proxy is configured in the client's Internet Explorer (IE) settings:
    - SOCKS proxy with detect protocol disabled on the ProxySG: The client can log in and chat normally.
    - SOCKS proxy with detect protocol enabled on the ProxySG: The client can log in and chat with a thirty-second delay.

- If an HTTP/Secure proxy is configured in the client PC's IE settings:
  - HTTP proxy with detect protocol disabled on the ProxySG: The client can log in and chat normally
  - HTTP proxy with detect protocol enabled on the ProxySG: The client login fails after about 30 seconds with the message Connection lost.
- Transparent deployment: AIM v6.1 cannot log in if an SSL service is configured on port 443. AIM can log in, with a 30-second delay, if a TCP tunnel service is configured on port 443 with protocol detection enabled. AIM can log in if the SSL forward proxy is also enabled and the ProxySG appliance's certificate is installed as the root certificate on the client's IE browser.

❑ AOL: v6.5

- The client can log in and chat unless the SSL connection is intercepted by the SSL forward proxy. Supported deployments, if the SSL connection is not intercepted by the SSL forward proxy include transparent/TCP tunnel on port 443, transparent/SSL proxy on port 443, and HTTP proxy or SOCKS proxy.

To deny login for AOL 6.x clients, the following policy can be used:

```
<Proxy>  
DENY url.host=kdc.uas.aol.com
```

## Streaming

Streaming media support is limited to the following media players and servers:

- ❑ The ProxySG supports the following versions and formats:
  - Windows Media Player 7, 9, and 10
  - Windows Media Server 4.1
  - Windows Media Server 9
- ❑ The ProxySG supports the following Real Media Players and Servers:
  - RealOne Player, version 2
  - RealPlayer 8 and 10
  - RealServer 8 through 10
  - Helix Universal Server
- ❑ The ProxySG supports the following versions and servers, but in pass-through mode only:
  - QuickTime Players v7.x, 6.x, and 5.x
  - Darwin Streaming Server 4.1.x and 3.x
  - Helix Universal Server

## WCCP

SGOS 4.x has been tested with several releases of Cisco's IOS: 12.0.7, 12.1.6E, and 12.2.18

## Limitations

Descriptions of limitations with the release that could be encountered by more than a few customers are provided. See "[Section B: Limitations](#)" to:

- ❑ Understand the issues before upgrading to this release.
- ❑ Verify that a problem you have is not a limitation or a known issue before reporting it to Blue Coat Support.

## Section B: Limitations

*Version: SGOS 4.2.x*

This document provides a subset of limitations with the Blue Coat SGOS 4.2 release that might be encountered by more than a few customers. It is updated with every SGOS release.

Read through the following issues before upgrading to the SGOS 4.2.x release. Also, if an operation issue arises, before contacting Blue Coat, visit this page to verify it is not a limitation or a known issue.

### Browsers

- ❑ If you use Firefox 1.x or Internet Explorer 7.x or higher, you cannot use the browsers' multi-tab functionality. This is because the Management Console is now one entity instead of numerous applets and because the browsers open only one instance of themselves; no matter how many tabs are open only one instance of the Java Virtual Machine is launched. For example, you can no longer use one tab to access the Management Console and another tab to watch the access logs.  
  
To use IE 7 or Firefox to watch multiple windows, launch separate instances of the browser.
- ❑ Pop-up blockers are enabled by default in IE 6 and IE7. In this case, you must change the browser options to access the Statistics URLs or the online help.
- ❑ With IE 7.x or higher, you might see a message that says **certificate error** instead of being presented with the certificate prompt. This is because the SG appliance is not trusted. You can add the SG appliance certificate to the browser's certificate store to eliminate the error message. You can also ignore the error and continue. (B#64916)
- ❑ If you are using HTTP to connect to the Management Console, clicking the Back button in the browser results in the following error message:  
  
*Unable to obtain session secret from ProxySG. Please try reloading the current page.*  
  
