



Blue Coat SGOS 5.4.x Release Notes

Version: SGOS 5.4.12.6

BCAAA Version 130

Release Date: 03/11/2013

Document Revision: 2.03 on 03/08/2013

Important Notes About SGOS 5.4.x

Before beginning the upgrade process, please read the following information:

- ❑ If you are using the Blue Coat Authentication and Authorization Agent (BCAAA), SGOS 5.4.x requires BCAA version 130 (located on the 5.4.x BlueTouch Online download page). Even if you are already running version 130, be sure to upgrade to the BCAA version associated with SGOS 5.4.x because it contains a security vulnerability fix. You must upgrade to BCAA version 130 before upgrading to SGOS 5.4.x. Do not upgrade SGOS unless you have first installed the compatible BCAA version. Refer to the following documents for more information:
 - The BCAA Read me for BCAA sizing requirements. This Read me is posted with the BCAA version on the BTO download portal.
 - The Blue Coat SGOS 5.4.x Upgrade/Downgrade Guide for instructions to upgrade or downgrade BCAA.
- ❑ The JRE version required to run the Management Console has changed. JRE 1.4.x is no longer supported. For SGOS 5.4.x, the earliest supported JRE is 1.5.0_15. See "[Java Runtime Environment \(JRE\) Information](#)" on page 4.
- ❑ This release introduces the Open ADN feature. With Open ADN, an unmanaged ADN node that is running SGOS 5.4.x cannot form tunnel connections to a 5.3 node or to any closed 5.4 ADN node. For information on Open ADN, see "[Open ADN](#)" on page 117.

Product Documentation

Access the 5.4.x product documentation on BlueTouch Online:

<https://bto.bluecoat.com/documentation/pubs/view/SGOS%205.4.x>

Support

Frequently asked questions and more information about this release can be found in the Knowledge Base:

<https://kb.bluecoat.com>

Direct support questions regarding this release to:

<http://www.bluecoat.com/support/contact.html>

For questions or comments related directly to these Release Notes, send an e-mail to:

documentation.inbox@bluecoat.com

Upgrade Prerequisites

To upgrade to this release, you must first determine if your hardware platform is supported, and whether you can upgrade directly or must upgrade through an interim release. You must also familiarize yourself with potential upgrade/downgrade issues.

Before installing or upgrading to SGOS 5.4.x, do the following:

1. Optional—Learn about the changes and fixes in the SGOS version you are upgrading to. See "[Release Note Directory](#)" on page 5.
2. Determine if SGOS 5.4.x is supported on your hardware platform. See "[Supported ProxySG Appliance Platforms](#)" on page 2.
3. Determine your upgrade path. See "[Supported Upgrade Paths](#)" on page 3.
4. Upgrade your license, see "Upgrading Licenses"
5. Ensure that your browser has the correct JRE installed. See "[Java Runtime Environment \(JRE\) Information](#)" on page 4.

To proceed with the upgrade, refer to the *Blue Coat SGOS 5.4.x Upgrade/Downgrade Guide*:

<https://bto.bluecoat.com/documentation/pubs/view/SGOS%205.4.x>

Downgrade Issues

Proxy traffic stops on SG9000 appliances after downgrade to 5.3.3.30. It is necessary to perform a `restore-defaults` `factory-defaults` after the downgrade. (B#134363)

Supported ProxySG Appliance Platforms

All SGOS 5.x versions, including 5.4.x, require a minimum of 512 MB of memory. SGOS 5.4.x contains significant new functionality and upgrading might impact CPU usage; therefore, proper sizing is critical. If the peak CPU utilization on your system exceeds 65 percent on SG810 and lower models, or 70 percent on SG8100 models running SGOS 4.2.8.6, contact your Blue Coat sales representative or Blue Coat reseller agent before upgrading to SGOS 5.4.x

Hardware: The following ProxySG models can be upgraded to SGOS 5.4.x:

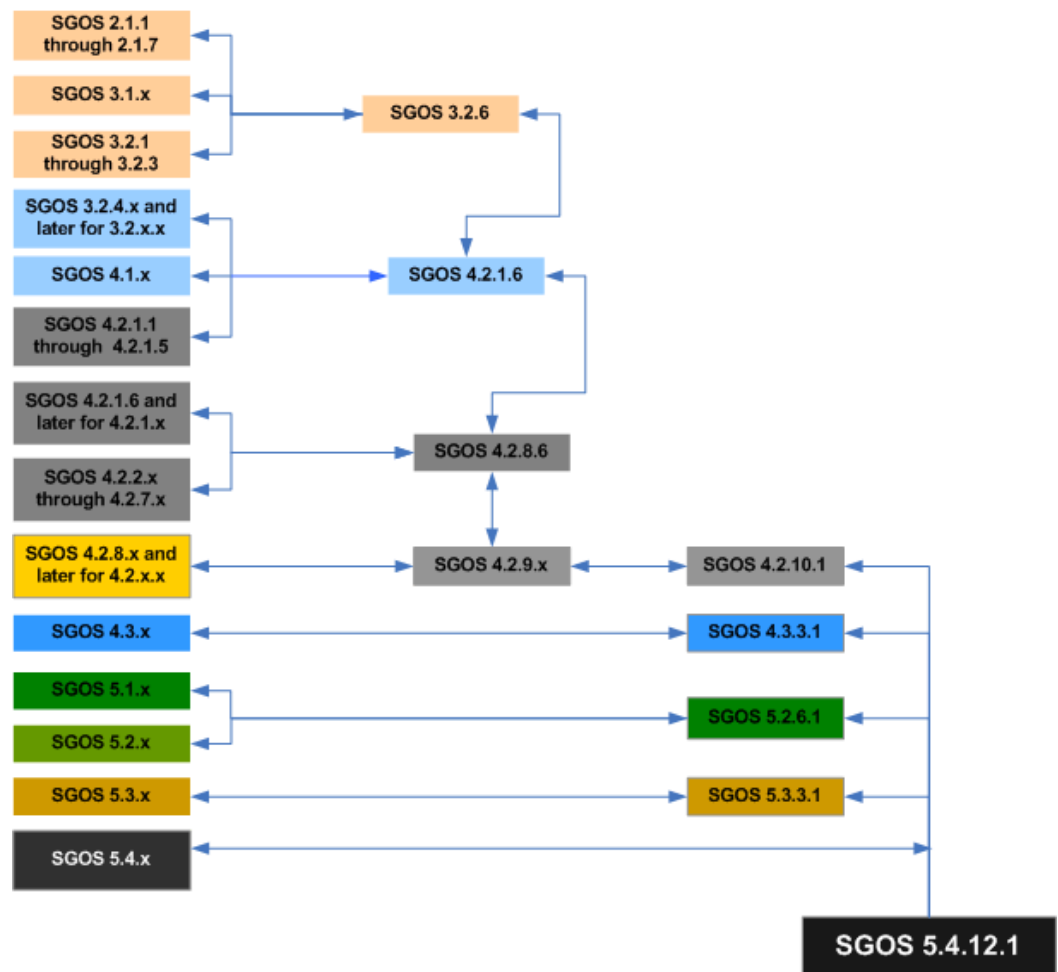
- ❑ SG200-x (except 200-A)
- ❑ SG210

- ❑ SG510
- ❑ SG810
- ❑ SG8100
- ❑ SG9000 (Except 9000-30 and 9000-40. 9000-20B model only supports 5.4.10.1 and later.)

Older ProxySG appliance models 800, 5xx, and 4xx cannot be upgraded to this release. In addition, 256 MB RAM systems, like the SG200-A, cannot be upgraded to SGOS 5.4.x. To upgrade the hardware to a newer model, contact your Blue Coat sales representative or Blue Coat reseller agent.

Supported Upgrade Paths

The ProxySG appliance must be running SGOS 4.2.10.1, 4.3.4.1, SGOS 5.2.6.1, SGOS 5.3.3.1, 5.4.1.x through 5.4.11.x. before directly upgrading to SGOS 5.4.12.x.



Upgrading Licenses

The ProxySG appliance automatically checks for license updates upon reboot or once daily for a month before the currently installed license expires. By default, automatic license check is enabled, that is the **Use Auto-Update** button is selected in the **Maintenance > Licensing > Install** tab.

Use the steps below to upgrade your license— from SGOS 4.x to 5.x license or from the MACH5 edition license to the Proxy Edition license, as applicable.

To upgrade the license:

In the Management Console, select **Maintenance > Licensing > Install**. In the **License Key Automatic Installation** field perform one of the following:

- If you previously used the Management Console to retrieve an SGOS license and the **Use Auto-Update** button is enabled, click **Update**.
- If you did not previously use the Management Console to retrieve an SGOS license and you have a valid WebPower/BlueTouch account login (for the appliance to be upgraded), click **Retrieve**. The Request License Key dialog displays. Enter your BlueTouch credentials and click **Send Request**.

The Blue Coat license server:

- Receives the request;
- Automatically upgrades the SGOS 4.x license to the SGOS 5.x license; and
- Returns the new license to the ProxySG appliance.

To verify the SGOS 5.x license has been loaded, click the **View** tab and look for SGOS 5.x components.

Alternate Methods

- If you cannot directly access the Internet, contact Blue Coat Support Services for assistance. You are asked to provide the hardware serial numbers of the appliances to be upgraded and account details, such as contact name, e-mail address, and BlueTouch Online account name. If you do not have a BlueTouch Online account or if you have lost the password, see <http://www.bluecoat.com/contact/customer-support> for details.

Java Runtime Environment (JRE) Information

To run the SGOS 5.4 Management Console, you must install the [Sun Java JRE](#) version 1.5.0_15 or later, including 1.6 (except for 1.6_05, which causes VPM on-line help problems).

JRE 1.4.x is no longer supported. For SGOS 5.4, the earliest supported JRE is 1.5.0_15.

You have the following options:

- ☐ Get a supported JRE from [Sun](#) and install it yourself.
- ☐ When you start the ProxySG Management Console for the first time after upgrading to SGOS 5.4 or later and your currently installed JRE is earlier than 1.5.0_15, your Web browser attempts to download a more current JRE.

Following are details about Internet Explorer and Firefox:

- *(Recommended.)* Use Internet Explorer because it attempts to download JRE 1.5.0_15. Follow the prompts on your screen to download and install this JRE.
- Firefox attempts to install the latest JRE, which might not be compatible with the Management Console.

Release Note Directory

These release notes present information by each release in the SGOS 5.4.x software line. Each section provides feature descriptions, fixes and known issues.