Refresh the current page to continue. (B#45351a)
- ❑ Netscape 4.x browsers are incapable of handling compressed content for certain content types. For now, it is advised to disable compression for all requests from Netscape 4.x browser. You can use following policy for this (B#46368a):  

```
<proxy>  
  request.header.User-Agent="Mozilla/4." request.header.User-  
  Agent="!.MSIE." http.allow_compression(no)
```
- ❑ If you are using Firefox to access one Management Console and open another Firefox browser to access a different ProxySG Management Console, the second browser might not be fully functional. This is a Firefox issue, not a ProxySG issue. (B#48146a)
- ❑ Firefox: When multiple JREs are installed in the system (such as JRE 1.4.1\_07 and JRE 5.0), uninstalling one of them could make some versions of Firefox think no JRE is installed in the system. If this is the case, when you use Firefox to try to start the Management Console, you are prompted to download JRE 5.0 even though it might be already installed. If this happens, two workarounds exist: Either use Internet Explorer or close all browsers, delete all JREs from the system, and relaunch the browser, which will then install the correct JRE. (B#56127a)
- ❑ When running JRE v1.4.1\_07, resizing the window does not repaint the browser. To repaint, reselect the applet.

- ❑ Internet Explorer does not include Pragma: no-cache header while refreshing an HTTPS URL; this can cause the ProxySG to serve stale content from cache when caching is enabled. The workaround is to write policy, such as `check_authorization(yes)` or `always_verify(yes)`, or set strict server expiration through the CLI by using the `http strict server expiration` command to avoid this issue. (B#53278a)
- ❑ Virtual URLs: RFCs 952, 1123, and 821 prohibit the use of underscore in hostnames and mail domains, but the use of underscores is permitted in domain names. Microsoft Internet Explorer did not abide by this rule until I.E. 6.0, XP SP2. Therefore, any virtual URL used in authentication realms cannot contain a "\_" (underscore) character in the hostname part of the URL. (B#54245a)

## Access Logging

- ❑ If you change log formats *on the fly*, the ProxySG continues logging to the same log object, resulting in a log upload of a file that contains two different formats. This is a transient condition that affects only a certain number of entries (the number depends on the load) after which the new file is generated with the correct ELFF header. This has the effect of Reporter not reporting that certain number of entries.
- ❑ The access log variable `x-cs-certificate-valid-to` gives an incorrect value for the HTTPS Forward Proxy and no value ("-") for HTTPS Reverse Proxy. (B#54389a)
- ❑ The access-log tail might not display the entries correctly if the entry being logged is greater than 8KB in size. This happened in the scenario where the `http-response` headers being logged were greater than 8KB. (B#55192a)

## Authentication

- ❑ NTLM/IWA Realms: Do not set cache credentials to 0. This will not work properly in NTLM/IWA realms until the credential cache is rewritten. (B#54982a)
- ❑ Without the LDAP realm in the sequence, the Windows SSO realm will not correctly authorize against its LDAP realm. (B#83010a, SR 2-57161790)
- ❑ Forms-based authentication is not supported through explicit proxy when a user attempts to visit an HTTPS site.
- ❑ When the Oracle COREid 6.5 WebGate server software is upgraded to Oracle COREid 7.0, the SSO feature might stop working even if the `ipvalidation` value in the WebGate configuration file (`WebGateStatic.lst`) is set to `false` by the administrator afterwards. The workaround is to uninstall and reinstall the Oracle COREid 7.0 WebGate software, and set `IPValidation` to **false**. Then restart the COREid Access server and the IIS server. (B#55167a)
- ❑ After an upgrade to SGOS 4.2.x client certificate authentication might stop working with Internet Explorer if the HTTPS reverse proxy service in question is not using a CA Certificate List (CCL). Internet Explorer cannot handle the long list of CAs presented by the ProxySG in one of the handshake messages. The workaround is to create a CCL with relevant CAs and use that CCL with the HTTPS reverse proxy service. (B#56027a)
- ❑ If the BCAA service creates and stores its own certificate when running as `LocalSystem`, the service fails if it is subsequently changed to run as a domain user. You must delete the stored certificate and import the newly created one onto the ProxySG. (B#61319a)

- ❑ If BCAA is set up to save its certificates (which it does by default) and the following conditions are met:
  - more than one agent realm is referenced in policy
  - each of those realms is configured to use SSL

multiple certificates are created.

When the policy is activated, the multiple realms each attempt to connect to BCAA; each connection spawns a separate process and each process attempts to create a certificate since none is available. If more than one process creates a certificate, multiple certificates are created in the certificate store. The Windows 2003 SSL library fails with a meaningless error.

If this occurs, complete the following steps:

- a. From the **Start>Run** menu, launch MMC (Microsoft Management Console.)
- b. From the File menu, select **Add/Remove Snap-in**. The Add/Remove Snap-in pane displays.
- c. Click **Add**. The list of available snap-ins displays.
- d. Select **Certificates**. Click **Add**.
- e. Select the Service Account radio button. Select **Next**.
- f. Set the options as appropriate for your environment. Select **Next**.
- g. Select **BCAA**.
- h. Click **Finish**; click **Close**.
- i. Click the **Certificates** folder. Click **OK**.
- j. Open the **BCAA\Personal** folder.
- k. Delete any extra certificates—only one should exist.

## Bandwidth Management

- ❑ There might be transient statistics measurements when changing the priority level of a bandwidth class. (B#483902a)
- ❑ Bandwidth Management hierarchy might need to be re-configured when copying the output of `show config` to reconfigure a ProxySG. (B#50382a, B#51418a)
- ❑ Enabling Bandwidth Management can add a small amount of latency (less than 10 millisecond) to traffic traversing the ProxySG. (B#55271a)
- ❑ Bandwidth Management hierarchy might need to be re-configured when copying the output of `show config` to reconfigure the ProxySG. (B#56140a)

## Branch Deployment

Before deploying ProxySG appliances for branch office acceleration through SOCKS compression, review the following:

- ❑ Enable SOCKS Proxy on Concentrator Proxy to compress Outlook/CIFS traffic between Branch Proxies and the Concentrator Proxy.
- ❑ Enable HTTP Proxy on Concentrator Proxy to compress HTTP responses Branch Proxies.
- ❑ SOCKS Compression and HTTP Compression are CPU and memory-intensive functions.

- ❑ Do not use existing Gateway Proxy or Reverse Proxy as a Concentrator Proxy.
- ❑ SOCKS Compression and HTTP Compression can be simultaneously active on Concentrator Proxy with certain caveats listed below.
- ❑ Do not enable other functions that require large memory allocations on Concentrator Proxy, such as:
  - HTTPS termination/origination.
  - HTTP decompression.
  - Policy for page transforms, response data and apparent data type triggers.
- ❑ Do not enable other high CPU intensive applications, such as:
  - HTTPS termination/origination.
  - Spyware policy.
- ❑ Implement Page transforms and Spyware policies on the Gateway Proxy (*not* the Concentrator Proxy).
- ❑ Implement HTTPS termination/origination on the Reverse Proxy (*not* the Concentrator Proxy).
- ❑ The same Branch Proxy can be used for SOCKS Compression and other protocols, such as HTTP.
- ❑ Blue Coat recommends that the Branch Proxy use the Concentrator Proxy as the HTTP Proxy for forwarding HTTP traffic (not as SOCKS Proxy).
- ❑ The ProxySG does not support load balancing across SOCKS gateways.
- ❑ To compress Microsoft Outlook traffic, the ProxySG in the branch office must be in line as a bridge. Because of dynamic traffic, you cannot use an L4 switch or a WCCP router to intercept RPC services.
- ❑ Verify duplex settings are compatible in bridged deployments (in branch offices).
- ❑ Specifying the ports that intercept the CIFS/printing protocol: In a deployment where one group of CIFS/printing services listens on both ports 139 and 445 and another group of CIFS/printing services listens only on port 139, configure the branch ProxySG to only intercept port 139; do not configure to intercept both ports 139 and 445. Otherwise, the port-139-only services will break. This presents the limitation that when clients choose to use port 445, that content is not compressed because 445 traffic is not intercepted.

## Bridging

- ❑ When a ProxySG is deployed inline as a bridge, it intercepts traffic (such as HTTP Port 80 traffic) from both inside (Intranet) and outside (Internet). This makes the ProxySG an Open Proxy unless it is explicitly configured to deny connections from the outside. If this is not intended, you must create explicit policy rules to only proxy connection from the inside.
- ❑ The PCAP bridging filter does not work in software bridge implementation. (B#53918a)

## Certificates

- ❑ Expired Certificates: The setting `is certificate date range valid` that is displayed as part of the keyring and certificate summary information shows whether the certificate in question was valid when the ProxySG was upgraded to SGOS 4.2. This setting does not change in real time. Certificates that have expired can still have this setting display yes if they were valid during the upgrade to SGOS 4.2. (B#54363a)
- ❑ Client Certificates: If client certificate verification fails, a generic exception page is displayed that does not pinpoint the exact certificate error. For error details, see the event log. (B#55358a)

## Compression

- ❑ <The following content types are already recognized by Internet Explorer as compressed. Regardless of the user-agent, these types are not compressed by the ProxySG (B#44032a):

```
image/gif
image/jpeg
image/png
image/pjpeg
application/x-compressed
application/x-zip-compressed
application/x-gzip-compressed
application/futuresplash
application/x-rtsp-tunnelled
application/x-shockwave-flash
```