- ❑ [Section A: "SGOS 5.4.12.6 build 108549" on page 6](#)
- ❑ [Section B: "SGOS 5.4.12.1 build 93329" on page 9](#)
- ❑ [Section C: "SGOS 5.4.11.1 build 79058" on page 12](#)
- ❑ [Section D: "SGOS 5.4.10.1 build 78212" on page 14](#)
- ❑ [Section E: "SGOS 5.4.9.1, build 76593" on page 23](#)
- ❑ [Section F: "SGOS 5.4.8.1, build 73295" on page 31](#)
- ❑ [Section G: "SGOS 5.4.7.1, build 65467" on page 41](#)
- ❑ [Section H: "SGOS 5.4.6.1, build 54128" on page 47](#)
- ❑ [Section I: "SGOS 5.4.5.1, build 51300" on page 53](#)
- ❑ [Section J: "SGOS 5.4.4.1, build 45872" on page 61](#)
- ❑ [Section K: "SGOS 5.4.3.7, build 45225" on page 66](#)
- ❑ [Section L: "SGOS 5.4.3.3, build 44321" on page 73](#)
- ❑ [Section M: "SGOS 5.4.3.2, build 44285" on page 77](#)
- ❑ [Section N: "SGOS 5.4.3.1, build 44023" on page 78](#)
- ❑ [Section O: "SGOS 5.4.2.11, build 42967" on page 86](#)
- ❑ [Section P: "SGOS 5.4.2.2, build 41580" on page 89](#)
- ❑ [Section Q: "SGOS 5.4.2.1, build 40763" on page 91](#)
- ❑ [Section R: "SGOS 5.4.1.12, build 40038" on page 103](#)
- ❑ [Section S: "SGOS 5.4.1.3, build 38863" on page 108](#)
- ❑ [Section T: "SGOS 5.4.1.1, build 38147" on page 116](#)
- ❑ [Section U: "SGOS 5.4.x — Limitations and Support for Other Products" on page 138—Provides the limitations for SGOS 5.4.x and a list of all supported clients, browsers, and products that work together with a ProxySG running SGOS 5.4.x.](#)

Section A: SGOS 5.4.12.6 build 108549

Section A: SGOS 5.4.12.6 build 108549

Release Date: 03/11/2013, build 108549

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.12.6 Contents

- ❑ "Security Fixes in SGOS 5.4.12.6" on page 6
- ❑ "Fixed Issues in SGOS 5.4.12.6" on page 6
- ❑ "Known Issues in SGOS 5.4.12.6" on page 7

Security Fixes in SGOS 5.4.12.6

- ❑ Fixed OpenSSL ASN1 BIO vulnerability (CVE-2012-2110 and CVE-2012-2131).
For more information see:
Knowledge Base Article
https://kb.bluecoat.com/index?page=content&id=SA70&cat=SGOS_5
(B#176493, SR 2-528961432 ,2-529026902)

Fixed Issues in SGOS 5.4.12.6

The following issues were fixed in this release.

Authentication

- ❑ The BCAA service was missing some Windows logon sessions for Windows Single Sign-On (SSO). (B#179329, SR 2-49102941, 2-498843282)

Cache Engine

- ❑ An internal error caused a page fault in process HTTP CW C329CEC0 in the ce_admin.dll file. (B#184382)
- ❑ An internal read error on an object caused a software restart issue at 0x40021 (CEA_REFERENCE_COUNT_ZERO_ON_BLOCK_CHANGE) .(B#185254)
- ❑ RAM Cache and UMBC management was not functioning correctly under the traffic load. (B#172391)

FTP Proxy

- ❑ The ProxySG appliance's memory usage increased when FTP objects ICAP were scanned and cached. (B#181364)

Section A: SGOS 5.4.12.6 build 108549

Health Checks

- ❑ The DRTR server did not failover even though the DRTR service sent back a `non-ok` response. for example: 403 or 503. (B#184174, SR 2-510248942)

HTTP Proxy

- ❑ A page fault was caused at `0x5d92e000` in process `HTTP_CW_BF26DEC0` within the `shared_dll.dll` file. The page fault occurred when encoded characters were in different segments of a message. (B#180515, SR 2-500444009)

MAPI_Proxy

- ❑ Logging into a Windows Domain was delayed when EPMapper was enabled. (B#179781, SR 2-492722232)

Policy

- ❑ The transformation of relative URLs starting with the string “`../`” was performing incorrectly. (B#181304, SR 2-505865972)

TCP/IP and General_Networking

- ❑ The ProxySG appliance returned `SYN-ACK` packets from the wrong VLAN interface when the incoming `SYN` packet had a `non-0` VLAN priority. (B#175015, SR 2-456368272, 2-485710701)

Known Issues in SGOS 5.4.12.6

Authentication

- ❑ IBM TDS password expired response is not used by the ProxySG appliance; therefore, no exception page is generated in the case of an AD authentication failure. (B#140546, SR 2-299103242)
- ❑ The BCAA service occasionally returns a `Too many users--won't work` error when one user logs out of a machine and another user logs in. This error occurs when the incorrect Win SSO info is provided by a Windows API and used by the ProxySG appliance. (B#141759, SR 2-291631132)
- ❑ IWA realms are displayed as a possible choice when configuring the attribute object in VPM; however, only RADIUS and LDAP are valid realms. (B#182532, SR 2-517171759)

CLI_Consoles

- ❑ When the time/date are incorrect on the ProxySG appliance, the archived configuration file `archconf.txt` cannot be opened; resulting in the following error message: `Could not open temporary_file`. (B#184421, SR 2-537478202)

Section A: SGOS 5.4.12.6 build 108549

FTP_Proxy

- ❑ Processing an explicit FTP proxy request, and forcing TYPE A (ASCII) in your FTP client breaks causes 0D0A1 resulting in line breaks changing to 0A. (B#158333, SR 2-361254152)

Section B: SGOS 5.4.12.1 build 93329

Section B: SGOS 5.4.12.1 build 93329

Release Date: 09/18/2012, build 93329

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.12.1 Contents

- ❑ "New in SGOS 5.4.12.1" on page 9
- ❑ "Security Fixes in SGOS 5.4.12.1" on page 9
- ❑ "Fixed Issues in SGOS 5.4.12.1" on page 9

New in SGOS 5.4.12.1

This release contains new licensing behavior.

Licensing

SGOS 5.4.12.1 and higher releases contain the updated licensing subsystem referenced in Technical Field Alert 109. This important upgrade includes the new licensing validation certificate and is required for future seamless operation of the ProxySG appliance.

For more information, see:

Technical Field Alert

<https://kb.bluecoat.com/index?page=content&id=TFA109>

Knowledge Base Article

<https://kb.bluecoat.com/index?page=content&id=FAQ2197>

Security Fixes in SGOS 5.4.12.1

- ❑ Common Vulnerability and Exposures (CVE-2011-4576): bytes used in block cipher padding for SSL3.0 were not cleared.
- ❑ Common Vulnerability and Exposures (CVE-2011-4619) Provisioning the ProxySG appliance with an SGC certificate left it vulnerable to a DoS attack if the attacker attempts to restart a session. This was applicable for management sessions and reverse proxy scenarios.

Fixed Issues in SGOS 5.4.12.1

The following issues were fixed in this release.

Authentication

- ❑ SGOS > BCAA > IWA did not ignore the user name: **NT AUTHORITY\ANONYMOUS LOGON**. The issue occurred because of a new implementation of active directory under Windows 2008. (B#173788)

Section B: SGOS 5.4.12.1 build 93329

- ❑ The LDAP directory returned an invalid UTF8 string, which in turn caused a Page Fault at 0x53fd8c2b in process "authenticator" in "shared_dll.dll". (B#165640, SR 2-393548022, 2-414334022)
- ❑ Defining a large authentication policy for users caused a software restart in process "PDW t=56823484 for=303EFC0" in "authenticator.dll". (B#172302, SR 2-432371432, 2-437937032)
- ❑ The logout action was inconsistent if authentication and logout actions were contained in the same transaction. (B#180078, SR 2-495512802)

Caching

- ❑ Software restart at 0x40042 in Process "Cache Administrator" in "kernel_shim.dll". Before this fix, it was necessary to re initialize the drives to get back to a clean state. (B#177185, SR 2-476494262)
- ❑ HTTP workers maxed out as a result of a disk read issue, which caused some connectivity problems. (B#174190, SR 2-442891731)
- ❑ When a connection closed while processing a multi-range request for a truncated object, it caused a software restart in process "CEA Cache Administrator" at .text+0x0.(B#174251)

CIFS Proxy

- ❑ Connection shutdowns caused page fault at linear address: 0x10 in process "CIFS::Worker: Connection 25690 (running)" in "cifs.dll" at .text+0x6d797. (B#176033, SR 2-466169962)

Content Filtering

- ❑ Smartfilter database download performed incorrectly when incremental updates were available. (B#175150, SR 2-457105242, 2-457212940, 2-457452432)
- ❑ You Tube videos were not categorized by WebPulse when the first request was initiated. The ProxySG returned **none** for such a request. (B#171152, SR 2-407995641, 2-441187871, 2-462811644)
- ❑ The Blue Coat Web Filter (BCWF) database did not return **email** category when a request with <https://securemail.bankofamerica.com> was submitted. (B#173414, SR 2-438827422)

Health Checking

- ❑ The user-defined composite health check of the forwarding host did not properly reflect component health checks. (B#174593, SR 2-441908893)

Section B: SGOS 5.4.12.1 build 93329

HTTP Proxy

- ❑ The ProxySG appliance no longer treats URLs starting with encoded forward slashes as relative URLs when transforming HTML pages. This caused server errors (code 500) to be sent back when transforming HTML pages. (B#177827, SR 2-477456472, 2-480774860)
- ❑ During file download, the ProxySG appliance displays a content-encoding error exception page if policy content decoding does not take place. With the fix, the ProxySG displays an exception page during content decoding. (B#171726, SR 2-418541804)
- ❑ Software restart (HTTP proxy and ICAP) at 0x40 in Process "HTTP SW B8098EC0 for B80DFEC0" in "ce_admin.dll" when ICAP was used. (B#173045, SR 2-435824822)
- ❑ TCP port reuse defined by `http.client.persistence(preserve)` policy did not apply in transparent deployment when Reflect Client IP is configured and object caching is enabled. (B#177619, SR 2-480999304)

Networking

- ❑ The ProxySG appliance stopped processing requests periodically for about one minute during which no new TCP connections were accepted and then returned to normal afterwards. This issue occurred when the ProxySG got flooded with duplicate FINs after a dropped packet. (B#172586, SR 2-416469172)
- ❑ When Spanning Tree is involved, software bridge failover to the second bridge took too long to occur. (B#174826, SR 2-447276202)
- ❑ On multi-processor platforms, the packet capture time was off from system clock. (B#174508, SR 2-448908992, 2-449062202)
- ❑ The access log replacement variable used for IP address was reporting the incorrect IP addresses when the log was captured. (B#174279, SR 2-441683712)
- ❑ The ProxySG appliance statistic counter displays incorrect values for the number of TCP connections in `established` or `close_wait` state ("1.3.6.1.2.1.6.9" oid) after long, continues uptime. (B#175755, SR 2-463050832)

Security

- ❑ Common Vulnerability and Exposures (CVE-2011-4576): bytes used in block cipher padding for SSL3.0 were not cleared.

SSL

- ❑ Common Vulnerability and Exposures (CVE-2011-4619) Provisioning the ProxySG appliance with an SGC certificate left it vulnerable to a DoS attack if the attacker attempts to restart a session. This was applicable for management sessions and reverse proxy scenarios.

Section C: SGOS 5.4.11.1 build 79058

Section C: SGOS 5.4.11.1 build 79058

Release Date: 01/24/2012, build 79058

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.11.1 Contents

- ❑ "Fixed Issues in SGOS 5.4.11.1" on page 12
- ❑ "Known Issues in SGOS 5.4.11.1" on page 12

Fixed Issues in SGOS 5.4.11.1

The following issues were fixed in this release.

Authentication

- ❑ Fixed the issue in which origin-cookie-redirect was used thereby causing intermittent authentication loops. (B#170809, SR 2-410306732)

Cache Engine

- ❑ Fixed the issue in which process `Disk 63CA000` in `at.text+0x0` restarted unexpectedly due to improper memory management. (B#170535, SR 2-416914452)

Health Monitoring

- ❑ Fixed the issue in which alert notification sensor configurations were not ported to ProxySG 5.x when upgraded from ProxySG 4.x. (B# 161608, SR 2-379195522)

Policy

- ❑ Fixed the issue in which `Force Deny` rule on SOCKS stopped working after upgrading from 4.3.2.3 to 5.4.7.1. (B#165289, SR 2-389303962)

Known Issues in SGOS 5.4.11.1

Following are the known issues in this release.

Authentication

- ❑ The ProxySG appliance does not serve the authentication failure exception page when it receives the IBM TDS password expired response from the server. (B# 140546, 2-299103242)
- ❑ BCAA occasionally returns `Too many users--won't work` error message when one user logs out of the machine and another user logs in. This occurs due to incorrect Windows SSO information provided by a Windows API. (B#141759, 2-291631132)

Section C: SGOS 5.4.11.1 build 79058

FTP Proxy

- ❑ Processing an explicit FTP proxy request, and forcing `TYPE A` (ASCII) in FTP client breaks causes `0D0A` line breaks to appear as `0A` instead. (B#158333, 2-361254152)

HTTP Proxy

- ❑ Using the `http.response.apparent_data_type` policy causes a forced decompression even if the rule using the policy does not match. (B# 171726, SR 2-418541804)

Policy

- ❑ On occasion, the redirection of the PAC/WPAD file using policy fails with 400-invalid_request. When using PAC/WPAD redirects, it is recommended to use the policy gesture “request_redirect” instead of “redirect”. The “request_redirect” gesture was first introduced in SGOS 5.5.7.1. (B#145454, SR 2-307668872)

SSL Proxy

- ❑ Accessing `www.hipassplus.co.kr` URL from Opera10 or Firefox 3.5 displays the following error: `SSL Certificate Verification Error (ssl_failed)`. This error displays because the intermediate certificate, `SignKorea mCA` has critical extensions that are not supported by the ProxySG appliance - Certificate policies and Policy Constraint.

Workaround: Disable SSL proxy for these URLs or disable certificate validation in the SSL layer for the specific URLs. (B# 123410, 2-195383742).

Section D: SGOS 5.4.10.1 build 78212

Section D: SGOS 5.4.10.1 build 78212

Release Date: 12/12/2011, build 78212

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.10.1 Contents

- ❑ "Changes in SGOS 5.4.10.1" on page 9
- ❑ "Fixed Issues in SGOS 5.4.10.1" on page 9
- ❑ "Known Issues in 5.4.10.1" on page 15
- ❑ "Limitations in 5.4.10.1" on page 16

Changes in SGOS 5.4.10.1

This section describes important changes in SGOS 5.4.10.1

- ❑ Added support for 1TB HDD Seagate ST1000NM0001 and Toshiba MK1001TRKB drives for the ProxySG 9000-20B appliance. Please note that running a system with 1TB drives on an earlier SGOS 5.4 release will cause the system to restart.

Fixed Issues in SGOS 5.4.10.1

The following issues were fixed in this release.

FTP Proxy

- ❑ For Proxy-IP(explicit proxy) and Origin-IP(transparent proxy) authentication modes, FTP proxy did not perform proxy authentication. Authentication of client should be done using some other protocol (like HTTP). Once the client ip is authenticated, FTP proxy accepts further connection requests. As a result of this change, clients no longer needed to send proxy authentication credentials to FTP proxy. (B# 160779, 2-375028002)

HTTP Proxy

- ❑ The HTTP client did not specify `gzip`; the ProxySG appliance returned the uncompressed object client; it included chunked response with **size 0**, causing the client to improperly reset (RST) the connection. (B# 166131, 2-394829092)
- ❑ Fixed a communication conflict between malware scanning and access log transactions on the ProxySG appliance. The conflict forced some administrators to disable custom access log fields. (B# 169708, 2-415849782)
- ❑ The FTP over HTTP uploads did not complete for large file transfers if requested content length was over 2GB in size. (B# 170562, 2-416999632)

Section D: SGOS 5.4.10.1 build 78212

SSL Proxy

- ❑ Throughput degradation was observed on the ProxySG appliance during specific performance testing. This was seen when Spirent's client/server profiles are configured to fetch data from the server instead of serving it from cache. (B# 167265, 2-312821502, 2-326263472, 2-373846692, 2-392960442)

Socks Proxy

- ❑ The new port assignment algorithm did not work for a non-compliant server. (B# 170265, 2-410593782)

TCP/IP and General Networking

- ❑ The ProxySG appliance intermittently becomes unresponsive after high surges of traffic. (B# 158640, 2-364252707)
- ❑ When an IP address of an interface connected to their access logging network, all client traffic stopped working even though the client traffic passed through two different ProxySG appliance ports. (B# 168252, 2-404611512)

URL Filtering

- ❑ The URL categorization results appear to persist even after a database purge. (B# 167677, 2-402796703, 2-407566732)
- ❑ The Smartfilter is not matching domains with .xxx (Dot TripleX) domains. (B# 168321, 2-404128802)

Windows Media Proxy

- ❑ The Media Streams played via Microsoft Silverlight plug-in may fail to play. (B# 168212, 2-390134973)
- ❑ Windows Media over HTTP fails when the URL format is `http://<Proxy_SG_IP>/redirect?mms://<streaming_server>/<filename>.wmv`
The workaround is to use `http://<Proxy_SG_IP>/redirect?http://<URL>` instead of using `http://<Proxy_SG_IP>/redirect?mms://<URL>`
(B# 124346, SR 2-198319392)

Known Issues in 5.4.10.1

Blue Coat is aware of the following issues.

Authentication

- ❑ The IBM TDS password expired response is not used by the ProxySG appliance causing the ProxySG appliance to not serve an exception page during an Active Directory authentication failure. (B# 140546, 2-299103242)

Section D: SGOS 5.4.10.1 build 78212

- ❑ BCAA occasionally returns `Too many users--won't work` error message. This is occurring when one user logs out of the machine and another user logs in, due to the incorrect Windows SSO information provided by a Windows API used by the ProxySG appliance. (B# 141759, 2-291631132)

FTP Proxy

- ❑ Processing an explicit FTP proxy request, and forcing TYPE A (ASCII) in your FTP client breaks, causes 0D0A line breaks to start coming in as 0A instead. (B#158333, 2-361254152)

Policy

- ❑ The FORCE_DENY rule does not take effect (the connection is still allowed) after the upgrade from 4.3.2.3 to 5.4.7.1. (B# 165289, 2-389303962)

SSL_Proxy

- ❑ Accessing url `www.hipassplus.co.kr` from Opera10 or Firefox 3.5 fails with the expectation error, `SSL Certificate Verification Error (ssl_failed)`. This is caused by the intermediate certificate, `SignKorea mCA`, which has critical extensions that are not supported by the ProxySG appliance - Certificate policies and Policy Constraint. The Workaround is : Disable SSL proxy for these URLs or disable certificate validation in the SSL layer for the specific URLs. (B# 123410, 2-195383742)

Limitations in 5.4.10.1

Limitations are issues that Blue Coat is aware of but has no current plan to address. Often, these issues are related to third-party products or other network-specific issues.

ADN

- ❑ ADN connections are not re-established after downgrading from 5.5 to 5.4. The workaround is setting both Tunnel and Manager listening ports to the same port number, before or after downgrading to 5.4x, reset one of the listeners to a different port number. (B# 132461)
- ❑ CIFS uploads over ADN through a 1Gbps/4ms latent WAN link becomes slower over time. The workaround is to disable byte caching, this seems to resolve the issue; SGOS 5.4.3.7. (B#139477, 2-296178771)

Authentication

- ❑ VPM browsing of nested iPlanet referral groups results in errors. If these referral groups have sub-groups then those groups are not visible in VPM. (B#102008)
- ❑ Radius realm configuration refresh time `rejected-credential-refresh`. The functionality might not work if the refresh time configured is less than 10 seconds. (B# 107016)

Section D: SGOS 5.4.10.1 build 78212

- ❑ Health checks are not supported when using the Mach5 license. (B#110095)
- ❑ When attempting to access the **Session > Monitor > Lookup** page—If **Session Monitor** is enabled, and failover is switched from disabled to enabled or enabled to disabled, a `500 Read Timeout` error might occur. (B# 110139)
- ❑ The `New Pin` and `Query` forms are only supported (and only required) for specific versions of RSA ACE Server. (B# 126838, 2-209163742)
- ❑ There is high CPU use by the Kernel when policy contains numerous user conditions with LDAP authentication. (B# 130313, 2-224197931, 2-288000692)

CIFS_Proxy

- ❑ Versions of MacOS 10.5.6 clients and later are not able to connect to the CIFS Shares on EMC servers. (B# 109212)
- ❑ Visio failed to save the `.vsd` file to EMC shared folders filer through CIFS proxy over ADN, causing a file corruption error. To avoid this issue, the customer should apply the latest Visio service pack SP3 for MS Visio 2003. (B# 109420)
- ❑ The command `client.protocol=cifs reflect_ip(client)` needs to be defined under the Proxy Layer CLI Consoles. (B# 109532)

CLI Console

- ❑ The administrator Login and Read/Write events repeat every second in the eventlog. (B# 106455)
- ❑ The ProxySG appliance Management Console does not display a message when policy produces warnings. (B# 131079, 2-230908952)

Client Manager

- ❑ The allowable range for values in the **Configuration > ProxyClient > Web Filtering > Log** in the **Upload** settings is 0-99 hours, 0-59 minutes, 0-9999 Megabytes. If a value larger than this range is entered the extra digits are truncated without generating an error message. (B# 108048)
- ❑ Configuring the `exclude port` from a client acceleration configuration does not negate the `include-port` command. The `exclude port` command can not be disabled. (B# 108262)
- ❑ Unable to negate the `warn` setting in CLI. (B# 108264)

Hardware_Drivers

- ❑ 1Gigabit-half duplex setting is not a valid option 1Gb interfaces. (B# 108063)

Hardware_Diagnostic

- ❑ The ProxySG appliance 210 SGOS failed to detect the removal of the hardware bridge.(B# 119333)

Section D: SGOS 5.4.10.1 build 78212

Health_Monitoring

- ❑ The Health Monitor displays Critical CPU warning in the Event Log when downloading the SmartFilter database. (B# 129709, 2-222655015)

HTTP_Proxy

- ❑ Emule login using the ProxySG appliance as SOCKS5_Proxy is not supported. (B# 107875)
- ❑ A crash occurs caused by a Downloading a particular text file in reverse-proxy mode might cause the ProxySG appliance to come down. (SR#2-272652382 B#136612)
- ❑ If upgrading from 3.2.8 -> 5.3 onwards, clear the cache after upgrading to prevent a restart of the ProxySG appliance. (SWE: 0x80005 PFA: 0x0 Process "HTTP Waiting Room" in "kernel_shim.dll" at .text+0xCDC). (B# 118952, 2-186276332)
- ❑ A connection error occurs with the latest browser version in FireFox (3.0.10 and higher) and Internet Explorer 8 when accessing HTTPS websites through exception pages. Firefox 3 and IE 8 are not displaying the HTML exception pages sent from the proxy. (B# 121066, 2-190436632, 2-321761552, 2-337433032)
- ❑ For an HTTP request, if you have a URL rewrite policy, the URL search patterns must be described in lowercase. The ProxySG appliance always performs a case insensitive search. (B# 151206, 2-337857952)
- ❑ The Detect protocol option cannot be enabled in the URL rewrite (forward explicit proxy) deployment. (B# 170324, 2-411599464)