Additionally, the following (standard) content-types are not able to be compressed:

```
application/zip
application/x-gzip
application/pdf
audio
video
```

- ❑ Blue Coat recommends using `gzip` encoding (or allowing both `gzip` and `deflate`) when using HTTP compression, for the following reasons:
  - Servers return `deflate`-encoded content, but do not return an `Accept-encoding` header.
  - Deflate is discussed in two standards: RFC1950 and RFC1951. Most servers return RFC1951, while the HTTP/1.1 standard requires RFC1950.
  - IIS HTTPZIP plugin (older versions) returns `gzip` when asked for `deflate`. (This is treated by SGOS 4.x as an unsolicited response and passed through to the browser).
  - IIS HTTPZIP plugin (newer versions) returns `gzip` when asked for `deflate`, but claims it is `deflate`. This appears as corrupt data to browsers and the ProxySG.

## Content Filtering

- ❑ The renamed SmartFilter categories are hard-linked between old-name and new-name (example: `High Bandwidth` and `Media Downloads`), regardless if SmartFilter is the selected vendor.(B#50420a)
- ❑ Prevent DRTR rating requests for invalid domains. (B#75483a)

## Downloads

- ❑ Servers providing download for policy files, configuration, etc. must have header responses configured for sizes less than 8k bytes. (B#55278a)
- ❑ A registry error is written to the event log when you downgrade from SGOS 4.2.5.1 to SGOS 4.2.3.26 and you have an access log with an upload client of none. The workaround is to reboot the system. (B#86559a, SR 2-71519383)

## FTP

- ❑ An FTP proxy username cannot contain a space; if a username contains a space, the FTP proxy does not send the entire username to the authentication server. (B#53890a)
- ❑ If, after establishing an upload connection using FTP client, the connection is closed (for example, by rotating the remote file) without sending any data to the remote server, then the ProxySG creates a zero-byte file on the remote server. (B#54654a)
- ❑ FTP proxy authentication does not take £ (pound) symbol. (B#62386a)
- ❑ Invalid characters get appended to the FTP command ABOR. (B#58185a, 2-31124911)
- ❑ TFTP: Transferring a file using TFTP through a SOCKS connection may cause a restart (B#61258a).
- ❑

## Hardware

- ❑ You cannot check the environmental statistics for a 400 Series ProxySG appliance. In the Management Console, the Statistics > General > Environment panel does not display and in the CLI; the command `SGOS# show environmental` is invalid. (B#45188a)
- ❑ SG8000 Adapter Configuration: Configuration of services for Interface 1 might not be possible through the Management Console. Blue Coat recommends using the equivalent CLI commands instead.
- ❑ There is a remote chance the network interface is disabled after the duplex/speed mode is changed. The workaround is to change the mode again.
- ❑ If you have a ProxySG SG-400 series model, do not use NIC-0 at 10 Mb/sec or half duplex. It might hang, although you will still be able to ping the system. Instead, use NIC-1. (B#27765a)
- ❑ Disk replacement or removal can result in event or access log loss. Replacement or removal of drives that contain mirrored event or access log objects can result in loss of portions of the logs (B#59321a, B#61529a). As a workaround, if disk removal or replacement is necessary, do the following:
  - Take the system offline to ensure minimal traffic on the box.
  - Upload all access logs.
  - Save the event log
  - Replace or remove the disks.
  - Bring the system back online.

## Health Checks

- ❑ Health check names are limited to 31 characters. If using the Management Console, the characters *icap\_hc\_* are automatically added to the prefix of the health check name, making the useable number of characters even smaller. To use the full allotment of characters, use the CLI. (B#58082a)
- ❑ Health Check notification e-mails are sent depending upon the event log threshold. If the event log threshold is set to less than *Informational*, notification e-mails are not sent for Websense off-box or manually created health checks. (B#53917a)