Initial_Configuration

- ❑ During the initial configuration setup, modifying the default gateway from an incorrect value to a valid value causes ping to fail if the change was not performed in Summary Mode. (B# 120422)

IPv6_Stack_and_IPv6_Proxies

- ❑ The CLI display command does not work using the link-local URL. (B# 120765)

Management_Console

- ❑ When the NTP server list is empty and the Acquire UTC time is executed, the message prompt incorrectly displays UTC time was successfully acquired when there is no NTP server. (B# 122335)
- ❑ An Out of memory error occurs when accessing the **Statistics->Proxy client->Details** page of the Management Console. (B# 122553)

Section D: SGOS 5.4.10.1 build 78212

MC_Legacy

- ❑ Manuals_and_User_Documentation: Management Console hangs on first access with Browser IE7 when Phishing filter is set to default, JRE - Java Plug-in 1.6.0_12 exception occurs. (B# 110413)
- ❑ Unable to set the February 29 date in the management console for leap years. (B# 119314)
- ❑ Any changes done with the WCCP configuration interface overwrites the Text Editor configuration. (B# 138424)

MC_Sky

- ❑ This is a very old version of FF which is no longer in use. (B# 109433)
- ❑ The CLI should display **NTP is enabled using Blue Coat's NTP servers** by default rather than **NTP enable**. (B# 131726. 2-233867949)
- ❑ You may see outdated information in the monitoring tab until the system performs a refresh. The monitoring tab refreshes once per minute. You are able to make a change in the configuration and quickly switch to the monitoring tab. (B#108407)

Multi Media Streaming

- ❑ Windows media player 10 can not access `HTTP://financialserv.edgeboss.net/wmedia/financialserv/committeemeeting010509.wvxin`, transparent proxy mode, mms server returns an `ErrorCode: (0x80070002)`. This is an isolated case caused by third party software unable to comprehend or be tolerant of the information sent between the ProxySG appliance and the Origin Content Server (OCS). (B# 109805)

Network Driver

- ❑ Changing the duplex on the ProxySG appliance SG8100 Cobra to HDX switches the speed from Gigabit to 100MB. (B# 108783)

Network_Security

- ❑ The `attack-detection server` command for limiting the number of server connection requests does not function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B# 109184)

Policy

- ❑ Pre-population of RealMedia content from web servers does not work. (B# 109339)
- ❑ The `deny.unauthorized (no)` property in CLI is configured within the `<proxy>` and `<ssl>` layers using the inline command `deny.unauthorized(no)`. (B#117482)

Section D: SGOS 5.4.10.1 build 78212

- ❑ The `ftp.server_connection (immediate)` property in CLI is configured within the `<proxy>` and `<cache>` layers using the inline commands `ftp.server_connection(immediate.` (B# 117484)
- ❑ When new Content Policy Language (CPL) gestures are introduced to a maintenance release, a system downgrade to an earlier release causes a policy compilation error message. This occurs because the new gesture is not supported in the previous version. (B# 122705)

Real_Media_Proxy

- ❑ Pre-population of RealMedia content from web servers does not work. (B# 109339)

SOCKS_Proxy

- ❑ Within the proxy chain environment the upstream proxy may display the `SOCKSHistory->ClntComp.Gain` calculation as 100% instead of 0%. (B# 107429)

SSL/TLS/and PKI

- ❑ When upgrading from 4.x/5.2 to 5.3/5.4, fields `x-cs-ocsp-error` and `x-rs-ocsp-error` are not part of the SSL format by default. These two fields must be added manually. (B# 107494)
- ❑ When disabling the **Verify peer** option in any HTTPS Access Log uploads, a certificate mismatch is still logged. (B# 107579)
- ❑ The SSL fails to initialize when `sslsv2` and `rc4-64-md5` are selected as the cipher in `ssl-client`. (B# 107847)
- ❑ The SSL Proxy does not support connecting to a server using DSA encryption; use `tcp-tunnel` proxy instead. (B# 109099)
- ❑ By default, hostname mismatch certificate validation does not occur unless the full SSL interception is enabled. (B# 119542, 2-184802562)
- ❑ Certain ciphers can not be set as the only cipher on HTTPS-Console. (B#138254)

TCP/IP_and_General_Networking

- ❑ When a hardware bridge is re-enabled to fail-open or fail-closed, the settings are maintained and the bridge may have a manual setting of 100/half speed and duplex on one side, and auto on the other. This can potentially cause performance problems. (B#108065)
- ❑ Interface 2:0 does not respond to incoming requests after upgrading to the ProxySG appliance 5.x. (B# 117121, 2-171069702)
- ❑ The ProxySG appliance platform SG210 does not support the configuration of Gigabit speed capacity on interface ports. (B# 120156)
- ❑ Configuring additional static routes entries prompts an inaccurately categorized warning message. (B# 120931)

Section D: SGOS 5.4.10.1 build 78212

- ❑ In a split-DNS, chained-proxy, environment, child proxy continues to send lookups to primary DNS server after health-check reports it down. A work-around was achieved by adding a condition `url.host.is_numeric=yes` in front of any condition. (B# 121987, 2-161499392)
- ❑ In SGOS 5.4x and higher, when an interface is down, the ProxySG appliance responds to an ARP Request with the MAC address of the receiving interface instead of the interface that the target IP address is configured on. To avoid this behavior, in the CLI enable: `tcp-ip-arp-strict-matching`. This command will ensure the proxy returns the MAC address of the interface where the target IP configured when an interface is down. (B# 122054, 2-192155074)
- ❑ TCP tunneled connections in `Established` state takes between 2-4 hours before they are terminated. (B# 130014, 2-225187609)
- ❑ When both the ProxySG appliance and its directly connected device are not set up for auto-negotiation, relying on `auto-sense` for a Gigabit Ethernet interface, may not sense the speed and duplex of the link. (B# 119562)
- ❑ Attack detection block and unblock settings are not reflected in the system configuration. (B# 109452)

Timezones_and_NTP

- ❑ The acquire UTC time returns a success message, although the NTP server is unreachable. (B# 119260)

User Documentation

- ❑ Relying on `auto-sense` where both the ProxySG appliance and its link partner are not both set up for auto-negotiation is problematic and can cause down interface links. It is recommended to manually set the speed and duplex appropriately. (B# 122028)
- ❑ The Management Console hangs on first access with Browser IE7 when Phishing filter is set to default, a JRE - Java Plug-in 1.6.0_12 exception occurs. (B# 110413)

Windows_Media_Proxy

- ❑ Clients requests are going into a waiting state causing delays or errors. This occurs in a proxy chain environment with log forwarding enabled on the downstream proxy and multiple clients requesting the same live stream from a playlist with multiple files. (B# 109745)
- ❑ In an explicit proxy chain environment, with authentication enabled, live stream request hangs WM-HTTP content. (B# 118032)
- ❑ Configuring a script to pull a file from a media server and saving it with a false name might result in an `Object not found` error message in the CLI. (B# 119290)

Section D: SGOS 5.4.10.1 build 78212

- ❑ Windows Media over HTTP fails when the URL format is `http://<Proxy_SG_IP>/redirect?mms://<streaming_server>/<filename>.wmv`
The workaround is to use `http://<Proxy_SG_IP>/redirect?http://<URL>` instead of using `http://<Proxy_SG_IP>/redirect?mms://<URL>`
SR 2-198319392 (B# 124346, 2-198319392)

Section E: SGOS 5.4.9.1, build 76593

Section E: SGOS 5.4.9.1, build 76593

Release Date: 10/20/2011, build 76593

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.9.1 Contents

- ❑ "Fixed issues in SGOS 5.4.9.1"
- ❑ "Known Issues in SGOS 5.4.9.1" on page 24
- ❑ "Limitations in SGOS 5.4.9.1" on page 25

Fixed issues in SGOS 5.4.9.1

CIFS Proxy

- ❑ Fixed the issue where ProxySG experienced high memory pressure even with reduced traffic due to slow memory leak. (B#158295, SR 2-349356592, SR 2-365616427)

Event Logging

- ❑ Fixed the issue where an event log or access log could not be retrieved because the system stopped logging access log data. (B#164284, SR 2-349356592, SR 2-386801404)

FTP Proxy

- ❑ Fixed the issue that caused software restart in process FTP CW B7712E50 in cmftpd.dll at .text+0x17250. (B#165418, SR 2-394932672)

HTTP Proxy

- ❑ Fixed the issue wherein two consecutive requests on a same persistent connection were resolved on a different https server, but the handshake to second server failed with SSL Certificate Hostname Mismatch (ssl_domain_invalid). (B#165424, SR 2-369853032)

IM Proxy

- ❑ Fixed the issue that caused software restart in process tcpip in process tcpip.dll at .text+0x3ec04. (B#147044, SR 2-322402252)

Kernel

- ❑ Fixed the issue where the SSL allocation sometimes caused high CPU utilization. This led to CLI or MC becoming unresponsive, thus preventing traffic from passing through the system. (B#147781, SR 2-321129422, 2-397425391, 2-408043882)

Section E: SGOS 5.4.9.1, build 76593

- ❑ Fixed the issue that caused degradation of system performance during surges in system load. (B#163649, SR 2-404945872)

MC Legacy

- ❑ Fixed the issue where the MC in the ProxySG appliance stopped responding while importing an archive that generated errors. (B#164683, SR 2-361719812)

NTP

- ❑ Fixed the issue where the NTP logged an error although the NTP server was reachable from the ProxySG appliance. Trigger condition: If configured server belongs to ntp server pool. (B#166305, SR 2-399026212)

SSL Proxy

- ❑ Fixed the issue with Event logs that contained the "Failed to get the peer certificate" error message. (B#164634, SR 2-378105602)

SNMP

- ❑ Fixed the issue wherein the SNMP stopped responding after a few days of uptime. (B#157113, SR 22-357518851, 2-373345415)

Windows Media Proxy

- ❑ Fixed the issue wherein the ProxySG went through memory utilization above 75% . This caused a failure in the Windows Media HTTP requests due to low memory conditions and thus resulting in a software restart. (B#164615 SR 2-2-381773352)
- ❑ Fixed the issue that caused software restart specific to vbrick's implementation of WM Server. The WM Server returned the whole file instead of metadata for a DESCRIBE WM-HTTP request. (B#166137 SR 2-400052509)

Known Issues in SGOS 5.4.9.1

Authentication

- ❑ The ProxySG appliance does not serve the authentication failure exception page when it receives the IBM TDS password expired response from the server. (B#140546, SR 2-299103242)
- ❑ BCAA occasionally issues the `Too many users--won't work` error when one user logs out of machine and another user logs in. This message is issued because the ProxySG appliance receives incorrect Win SSO information from the Windows API that the ProxySG appliance uses. (B#141759, SR 2-291631132)

Section E: SGOS 5.4.9.1, build 76593

FTP Proxy

- ❑ Processing an explicit FTP proxy request, and forcing TYPE A (ASCII) in your FTP client breaks causes 0D0A line breaks to start appearing in as 0A instead. (B#158333, SR 2-361254152)

HTTP Proxy

- ❑ When accessing HTTPS websites, should a connection error occur with FireFox (3.0.10 and higher) and Internet Explore 8, the Web browser does not display the HTML exception pages sent from the proxy. (B#121066,SR 2-190436632, 2-321761552, 2-33743303)

Policy

- ❑ The `FORCE_DENY` rule does not take effect (the connection is still allowed) after the upgrade from 4.3.2.3 to 5.4.7.1. (B#165289, SR 2-389303962)

TCP/IP and General Networking

- ❑ When dynamic bypass feature is enabled, the ProxySG appliance frequently bypasses all connections without any updates in any of the logs. (B#158640, SR 2-364252707)

URL Filtering

- ❑ Smartfilter does not match domains with .xxx (Dot TripleX) domains. (B#168321, SR 2-404128802)

Windows Media Proxy

- ❑ Media Streams played through Microsoft Silverlight plug-in may fail to play.(B#168212, SR 2-390134973)

Limitations in SGOS 5.4.9.1

ADN

- ❑ ADN connections are not re-established after downgrading from 5.5 to 5.4. Workaround: If setting both Tunnel and Manager listening ports to the same port number, before or after downgrading to 5.4x reset one of the listeners to a different port number. (B#132461)

Authentication

- ❑ **New Pin** and **Query** forms are only supported (and only required) for specific versions of RSA ACE Server. (B#126838)
- ❑ High CPU utilization by the Kernel when policy contains numerous user conditions with LDAP authentication. (B#130313)

Section E: SGOS 5.4.9.1, build 76593

Access log

- ❑ `x-cs-ocsp-error` and `x-rs-ocsp-error` fields are not part of the “SSL” format by default when upgrading from 4.x/5.2 to 5.3/5.4. These two fields must be added manually. (B# 107494)

Auto-Sense

- ❑ Relying on auto-sense where both the SG and its link partner are not both set up for auto-negotiation can cause down interface links. You must manually set the speed and duplex appropriately. (B#122028)

Authentication

- ❑ Radius realm configuration refresh time `rejected-credential-refresh` functionality may not work if the refresh time configured is less than 10 seconds. (B#107016)
- ❑ When using the Mach5 license health checks are not supported. (B#110095)
- ❑ If Session Monitor is enabled, and failover is switched from disabled to enabled or enabled to disabled, an 500 `Read Timeout` error may be received when attempting to access the Session-Monitor Lookup page. (B#110139)

CIFS Proxy

- ❑ MacOS 10.5.6 clients and later will not be able to connect to CIFS Shares on EMC servers. (B#109212)
- ❑ Visio fails to save `vsd` file to EMC shared folders filer through CIFS proxy over ADN causing a file corruption error. To avoid this issue, you should apply the latest Visio service pack SP3 for MS Visio 2003. (B#109420)
- ❑ `Client.protocol=cifs reflect_ip(client)` must be defined under the Proxy Layer. (B#109532)

CLI Consoles

- ❑ Administrator Login and Read/Write events repeat every second in the event log. (B#106455)
- ❑ Configuring the `exclude port` from an client acceleration configuration does not negate the `include-port` command. The `exclude port` command cannot be disabled. (B# 108262)
- ❑ Cannot negate the warn setting in CLI. B#108264
- ❑ Attack detection `block` and `unblock` settings are not reflected in the system configuration. (B#109452)
- ❑ The ProxySG appliance Management Console does not display a message when policy produces warnings. (B#131079)

Section E: SGOS 5.4.9.1, build 76593

- ❑ By default the CLI should display **NTP is enabled using Blue Coat's NTP servers** rather than **NTP enable** since it is enable only for Bluecoat NTP server. (B#131726)

Client Manager

- ❑ The allowable range for values in the **Configuration > ProxyClient > Web Filtering > Log** in the Upload settings is 0-99 hours, 0-59 minutes, 0-9999 MB. If a value that is larger than this range is entered, the extra digits are truncated without generating an error message. (B#108048)

Hardware Diagnostic

- ❑ The ProxySG appliance 210 SGOS failed to detect the removal of the hardware bridge.
(B#119333)

Health Monitoring

- ❑ The Health Monitor displays Critical CPU warning in the Event log when downloading SmartFilter database. (B#129709)

HTTP Proxy

- ❑ Emule login using the ProxySG appliance as SOCKS5_Proxy is not supported.
(B#107875)
- ❑ If upgrading from SGOS 3.2.8 to 5.3 or later, onwards, clear the cache after upgrading to prevent a restart of the ProxySG (SWE: 0x80005 PFA: 0x0 process HTTP Waiting Room in kernel_shim.dll at .text+0xCDC). (B#118952)
- ❑ If you have a URL rewrite policy for an HTTP request, the URL search patterns must be described in lowercase. This helps the ProxySG appliance to perform a case-insensitive search. (B#151206)

Initial Configuration

- ❑ During the initial configuration setup. Modifying the default gateway from an incorrect value to a valid value causes ping to fail if the change was not performed in the Summary Mode. (B#120422)

IPv6 Stack and IPv6 Proxies

- ❑ The `display` command in CLI does not work using the link-local URL. (B# 120765)

LDAP Groups

- ❑ VPM browsing of nested iPlanet referral groups results in errors. If these referral groups have sub-groups then those groups are not visible in VPM.
(B#102008)

Section E: SGOS 5.4.9.1, build 76593

Management Console

- ❑ Unable to set the February 29 date in the management console for leap years. (B#119314)
- ❑ When the NTP server list is empty and the `Acquire UTC time` is executed. The message prompt incorrectly displays `UTC time was successfully acquired` when there is no NTP server. (B#122335)
- ❑ An `Out of memory` error occurs when accessing **Statistics->Proxy client->Details** page of the Management Console. (B#122553)

MC Legacy

- ❑ Any changes done with the WCCP configuration interface results in the configuration done with the Text Editor to be overwritten. (B#138424)

Monitoring GUI

- ❑ The monitoring tab refreshes once per minute. It is possible to make a change in configuration and quickly switch to the monitoring tab. You may then see outdated information until the system performs a refresh. (B#108407)

User Documentation

- ❑ The Management Console hangs on first access with Browser IE7 when Phishing filter is set to default, JRE - Java Plug-in 1.6.0_12 exception occurs. (B#110413)

Multimedia Service

- ❑ Windows media player 10 can not access `http://financialserv.edgeboss.net/wmedia/financialserv/committeemeeting010509.wv` in transparent proxy mode, mms server return `ErrorCode: (0x80070002)`. This is an isolated case caused by third party software unable to comprehend or tolerant the information sent between the ProxySG appliance and the Origin Content Server (OCS). (B#109805)

Network Driver

- ❑ Changing the duplex on SG8100 Cobra to HDX switches the speed from Gigabit to 100MB. (B#108783)

Network Security

- ❑ The `attack-detection server` command for limiting number of server connection requests does not function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B#109184)

Section E: SGOS 5.4.9.1, build 76593

Policy

- ❑ The `deny.unauthorized (no)` property in CLI is configured within the `<proxy>` and `<ssl>` layers using the inline command `deny.unauthorized(no)`. (B#117482)
- ❑ The `ftp.server_connection (immediate)` property in CLI is configured within the `<proxy>` and `<cache>` layers using the inline commands `ftp.server_connection(immediate)`. (B#117484)
- ❑ A system downgrade to an earlier release causes policy compilation error message when the new Content Policy Language (CPL) gestures are introduced to a maintenance release. This is because the new gesture is not supported in the previous version. (B#122705)
- ❑ On occasion, the PAC/WPAD redirection fails with `400-invalid_request` when policy is used. Blue Coat recommends using policy gesture `request_redirect` instead of `redirect`. This was first introduced in SGOS 5.5.7.1. (B#145454, SR 2-307668872)

RealMedia

- ❑ Pre-population of RealMedia content from web servers does not work. (B#109339)

SSL Ciphers

- ❑ SSL fails to initialize when `sslv2` and `rc4-64-md5` are selected as the Cipher in SSL-Client. (B#107847)

SSL Proxy

- ❑ SSL Proxy does not support connecting to a server using DSA encryption. It is recommended to use `tcp-tunnel proxy` instead. (B#109099)
- ❑ By default, hostname mismatch certificate validation does not occur unless the full SSL interception is enabled. (B#119542)

SSL/TLS and PKI

- ❑ When disabling `verify peer` option in any HTTPS Access Log uploads, a certificate mismatch is still logged. (B#107579)

SOCKS Proxy

- ❑ Within proxy chain environment the upstream proxy may display the `SOCKSHistory->ClntComp.Gain` calculation as “100%” instead of “0%”. (B#107429)

TCP/IP and General Networking

- ❑ When an hardware bridge is re-enabled to fail-open or fail-closed the settings are maintained and the bridge may have manual setting of 100/half speed and duplex on one side, and auto on the other. This can potentially cause performance problems. (B#108065)
- ❑ Relying on auto-sense for a Gigabit Ethernet interface may not sense the speed and duplex of the link, when both the SG and its directly connected device are not set up for auto-negotiation. (B#119562)
- ❑ The SG210 appliance does not support the configuration of Gigabit speed capacity on interface ports. (B#120156)
- ❑ Configuring additional static routes entries prompts an warning message which does not reflect the correct cause of the error. (B#120931)
- ❑ In a split-DNS, chained-proxy, environment, child proxy continues to send lookups to primary DNS server after health-check reports it down.
Workaround was achieved by means of adding a condition `url.host.is_numeric=yes` in front of any condition. (B#121987)
- ❑ In SGOS 5.4x and higher, when an interface is down, the ProxySG responds to ARP Request with the MAC address of the receiving interface instead of the interface that the target IP address is configured on. To avoid this behavior, within the CLI enable `tcp-ip-arp-strict-matching`. This command will ensure the proxy returns the MAC address of the interface where target IP configured when an interface is down. (B#122054)
- ❑ TCP Tunneled connections in `Established` state takes between 2-4 hours before it gets terminated. (B#130014)

Windows Media Proxy

- ❑ In an proxy chain environment with log forwarding enable on the downstream proxy and multiple clients requesting the same live stream from a playlist with multiple files. Clients request are going into a `waiting` state causing delays or errors. (B#109745)

In an explicit proxy chain environment with authentication enabled, live stream request hangs WM-HTTP content. (B#118032)

Section F: SGOS 5.4.8.1, build 73295

Section F: SGOS 5.4.8.1, build 73295

Release Date: 08/16/2011, build 73295

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.8.1 Contents

- ❑ "Fixed Security Advisory Issues"
- ❑ "Changes in SGOS 5.4.8.1"
- ❑ "Fixed issues in SGOS 5.4.8.1"
- ❑ "Known Issues in SGOS 5.4.8.1"
- ❑ "Limitations in SGOS 5.4.8.1"

Fixed Security Advisory Issues

This section lists important fixes in SGOS 5.4.8.1 that address specific security threats.

- ❑ Online Certificate Status Protocol (OCSP) response validation error fixed. The ProxySG appliance incorrectly returned an error when validating the certificate chain for the OCSP responder. The OCSP responder's certificate could not be validated. Workaround: Explicitly import and trust the certificate of the CA that signed the OCSP responder's certificate. The explicit trust is no longer required if the CA that signed the OCSP responder's certificate is a CA in the certificate chain for the server certificate being validated.

Changes in SGOS 5.4.8.1

This section lists important changes in 5.4.8.1

- ❑ Added support for the Seagate 500GB HDD SST500NM0001 for the ProxySG 9000-5/10/20 appliances.