## HTTPS

- ❑ When you open the Visual Policy Manager or Bandwidth Management pages in the Management Console through HTTPS, you might see a security information dialog warning about a mixture of secure and non-secure content. This is due to a link on the page that allows you to download the Java Virtual Machine from Sun's Web site. All communication with the ProxySG is encrypted and remains secure. Some versions of the Sun Java Virtual Machine might also be unable to share credentials with the browser, causing a dialog box to appear asking again for your username and password. In these cases, re-enter the same credentials that you used to first access the Proxy SG. (B#45449a)
- ❑ Creating HTTPS services on 255.255.255.255:443 can result in a service that cannot be deleted. This should not prevent the creation of other valid HTTPS services on the same port. (B#50384a)
- ❑ HTTPS Reverse Proxy: If a service for HTTPS reverse proxy is created on an IP:port, the same port cannot be used for creation of TCP tunnel services. However, if a TCP tunnel service is created on a specific port, an HTTPS reverse proxy service can be created on the same IP and port. (B#54377a)
- ❑ HTTPS Reverse Proxy: When an HTTPS reverse proxy is created on IP 255.255.255.255, it cannot be deleted. (B#54390a)

## ICAP

- ❑ When enabling RESPMOD, cached JPG files are not refreshed when a PNC header is received. (B#79404a, SR-2-44961061)
- ❑ Under certain configuration and load scenario, CPU consumption may be 10% higher than it was in SGOS 4.1.3. (B#55771a)
- ❑ If the ProxySG is sending patience text, an ICAP error occurs while scanning the content, and policy is configured to fail close or to deny for that ICAP error, the ProxySG might not send a 421 error code to the client and client connection might eventually time out. (B#55818a)
- ❑ If multiple clients request the same object within 10 seconds of completing a scan that had resulted in an ICAP error and the object was cached because of policy, the object might get re-scanned for subsequent requests, instead of using the previous scan result for the next 10 seconds. (B#55925a)
- ❑ If you try to save a download by right-clicking the link but that download resulted in a patience page, then the patience page response is saved rather than the actual contents of the download. (B#56061a)

- ❑ The "bytes transferred" value is not updated for an uncacheable virus-infected file when ICAP is configured. (B#55457a)

## Instant Messaging

- ❑ MSN: SG does not apply policy to MSN 8.0 offline messages. (B#64591a)
- ❑ Yahoo IM file transfer fails when it uses HTTP to transfer files. (B#64465a)
- ❑ MSN-IM: Version 7.5 - Messaging may not work when Reflection is enabled. (B#55642a)
- ❑ Video and audio are not supported with any of the Instant Message protocols: MSN, Yahoo!, AOL. (B#52283a)
- ❑ AOL-IM: File transfer may not work as expected if the file name contains Chinese characters. (B#55126a)
- ❑ The ProxySG sends *alert* messages to the user in-band or out-of-band as specified by the configuration variable *exceptions*. However, alert messages for those IM activities such as file transfer (that use direct connections), are always sent out-of-band. (B#54481a)
- ❑ Connection through SOCKS V5 from a Windows2K desktop might fail when using MSN 7.0. (B#54009a)
- ❑ Proxy authentication doesn't work when logging in with MSN 7.5 client. (B#58904a)
- ❑ Yahoo 7.0: The file transfer requests going through the Yahoo! file server now are sent as http requests (HEAD/GET/POST). If you have a Yahoo client explicitly proxied (SOCKS/HTTP), the file transfer requests might not go through the ProxySG even though all the traffic from the Yahoo client is going through the proxy.
- ❑ Yahoo Messenger version 7.0.2.120 cannot login through the HTTP proxy when the ProxySG is configured to authenticate users using an IWA realm and Yahoo Messenger uses HTTP/1.0 for its transaction. To force Yahoo Messenger to use HTTP/1.1, set the Internet options in your browser to use HTTP 1.1 for proxy connections.(B#59874a)
- ❑ SOCKS authentication might not work as expected for Windows MSN-IM clients. (B#55615a)
- ❑ AOL-IM: Messaging with IM Reflection enabled might not work if messaging with Chinese characters (B#55129a)
- ❑ AOL-IM: With IM reflection on, non-ascii messages might not be transferred correctly to the receiving clients. (B#61079)
- ❑ Logging into Yahoo IM transparently (such as through a ProxySG bridge) can cause a client-side pop-up error message. This does not affect IM proxy functionality. (B#55955a)
- ❑ MSN: File transfers using HTTP proxy mail fail for large (>1MByte) files. (B#55640a)
- ❑ MSN: im.reflection does not work when three users chat in conference room. (B#64152a)
- ❑ MSN 8: sharing folders (MS Live) is not supported. (B#63770a)

## JRE 1.5 (5.0)

- ❑ If you experience system slowness issues with JRE 1.5, enter the following command from the `(config)` prompt:

```
SGOS# (config) netbios
SGOS# (config netbios) nbstat responder enable
```

(B#48920a)

- ❑ JRE 1.5 on Windows XP; Visual Policy Manager: In the All Objects dialog, when you select New, an unselectable field appears in the menu shown below Combined Objects.