Fixed issues in SGOS 5.4.8.1

Access Logging

- ❑ Active FTP upload of access logs stopped responding and prevented all subsequent periodic uploads from being performed. (B#159023, SR 2-369935715)

ADN

- ❑ The ProxySG appliance causes Projectwise application to fail when using policy to perform compression and byte caching. (B#157470)

Section F: SGOS 5.4.8.1, build 73295

Authentication

- ❑ Fixed the issue where SSO failed to initialize, and an SSO authorization failure occurred while configuring an `ignore user` in the SSO.ini file under `[SSOServiceUser]` using the LDAP FQDN:
`cn=ignoreuser,ou=division,ou=location,o=company`. (B#157474, SR 2-358445202).
- ❑ Fixed the issue where SiteMinder authentication failed after upgrading from 5.4.1.12 to 5.4.4.1 or 5.4.6.1. (B#157883, SR 2-356117612)
- ❑ Fixed the issue where BCAAA Siteminder Agent inserted incorrect character in the form login URL leading to users being denied access. (B#158572)
- ❑ Fixed the issue where high CPU utilization in the ProxySG appliance caused slow down in web access when evaluating a policy that contains around 200 LDAP user DN's with Novell SSO & eDirectory. (B#158986, SR 2-367218252)
- ❑ Fixed the issue where WinSSO DC query failed on Windows 2008 machines due to disabled Computer Browser service. (B#161723, SR 2-352163642, SR 2-375176977)

CIFS Proxy

- ❑ When ADN is enabled, you cannot save MS Word 2010/2003/2007 documents with CIFS. (B#151371, SR 2-335251542)
- ❑ Fixed the issue where theProxySG appliance experienced high memory pressure even with reduced traffic due to slow memory leak. (B#158295, SR 2-349356592, SR 2-365616427)

CLI Consoles

- ❑ Fixed the issue that caused software restart on `show config` if accelerated PAC files contain invalid utf8 characters. (B#158742 SR 2-368542022)

Hardware Drivers

- ❑ Fixed the issue that caused software restart in Process `CAG_Maintenance` in `ata.dll` at `.text+0x12445` during a restart upgrade if there is a command in flight when the shutdown code is initiated. (B#160482, SR 2-376165275)

Health Checks

- ❑ Sometimes the health of a composite health check is affected by a change in the health state of a host that is not a member of the composite group. (B#152916, SR 2-347177582)
- ❑ 'alert notification sensor' configurations were not ported to SGOS 5.x when upgrading from SGOS 4.x. (B#161608, SR 2-379195522)

Section F: SGOS 5.4.8.1, build 73295

HTTP Proxy

- ❑ Fixed the issue where the ProxySG appliance intermittently returned a `403-Policy denied exception` as a redirect response was being misinterpreted as a "policy denied" error. (B#161096, SR 2-374525142)
- ❑ Fixed the issue that caused a software restart in `process PDW` in `http.dll` while evaluating the policy for `raw_header` regex pattern match with a request that exceeds `2^16` large size. (B#161930, SR 2-381537292)
- ❑ Fixed the issue with URL rewrite policy when the pattern in the policy and the matched sub-string in the URL was different in the way special characters were represented. (B#163606, SR 2-373297702)
- ❑ Fixed the issue that caused software restart within `HTTP SW B72DEEC0` for `B8F3CEC0` at linear address `0x00000000` due to insufficient error checking of mangled cookie. (B#164064, SR 2-387417962)

Kernel

- ❑ Fixed the issue where software restart was caused in `process Idler 0` in `Kernel.dll` at `.text+0x2ed3f` due to incorrect watchdog updates by the Kernel. (B#159213, SR 2-369325572, SR 2-376154604)
- ❑ Fixed the issue where Squid access log format recorded 4 significant digits at the 1000 mark. (B#159613, SR 2-368982662)
- ❑ Fixed the issue that caused a software restart in `process osconfig` in `Kernel.dll` at `.text+0x28602` caused by system watchdogs due to missed interrupts from serial console. (B#161385, SR 2-375631171)

User Documentation

- ❑ SGOS 5.4 and 5.5 *Feature Change Reference* document had a reference in WCCP to a non-existent sizing guide. (B#162409, SR 2-375176977)

Net Security/Attack Detection

- ❑ Fixed the Event log issue. The event log now shows `connection denied to client` due to `connection limit` events. (B#162725, SR 2-379248642)

OCSP

- ❑ Fixed the OCSP response validation error. The ProxySG appliance incorrectly returned an error when validating the certificate chain for the OCSP responder. The error was that the OCSP responder's certificate could not be validated. The work around was to explicitly import and trust the certificate of the CA that signed the OCSP responder's certificate. The explicit trust is no longer needed if the CA that signed the OCSP responder's certificate is a CA in the certificate chain for the server certificate being validated. (B# 158945)

Section F: SGOS 5.4.8.1, build 73295

Policy

- ❑ Fixed the issue where the domain could not be resolved while accessing an URL. A policy that contained the condition "url.host.is_private=yes" was matching even if the condition was irrelevant. (B#162221, SR 2-376617402)

SNMP

- ❑ Fixed the issue wherein the user modified the appliance name, SNMP GET for host name always returned the old name instead of the new name. (B#160254, SR 2-366950202, 2-386950242)

SSL/TLS and PKI

- ❑ Fixed the issue that caused software restart at process `SSL-map Proprietor` in `crypto.dll` at `.text+0x32514`. (B#161004, SR 2-377638132)

Storage

Fixed the issue where the Cache Engine did not recognize a faulty disk, but Health Monitor and SG recognized it. With this fix, the system attempts to recover the disk and marks it as bad if the recovery fails. (B#162554, SR 2-376805172)

TCP/IP and General Networking

- ❑ Fixed the issue where software restart was caused at `CAG_Maintenance` in `Kernel.dll` at `.text+0xe7b6` while performing a hardware restart on SG-9000 with Nvidia driver and a VLAN created on software bridge interface. (B#160151 SR 2-373228992)

Timezones and NTP

- ❑ Fixed the issue where the time zone archived out of date and showed DST for Egypt. (B#161999, SR 2-381920522)

VPM Policy

- ❑ Fixed the issue where selecting multiple groups when domain is specified corrupted the group name. (B#160191, SR 2-373037582)
Workaround: Select 1 group at a time, or do not specify a domain name.
- ❑ Fixed the issue where layer guard comments were not always saved when policy was installed. B# 162034, SR 2-377534852
- ❑ Fixed the issue where the VPM policy generated for content filtering sub-categories was incorrect. If a category was selected but not some of its sub-categories, the entire category would erroneously be blocked. (B#162588, SR 2-381379772, 2-381437842)

Section F: SGOS 5.4.8.1, build 73295

URL Filtering

- ❑ Fixed the issue where the memory fragmentation causes the ProxySG appliance to become unstable during Smartfilter update. (B#156792, SR 2-360768162, SR 2-373284052)

Known Issues in SGOS 5.4.8.1

Authentication

- ❑ The ProxySG appliance does not serve the authentication failure exception page when it receives the IBM TDS password expired response from the server. (B#140546, SR 2-299103242)
- ❑ BCAA occasionally issues the Too many users--won't work error when one user logs out of machine and another user logs in. This message is issued because the ProxySG appliance receives incorrect Win SSO information from the Windows API that the ProxySG appliance uses. (B#141759, SR 2-291631132)

FTP Proxy

- ❑ Processing an explicit FTP proxy request, and forcing TYPE A (ASCII) in your FTP client breaks causes 0D0A line breaks to start appearing in as 0A instead. (B#158333, SR 2-361254152)

HTTP Proxy

- ❑ When accessing HTTPS websites, should a connection error occur with FireFox (3.0.10 and higher) and Internet Explore 8, the Web browser does not display the HTML exception pages sent from the proxy. (B#121066, SR 2-190436632, 2-321761552, 2-33743303)

TCP/IP and General Networking

- ❑ When dynamic bypass feature is enabled, the ProxySG appliance frequently bypasses all connections without any updates in any of the logs. (B#158640, SR 2-364252707)
- ❑ Configurable option to disable silly-window syndrome avoidance. (B#131046, SR 2-378568521)

Limitations in SGOS 5.4.8.1

ADN

- ❑ ADN connections are not re-established after downgrading from 5.5 to 5.4. Workaround: If setting both Tunnel and Manager listening ports to the same port number, before or after downgrading to 5.4x reset one of the listeners to a different port number. (B#132461)

Section F: SGOS 5.4.8.1, build 73295

Authentication

- ❑ **New Pin** and **Query** forms are only supported (and only required) for specific versions of RSA ACE Server. (B#126838)
- ❑ High CPU utilization by the Kernel when policy contains numerous user conditions with LDAP authentication. (B#130313)

Access log

- ❑ `x-cs-ocsp-error` and `x-rs-ocsp-error` fields are not part of the “SSL” format by default when upgrading from 4.x/5.2 to 5.3/5.4. These two fields must be added manually. (B# 107494)

Auto-Sense

- ❑ Relying on auto-sense where both the SG and its link partner are not both set up for auto-negotiation can cause down interface links. You must manually set the speed and duplex appropriately. (B#122028)

Authentication

- ❑ Radius realm configuration refresh time `rejected-credential-refresh` functionality may not work if the refresh time configured is less than 10 seconds.
- ❑ When using the Mach5 license health checks are not supported. (B#110095)
- ❑ If Session Monitor is enabled, and failover is switched from disabled to enabled or enabled to disabled, an 500 `Read Timeout` error may be received when attempting to access the Session-Monitor Lookup page. (B#110139)

CIFS Proxy

- ❑ MacOS 10.5.6 clients and later will not be able to connect to CIFS Shares on EMC servers. (B#109212)
- ❑ Visio fails to save `vsd` file to EMC shared folders filer through CIFS proxy over ADN causing a file corruption error. To avoid this issue, you should apply the latest Visio service pack SP3 for MS Visio 2003. (B#109420)
- ❑ `Client.protocol=cifs reflect_ip(client)` must be defined under the Proxy Layer. B#109532

CLI Consoles

- ❑ Administrator Login and Read/Write events repeat every second in the event log. (B#106455)
- ❑ Configuring the `exclude port` from an client acceleration configuration does not negate the `include-port` command. The `exclude port` command cannot be disabled. (B# 108262)

Section F: SGOS 5.4.8.1, build 73295

- ❑ Cannot negate the warn setting in CLI. B#108264
- ❑ Attack detection `block` and `unblock` settings are not reflected in the system configuration. (B#109452)
- ❑ The ProxySG appliance Management Console does not display a message when policy produces warnings. (B#131079)
- ❑ By default the CLI should display **NTP is enabled using Blue Coat's NTP servers** rather than **NTP enable** since it is enable only for Bluecoat NTP server. (B#131726)

Client Manager

- ❑ The allowable range for values in the **Configuration > ProxyClient > Web Filtering > Log** in the Upload settings is 0-99 hours, 0-59 minutes, 0-9999 MB. If a value that is larger than this range is entered, the extra digits are truncated without generating an error message. (B#108048)

Hardware Diagnostic

- ❑ ProxySG 210 SGOS failed to detect the removal of the hardware bridge. (B# 119333)

Hardware Drivers

- ❑ 1 Gigabit-half duplex setting is not a valid option 1GB interfaces.

Health Monitoring

- ❑ The Health Monitor displays Critical CPU warning in the Event log when downloading SmartFilter database. (B#129709)

HTTP Proxy

- ❑ Emule login using ProxySG as SOCKS5_Proxy is not supported. (B# 107875)
- ❑ If upgrading from SGOS 3.2.8 to 5.3 or later, onwards, clear the cache after upgrading to prevent a restart of the ProxySG (SWE: 0x80005 PFA: 0x0 process HTTP Waiting Room in kernel_shim.dll at .text+0xCDC). (B#118952)
- ❑ If you have a URL rewrite policy for an HTTP request, the URL search patterns must be described in lowercase. This helps the ProxySG appliance to perform a case-insensitive search. (B#151206)

Initial Configuration

- ❑ During the initial configuration setup. Modifying the default gateway from an incorrect value to a valid value causes ping to fail if the change was not performed in the `Summary Mode`. (B#120422)

IPv6 Stack and IPv6 Proxies

- ❑ The `display` command in CLI does not work using the link-local URL. B# 120765

LDAP Groups

- ❑ VPM browsing of nested iPlanet referral groups results in errors. If these referral groups have sub-groups then those groups are not visible in VPM. (B#102008)

Management Console

- ❑ Unable to set the February 29 date in the management console for leap years. (B#119314)
- ❑ When the NTP server list is empty and the `Acquire UTC time` is executed. The message prompt incorrectly displays `UTC time was successfully acquired` when there is no NTP server. (B#122335)
- ❑ An `Out of memory` error occurs when accessing **Statistics->Proxy client->Details** page of the Management Console. (B#122553)

MC Legacy

- ❑ Any changes done with the WCCP configuration interface results in the configuration done with the Text Editor to be overwritten. (B#138424)

Monitoring GUI

- ❑ The monitoring tab refreshes once per minute. It is possible to make a change in configuration and quickly switch to the monitoring tab. You may then see outdated information until the system performs a refresh. (B#108407)

User Documentation

- ❑ The Management Console hangs on first access with Browser IE7 when Phishing filter is set to default, JRE - Java Plug-in 1.6.0_12 exception occurs. (B#110413)

Multimedia Service

- ❑ Windows media player 10 can not access `http://financialserv.edgeboss.net/wmedia/financialserv/committeemeeting010509.wvx` in transparent proxy mode, mms server return ErrorCode: (0x80070002). This is an isolated case caused by third party software unable to comprehend or tolerate the information sent between the ProxySG appliance and the Origin Content Server (OCS). (B#109805)

Section F: SGOS 5.4.8.1, build 73295

Network Driver

- ❑ Changing the duplex on SG8100 Cobra to HDX switches the speed from Gigabit to 100MB. (B# 108783)

Network Security

- ❑ The `attack-detection server` command for limiting number of server connection requests does not function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B# 109184)

Policy

- ❑ The `deny.unauthorized (no)` property in CLI is configured within the `<proxy>` and `<ssl>` layers using the inline command `deny.unauthorized(no)`. (B#117482)
- ❑ The `ftp.server_connection (immediate)` property in CLI is configured within the `<proxy>` and `<cache>` layers using the inline commands `ftp.server_connection(immediate)`. (B#117484)
- ❑ A system downgrade to an earlier release causes policy compilation error message when the new Content Policy Language (CPL) gestures are introduced to a maintenance release. This is because the new gesture is not supported in the previous version. (B#122705)

RealMedia

- ❑ Pre-population of RealMedia content from web servers does not work. (B#109339)

SSL Ciphers

- ❑ SSL fails to initialize when `sslv2` and `rc4-64-md5` are selected as the Cipher in SSL-Client. (B#107847)

SSL Proxy

- ❑ SSL Proxy does not support connecting to a server using DSA encryption. It is recommended to use `tcp-tunnel proxy` instead. (B#109099)
- ❑ By default, hostname mismatch certificate validation does not occur unless the full SSL interception is enabled. (B#119542)

SSL/TLS and PKI

- ❑ When disabling `verify peer` option in any HTTPS Access Log uploads, a certificate mismatch is still logged. (B#107579)

Section F: SGOS 5.4.8.1, build 73295

SOCKS Proxy

- ❑ Within proxy chain environment the upstream proxy may display the `SOCKSHistory->ClntComp.Gain` calculation as “100%” instead of “0%”. (B#107429)

TCP/IP and General Networking

- ❑ When an hardware bridge is re-enabled to fail-open or fail-closed the settings are maintained and the bridge may have manual setting of 100/half speed and duplex on one side, and auto on the other. This can potentially cause performance problems. (B#108065)
- ❑ Relying on auto-sense for a Gigabit Ethernet interface may not sense the speed and duplex of the link, when both the SG and its directly connected device are not set up for auto-negotiation. (B#119562)
- ❑ The SG210 appliance does not support the configuration of Gigabit speed capacity on interface ports. (B#120156)
- ❑ Configuring additional static routes entries prompts an warning message which does not reflect the correct cause of the error. (B#120931)
- ❑ In a split-DNS, chained-proxy, environment, child proxy continues to send lookups to primary DNS server after health-check reports it down.
Workaround was achieved by means of adding a condition
`url.host.is_numeric=yes` in front of any condition. (B#121987)
- ❑ In SGOS 5.4x and higher, when an interface is down, the ProxySG responds to ARP Request with the MAC address of the receiving interface instead of the interface that the target IP address is configured on. To avoid this behavior, within the CLI enable `tcp-ip-arp-strict-matching`. This command will ensure the proxy returns the MAC address of the interface where target IP configured when an interface is down. (B#122054)
- ❑ TCP Tunneled connections in `Established` state takes between 2-4 hours before it gets terminated. (B#130014)

Windows Media Proxy

- ❑ In an proxy chain environment with log forwarding enable on the downstream proxy and multiple clients requesting the same live stream from a playlist with multiple files. Clients request are going into a `waiting` state causing delays or errors. (B#109745)
- ❑ In an explicit proxy chain environment with authentication enabled, live stream request hangs WM-HTTP content. (B#118032)

Section G: SGOS 5.4.7.1, build 65467

Section G: SGOS 5.4.7.1, build 65467

Release Date: 04/27/2011, build 65467

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.7.1 Contents

- ❑ "Fixed Security Advisory Issues"
- ❑ "Fixes in 5.4.7.1"
- ❑ "Known Issues in 5.4.7.1"

Fixed Security Advisory Issues

This section lists important fixes in SGOS 5.4.7.1 that address specific security threats.

- ❑ BCAA Stack overflow vulnerability fixed. (B# 157580) See Security Advisory SA55 (<https://kb.bluecoat.com/index?page=content&id=SA55>)

Fixes in 5.4.7.1

Access Logging

- ❑ Fixed problem where one backslash got removed from the Access Log FTP username field when using the CLI. For example, when typing `show config` it displayed `domain username` instead of `domain\username`. (B#152834, SR 2-339211523)
- ❑ Resolved issue where the ProxySG appliance showed degradation in performance when Surf Control ver.5 required a reverse DNS lookup for access logging. (B#154433, SR 2-352240862)

Authentication

- ❑ Fixed issue where in some requests to the upstream proxy, the BASIC authentication credentials were included in a Proxy-Authentication header despite no such request being received. (B#153274, SR 2-348468372)
- ❑ Resolved BCAA's processor threads that got blocked while trying to do an IP-to-user table lookups, which caused BCAA to get dead-locked. (B#154042, SR 2-345314512)

Cache Engine

- ❑ Fixed the issue where the ProxySG appliance was unable to read a valid SmartFilter license installed on the appliance. (B#149368)

Section G: SGOS 5.4.7.1, build 65467

- ❑ Fixed the issue with stale client connections when multiple concurrent connections request an object with the following specifications: the response header does not contain content-length, object is not chunked-encoded, and object is larger than 500KB. (B#145698)

CIFS Proxy

- ❑ Resolved restart of SGOS restart in process CIFS::Worker: Connection 41 (running) in ce_admin.dll at .text+0x2da6. (B#152806, SR 2-344801482)
- ❑ Resolved the data backup failure caused by the CIFS proxy. This caused the OCS (Office Communications Server) to respond to subsequent requests with STATUS_INVALID_HANDLE. (B#156702)

Client Manager

- ❑ Fixed restart of SGOS in process mgmt.worker.02227181 in util.dll at .text+0x16413. (B#151401, SR 2-340796992)

DNS Proxy

- ❑ After upgrading to SGOS 5.4.5.1, the issue where the DNS resolver did not show a median value, is now fixed. The query SNMP OID 'sgProxyDnsMedianServiceTime', no longer shows increments. (B#156525, SR 2-354581522)

FTP Proxy

- ❑ Added support for the MLSD and MLST FEAT commands for browsing an FTP server. (B#140467, SR 2-300231892)

HTTP Proxy

- ❑ Fixed the issue that caused the inability to download a local content filter database over FTP after upgrading to 5.5.3.1 from 5.5.1.1. This issue was seen if ICAP trickle at start was enabled. (B#147302)
- ❑ Fixed the issue where SGOS restarted in Process HTTP Waiting Room in http.dll at .text+0x93df7. (B#156140, SR 2-358661832, 2-360499632)
- ❑ Resolved issue where the HTTP Proxy could not recognize \r\n\r\n (0d0a0d0a) as continuous data of the last chunking packet, in the header of a HTTP POST request. (B#156186, SR 2-334000342)
- ❑ Resolved issue where a small buffer size prevented large JavaScripts responses and TWURL rewrites, which caused the ProxySG to close connection. (B#153740)

Section G: SGOS 5.4.7.1, build 65467

ICAP

- ❑ Infrequent and non-service impacting error messages such as "Cannot establish connection to service Vontu" or "Cannot establish connection to service ProxyAV" are not recorded in the event log any longer. (B#142662, SR 2-297064887, 2-319977085, 2-342771072)
- ❑ No deletion of the ICAP service occurs in the ICAP statistics GUI page. This is the expected behavior of the ProxySG appliance. As a workaround to delete the ICAP statistics page, use the `clear-statistics persistent` command in the CLI, or in the Management Console, select **Maintenance > System and Disks**. Under the **Tasks** tab, go to **Cache and Statistics Tasks**, click **Clear** the trend statistics. (B#154171, SR 2-347948182)
- ❑ Fixed issue where the ProxySG appliance closed connections with Websense Off-box prematurely resulting in reduced performance & delayed responses from Websense. (B#154741, SR 2-344022992)

IM Proxy

- ❑ Fixed the problems with high CPU and memory pressure. (B#148626, SR 2-326634124)

Management Console

- ❑ Resolved the issue where Advanced URL links were not displayed in the Management Console menu, when selecting the **Statistics > Advanced** link. (B# 156669, SR 2-343491802)

Network Drivers

- ❑ Fixed the large number of input errors seen on the Intel Gigabit dual/quad port passthru card. (B#145352, SR 2-320342602)

Sky UI

- ❑ Resolved issue where the Sky UI incorrectly reported zero ADN peer counts when in an active ADN session. (B#153440, SR 2-349556831)

SNMP

- ❑ Fixed the issue where the SNMP Trap did not generate Disk read write error notifications. Workaround: the Blue Coat private Management Information Base (MIB) file **BLUECOAT-SG-DISK-MIB.txt** must be modified in order to receive the new alert. (B#157802)
- ❑ SNMP device ID's added in the MIB file for SG 300, SG 900, SG 9000, AV 1200 and AV 1400 product lines. (B#157493)

SOCKS Proxy

- ❑ Resolved issue where in an Active FTP connection mode, in a SOCKS configuration with virtual IP, the ProxySG appliance responds with a RST to the server attempting to establish a connection. (B#153180, SR 2-362882334)