## Licensing

If the system clock has the date 2013-07-06 or later, the license fails to install. (B#87592a, SR 2-76625491)

## Management Console

The Management Console might occasionally crash under the following conditions: You have upgraded or rebooted the ProxySG to a new image and have refreshed the browser. The workaround to prevent crashing is to close the browser during a ProxySG upgrade or reboot and launch the browser again only after the new image is ready. (B#55302a)

## Passive FTP Exception

For a configuration that uses Passive FTP through SOCKS, the above policy might not avoid the 30-second delay caused by protocol detection. The reason for this is because a separate DATA connection is created to transfer data and the port used on this DATA connection is random, and policy cannot be enforced. If this configuration is necessary, there are two options:

- ❑ Generate a white list of FTP servers that can be accessed. For example:

```
<proxy>
  client.protocol=socks condition=ftp_destination
  detect_protocol(none)
  define_condition ftp_destination
  url.address = IP_address
  url.address = IP_address
  end condition
```

- ❑ Implement policy to disable protocol detection for all SOCKS tunnels. For example:

```
<proxy>
  client.protocol=socks detect_protocol(none)
```

## Patience Page

- ❑ If `always-verify` is set, whether through CLI or through policy, the Patience Page goes into a loop. (B#58025a)
- ❑ If you make a change to the text field of the Patience Page and apply the change, the help text field might later display as very small. To solve this problem, click in the middle of the unusable text area so that the cursor is placed in the text area. Then click on enter to increase the number of lines to more than nine and apply these changes. (B#75540a)

## Peer to Peer

- ❑ The following peer-to-peer (P2P) clients cannot connect to the ProxySG using SOCKS V5 authentication (B#45540a):

- eMule Version 0.43b
  - KazaaPlus 2.6.4
- ❑ When a CONNECT is issued with a Content-Length header, the ProxySG attempts to parse the request entity body to determine whether it is from a known P2P agent. If no data is received within 30 seconds, the ProxySG aborts the transaction. Because this client is broken and is sending an invalid content-length header, the ProxySG stalls on this request. Use the following CLI command to enable tolerant-request-parsing:
- ```
#(config) http tolerant-request-parsing
```

## Policy

- ❑ VPM: Use the header user-agent in the object Request Header (source) to specify any missing user agents in the User Agent (source) object. (9B#56110a)
- ❑ VPM: When creating a time object, if you enable some of the options, the tabbing sequence does not select the newly enabled fields. It simply runs through all the enable checkboxes, through the buttons, and back to the top. For example, if you enable Only Between The Following Times of the Day and tab through all the options, the From and To fields do not get selected. (B#48267a)
- ❑ VPM: The progress bar in the Management Console VPM applet is editable, but does not result in any action. (B#48694a)
- ❑ VPM: After declaring patience on an object, if the server connection is reset, the object re-fetches and re-scans, causing repeats. (B#50386a)
- ❑ VPM: Category-URLs should not contain the equal (=) character. If a user enters category=name as part of URLs of a category, it is treated as subcategory. (B#50420a)
- ❑ VPM: If a category exists under more than one parent, the generated policy also contains repetitive entries of the same category; this does not present any complications. (B#50424a)
- ❑ VPM: Cutting and pasting of a category does not work as expected. Once policy is installed, the effect of an earlier cut and paste disappears. (B#49036a)
- ❑ Content Filtering: The test-url command with an embedded '&' might create extra newlines in the output. (B#51298a)
- ❑ Policy trace: Policy trace doesn't display custom header. (B#63168a, SR 2-28745607)

## Protocol Detection

A 30-second delay occurs when the ProxySG tunnels any protocol where the server *speaks first*. Examples of these protocols are FTP, SMTP, POP3, and IMAP. Currently, the ProxySG does not support protocol detection for such protocols; therefore, the delay occurs in all three types of tunnels:

- ❑ TCP tunnel
- ❑ SOCKS tunnel
- ❑ HTTP CONNECT tunnel

The workaround for this is to define policy that disables the protocol detection for all tunnels where the tunneled protocol is the one where the server speaks first. The following is an example of such policy.

```
<Proxy>
;Rule 1
  condition=server_speaks_first_port_list condition=tunneling_protocol
  detect_protocol(none)
; Definitions
  define condition server_speaks_first_port_list
    url.port=25
    url.port=143
    url.port=21
    url.port=110
  end

  define condition tunneling_protocol
    client.protocol=http
    client.protocol=tcp
    client.protocol=socks
  end
```

**Notes:**

- ❑ The destination-based condition in Rule-1 must be included to avoid a security issue.
- ❑ If a server is listening on a non-default port, you must add a line in with that port (for this example, in the server\_speaks\_first\_port\_list condition).

## RADIUS

- ❑ When using Challenge/Response (such as SecurID or SafeWord tokens), the best user experience is seen when using an authentication mode with Forms (Form Cookie Redirect being the optimal). Standard browser authentication dialogs can be used; however, there are some limitations.
- ❑ Firefox 1.0.x does not display the realm string for proxy authentication dialogs. This means that it cannot be used for Challenge/Response authentication when an explicit proxy mode is used. Firefox 1.5 fixes this issue. Using forms avoids this issue.
- ❑ Internet Explorer stops displaying authentication dialogs after three consecutive "failed" attempts. This is an issue when changing a PIN for RSA SecurID. The process is usually four steps, which means that the last step is missed when using standard authentication with Internet Explorer. Using forms avoids this issue.

## RIP

- ❑ The route entries from RIP cannot be automatically restored by the ProxySG if the Ethernet cable is disconnected and reconnected. When an interface on the system is disconnected, the ProxySG flushes all the routing information related to that interface, including the information from RIP. After the interface is reconnected, the ProxySG cannot restore the information from RIP. (B#55298a)
- ❑ Default route in "show rip route" is 0.0.0.0/32 instead of 0.0.0.0/0. (B#80241a, SR 2-46609131)

## RTSP

- ❑ The RTSP proxy might sometimes close connections when using UDP or multicast transports in the new Helix series of players (such as Real Player). The workaround is to use the TCP or HTTP transport. (B#83620a)

- ❑ Page Fault at 0x45 in Process "tcpip" in "tcpip.dll" at .text+0x13FC5 using RTSP. Workaround: Create a new log format for the RTSP service which does not contain the "s-ip" symbol. (B#63181a, SRs 2-29386641, 2-31116681, 2-38642746, 2-40629092)

## SSH

If you execute a number of commands in quick succession using the command line execution feature of ssh, the SSH client might terminate the connection before displaying the output of all the commands. For example:

```
ssh -T -l user -i user_private_key proxysg_IP test
```

where file test contains a list of CLI commands. This might not give the output of all the commands listed in file test. (B#48912a)

## SSL Proxy

- ❑ If you configure IIS servers to support only SSLv2 and TLSv1 protocols, and you configure the client browser to support only SSLv2 and SSLv3 protocols, you might see the following error messages when making a HTTPS request to the IIS server from the browser:

```
Internet Explorer: Page cannot be displayed
Firefox: Firefox received a message with Incorrect message
authentication code.
```

This is an IIS issue, not a ProxySG issue. (B#54751a)

- ❑ Early denials for SSL/HTTPS traffic are no longer possible when the SSL proxy is used in transparent deployments. (Note that this does not affect HTTPS Reverse Proxy deployments.) For example:

```
<proxy>
DENY server_url.host=abc.com
```

In this case, a request for https://abc.com is expected to be denied before contacting the server. But in SGOS 4.2.2 with the above policy, the SSL proxy contacts the server and fetches the certificate before denying a request to https://abc.com. (B#59431a)

- ❑ Forwarding discrepancies can occur with the SSL proxy if URL rewrites that change the URL host are present because URL rewrites no longer apply until the SSL proxy contacts the server and makes the intercept versus tunnel decision. (Note that this does not affect HTTPS Reverse Proxy deployments.) For example, assuming that a URL rewrite present in policy that rewrites hostname abc.com to def.com:

- The SSL proxy contacts abc.com and uses the site's certificate contents to make the intercept vs. tunnel decision. URL rewrites no longer apply when SSL Proxy contacts the server for making the intercept vs. tunnel decision.
- After the intercept vs. tunnel decision is made, URL rewrites do apply when forwarding user requests to the server. So with the URL rewrite in the example, user data is sent to def.com even though the decision to intercept/tunnel was made by contacting abc.com.

The workaround is to use forwarding rules to ensure that def.com is contacted when the SSL proxy makes the tunnel vs. intercept decision as well. (B#59431a)

- ❑ Proxy Chaining: Authentication forwarding to parent proxy does not work on HTTPS. (B#60476a)

Assumptions:

- SG1 is using SG2 as the upstream HTTP Proxy.
- SG2 has authentication enabled.
- SG1 is used as an explicit proxy by user desktops .

In these cases HTTPS traffic breaks because the 407 challenge from the upstream proxy is not correctly forwarded to the client in case of HTTPS. When the protocol recognizer is enabled on SG1, it sends 200 OK response to HTTP CONNECT method before contacting SG2.

Workaround: Disable protocol detection on SG1 for HTTP CONNECT.

```
<proxy>  
  http.method=CONNECT detect_protocol (none)
```

This also disables the SSL proxy functionality on SG1. However, SSL Proxy functionality can still be enabled on the upstream proxy (SG2), allowing the user to take advantage of the SSL proxy while making authentication work correctly. (B#60476)

## Statistics

- ❑ Policy /Statistics sometimes report active FTP sessions when there are no active FTP sessions. FTP /Statistics properly reports no active sessions in such cases. This inconsistency is a known issue.(B#48565a)
- ❑ SSL Statistics: The field "Currently active sessions" under SSL Origination on the SSL/ Statistics page displays an invalid counter value. (B#55356a)
- ❑ Admin Monitoring: Read-only Admin cannot access some statistics pages. (B#56142a)

## Streaming

- ❑ MMS traffic forwarded to a socks gateway is not SOCKSified. (B#62303a)

## Telnet Client

Blue Coat does not support the use of non-ASCII characters with the standard Windows Telnet client, since it does not support UTF-8. Note that the Telnet client must be configured to send and receive UTF-8. (B#56353a)

## Windows Updates

- ❑ A Windows update for either Windows 5 or 6 might fail if you access the Windows Update Version 5 or Version 6 Web site through authenticating proxy servers, such as the ProxySG. The message you see is similar to the following:

**Windows Update has encountered an error and cannot display the requested page.**

You might also see [Error number: 0x80072F78] in the upper-right corner of the Web page.

To correct this situation, you must upgrade to SGOS 4.1.3 or higher; in addition, you must apply the fix found in the Microsoft knowledge base. For more information, go to: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;885819>

- ❑ The Windows update does not work when the SSL Proxy is enabled. This is because the Windows update client does not trust the emulated certificate presented by the SSL Proxy. The workaround is to tunnel the `http://update.microsoft.com/windowsupdate` Website.

## Support

Direct support questions regarding this release to <http://www.bluecoat.com/support/contact.html>.

## Known Issues with Management Console and VPM Design Changes

### Management Console

- ❑ Duplicate aliases are not caught for forwarding hosts and socks-gateways if configured thru `installable-list`. (B#64616a)
- ❑ Disk status is not updated when it is taken offline from the Management Console. If disk status does not update after taking the disk off-line, switch tab selection and switch back. (B#64617a)
- ❑ A weak password can be set on the console without confirmation from the administrator.
- ❑ Policy Files -> Install from Text Editor does not allow resizing. (B#64625)
- ❑ If you are in the **Configuration > Services > Ports New/Edit** dialog and use the up and down arrows to navigate through the proxies drop-down list, there might be graphic corruption within the dialog. Select the proxy services with the mouse cursor to avoid graphic corruption (B#62218).
- ❑ Clicking **Maintenance > General > Restore** does a `restore-defaults keep-console` operation instead of `restore-defaults factory-default` operation as in previous releases. This means that the following settings are maintained:
  - IP addresses, including default gateway and bridging, except for virtual IP addresses).
  - Settings for all consoles.
  - Ethernet maximum transmission unit (MTU) size.
  - TCP round trip time.
  - Static routes table information.To do a `restore-defaults factory-defaults` operation, which clears everything but trial period information and the last five installed appliance systems, use the CLI. (B#75825a)
- ❑ DER encoded CRLs can no longer be uploaded onto the SG using the Local File option. To download a DER encoded CRL, use the Remote URL option instead. (B#64611a)
- ❑ The Management Console depends on the CLI for some of its data validation. As a result, some invalid data or invalid operations are not detected until the changes are applied to the SG. The errors are then displayed in a dialog in the Management Console.

## VPM

- ❑ Changes made to the "Comment" column would not prompt "Unsaved changes" when closing. (B#64627a)
- ❑ Cutting and pasting categories fails to update parent pointers. (B#64629a)

Copyright© 1999-2007 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxyAV™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, RA Connector™, RA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT SYSTEMS, INC., ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.