SSL/TLS and PKI

- ❑ Resolved issue where memory is leaked if there is no responder certificate in the OCSP Response.(B#158328, SR 2-332196632, 2-344022512, 2-357205221, 2-359782352)
- ❑ Fixed the issue that caused increased memory usage during HTTP policy evaluation. (B#148731)
- ❑ Resolved the issue where SSL Proxy s-ip shows the IP address of the OCS instead of the ProxySG appliance, when SSL Proxy intercept is enabled. (B#153574, SR 2-348101082)

TCP/IP and General Networking

- ❑ Configuring a delay in the ProxySG appliance's Health Check procedure fixed an issue where ProxySG appliance restarted in `Process tcpip` in `tcpip.dll` at `.text+0x134ca6`, after upgrade to SGOS 5.5.4.4. (B#157270)
- ❑ Fixed issue where ProxySG appliance was not tagging VLAN packets correctly when intercepting network traffic. (B#152547, SR 2-338779952)
- ❑ Resolved issue where the ProxySG appliance did not respond to a client PC when it's configured in a bridged mode, and the link to the interface which has the IP configured was down. (B#152897, SR 2-346476282)
- ❑ The value of `tcp-keepalive-timeout` is now included in the Configuration Archive, as it is no longer a hidden command. (B#156327, SR 2-356999142)
- ❑ Resolved issue where a single bad entry in the static route table lead to ARP requests for the 10.0.0.0 subnet, causing problems with sensitive upstream firewalls. (B#150718, SR 2-332947282)
- ❑ Resolved the issue when multiple entries in the TCP/IP routing table were used, overlapping routes were not displayed in proper order according to their subnet mask value. (B#152892, SR 2-344886762)
- ❑ In a situation where a cable between the primary router and the interface 2:0 is disconnected and the failure is properly propagated to interface 2:1. ProxySG is now reachable in both scenarios; when using the IP address defined on the bridge `passthru-2`, and when using the IP address defined on the bridge `passthru-2:2`. (B#155775)

VPM Policy

- ❑ The ProxySG appliance no longer stalls the policy installation, following a large VPM-XML policy file that caused the VPM Java applet to consume over 600M of memory. (B#156183, SR 2-358199687)

Section G: SGOS 5.4.7.1, build 65467

- ❑ Reduced excessive route re-shuffling and inconsistencies. When the interface goes down or comes back up, the stack used to reshuffle the interface routes for the subnet. Now when an interface route is selected, we try to provide the first route in the list, whose interface is up and running. An additional fix was made when an interface comes back up, all matching interface routes are checked and any host routes that lead to downed interfaces, are simply deleted. They will be regenerated based on use. (B#154857)

Windows Media Proxy

- ❑ Fixed the issue where the ProxySG appliance stops processing traffic due to an improper memory handing and requires a restart to resume proper functioning. (B#133131, SR 2-241549888, 2-311429344, 2-355920272, 2-358499432)
- ❑ Resolved issue where the ProxySG appliance stripped out the referrer header from the client request, for streaming Windows Media over HTTP. It did not forward the referrer header on the server side when HTTP handoff is enabled, which caused the OCS to deny the connection. B#151870, SR 2-342016457

URL Filtering

- ❑ Fixed the CPU utilization limit at 25% for content filtering database update tasks. A CLI command is added to enable/disable this value. (B#143851)

Known Issues in 5.4.7.1

Authentication

- ❑ SSO fails to initialize, and an SSO authorization failure occurs when you configure an `ignoreuser` in the SSO.ini file under [SSOServiceUser] using the LDAP FQDN: `cn=ignoreuser,ou=division,ou=location,o=company`. (B#157474, SR 2-358445202) *Fixed in 5.4.8.1*
- ❑ The ProxySG appliance does not serve the authentication failure exception page when it receives the IBM TDS password expired response from the server. (B#140546, SR 2-299103242)
- ❑ BCAA occasionally issues the `Too many users--won't work` error when one user logs out of machine and another user logs in. This message is issued because the ProxySG appliance receives incorrect Win SSO information from the Windows API that the ProxySG appliance uses. (B#141759, SR 2-291631132)

CIFS Proxy

- ❑ When ADN is enabled, you cannot save MS Word 2010/2003/2007 documents with CIFS. (B#151371, SR 2-335251542) *Fixed in 5.4.8.1*

Section G: SGOS 5.4.7.1, build 65467

Health Checks

- Sometimes the health of a composite health check is affected by a change in the health state of a host that is not a member of the composite group. (B#152916, SR 2-347177582) *Fixed in 5.4.8.1*

HTTP Proxy

- When accessing HTTPS websites, should a connection error occur with FireFox (3.0.10 and higher) and Internet Explore 8, the Web browser does not display the HTML exception pages sent from the proxy. (B#121066, SR 2-190436632, 2-321761552, 2-33743303)

SSL Proxy

- Accessing the URL www.hipassplus.co.kr using Opera 10 or Firefox 3.5 fails with the exception error, "SSL Certificate Verification Error (ssl_failed)". This failure occurs because the intermediate certificate "SignKorea MCA" has critical extensions that are not supported by the ProxySG appliance. (B#123410, SR 2-195383742)

Workaround: You can either disable SSL-proxy for these URLs or disable certificate validation in the SSL layer for the specific urls. (B#123410, SR 2-195383742)

IM Proxy

- Software restart occurs in process "tcpip" in "tcpip.dll" at .text+0x3ec04. (B#147044, SR2-322402252)

Section H: SGOS 5.4.6.1, build 54128

Section H: SGOS 5.4.6.1, build 54128

Release Date: 02/01/2011, build 54128

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.6.1 Contents

- ❑ "Changes in 5.4.6.1"
- ❑ "Fixes in 5.4.6.1"
- ❑ "Known Issues in 5.4.6.1"

Changes in 5.4.6.1

This section describes important changes in SGOS 5.4.6.1

SNMP

- ❑ SNMP MIB has been extended to support multiple CPU cores. (B# 146821)

Vulnerability Fixes in 5.4.6.1

Open SSL

- ❑ Open SSL for Ciphersuite Downgrade Attack - CVE-2010-4180 has been fixed. For details see, SA53.

Fixes in 5.4.6.1

Access Logging

- ❑ Fixed the issue where the archive configuration did not preserve the backslash characters (\) unless they were escaped. This was a common construct for Active Directory (Domain\UserName) and caused FTP to fail authentication. (B# 151281, SR# 2-338026112)

Authentication

- ❑ Resolved the issue where LDAP users failed to authenticate when more than 64 outstanding requests were pending. SR#2-317578152, 2-319945662, 2-326905241, 2-327018212, 2-329707037, 2-330026597, 2-334052169, 2-335901352 (B# 144232)
- ❑ Fixed the issue where cookies set at the wrong level caused `origin-cookie` to not work as expected for `.co.jp` domain URLs. SR# 2-321409402 (B# 146465)

Section H: SGOS 5.4.6.1, build 54128

- ❑ Fixed the issue where the ProxySG appliance discarded or ignored valid DNS information for the authentication server host, when it queried this during SGOS boot sequence. SR# 2-325863031, 2-328712765 (B#146958)

Cache Engine

- ❑ Fixed the software restarts in Process Cache Administrator in `ce_admin.dll` at `.text+0x8211`. SR#2-335498701 (B#137247)

CIFS Proxy

- ❑ Resolved the issue where CIFS Proxy stopped passing traffic due to a rare deadlock caused by a file rename operation, resulting in numerous connections being blocked. SR#2-328695892 (B# 147675)
- ❑ Fixed software restart in process `CIFS::Worker: Connection 65252 (running)` in `cifs.dll` at `.text+0x436a5`. SR#2-325389202 (B# 146652)
- ❑ Resolved the issue where CIFS stale connections were not cleaned up from the proxied sessions list. SR#2-334674529 (B# 148978)

CLI Consoles

- ❑ Resolved the issue where upgrading from SGOS 4.x with SNMP configured, `factory-restore keep-console` restored an already deleted SGOS 4.x configuration for the SNMP community string. SR#2-328319512 (B#147589)
- ❑ Resolved the issue when archiving proxy configuration via FTP or TFTP. A failure occurred after a certain number of uploads, due to an internal limitation related to file creation. (B#147324, SR#2-319823653)

Event Logging

- ❑ Fixed the issue where the event logs from the ProxySG appliance could not be downloaded over HTTPS using Internet Explorer via the advanced URL: https://<SG_IP_address>:8082/eventlog/download/events.log. SR#2-334375042 (B#150076)

HTTP Proxy

- ❑ Fixed the issue that prevented Internet Explorer 6.x users from accessing Siebel 8 through the ProxySG appliance, unless pipelining to the server was disabled. SR#2-288338322 (B#139572)
- ❑ Fixed software restart in process `HTTP SW BE21EEC0 for BE0E3EC0` in `http.dll` at `.text+0x98618`, when it serviced WebFTP traffic over HTTP, which connected to Linux/Unix based FTP servers. This issue is restricted to multi-processor models like ProxySG appliance: 810-10 and above. SR#2-316716962 (B#143612)
- ❑ Fixed the issue where URLs longer than 4096 characters resulted in `Parse Error` and had to go around the ProxySG appliance in order to resolve the URL. SR#2-310461732 (B#144175)

Section H: SGOS 5.4.6.1, build 54128

- ❑ Fixed issue with deteriorating ProxySG appliance performance when using `x-cs-netbios-*` access log fields and NETBIOS calls. SR#2-339694024 (B#151685)
- ❑ Fixed issue with Patience Page not working when files were downloaded in IE 8.0. SR#2-332004377 (B#148386)
- ❑ Fixed the issue when XML Name Space contents got converted to lowercase by the URL transform rule, it broke the W3C recommendations. SR#2-312553992 (B#144972)
- ❑ Fixed software restart in process HTTP SW Bf1E5EC0 for BFB2BEC0 in `ce_admin.dll` at `.text+0x40c79`. SR#2-331226012 (B# 148313)
- ❑ Fixed the issue where the ProxySG appliance responded with a HTTP Error 400 Bad Request, right after 302 redirected a response from Websense. SR#2-330019722 (B#149883)

IM Proxy

- ❑ Resolved issue where CPU utilization ran high in IM MSN when traffic was low and other proxy services were at optimal state. SR#2-325160702 (B#146635)

Kernel

- ❑ Fixed the issue where the restart of the ProxySG appliance software was caused by Profile push from Director. SR#2-336840411 (B#150645)
- ❑ Fixed the issue where all memory slots were showing as empty on **/Diagnostics/Hardware/Info** or `sysinfo` on SG9000-5. SR#2-325091272 (B#146510)

MAPI Proxy

- ❑ Fixed software restart in process EPM Worker in `util.dll` at `.text+0x12c0 (FDT::BGet_heap::brel)`. SR# 2-337745742, 2-340213278, 2-348240021 (B# 150764)

Management Console

- ❑ Resolved issue where user was unable to select a row in the first column in the Management Console menu, **Statistics>Sessions>Active Sessions>ADN Inbound**. SR#2-313686401 (B#144173)

Policy

- ❑ Fixed the issue when a user-defined exception page was used, a blank page was displayed on the web browser if the exception was hit for HTTPS URLs. This worked fine when with built-in exceptions & with HTTP URLs. SR#2-318029485, 2-330083332 (B#146163)

Section H: SGOS 5.4.6.1, build 54128

SNMP

- ❑ Fixed issue where the SNMP utilized 85-90% of the CPU after a reboot of the ProxySG appliance. SR#2-323815463 (B#146495)

SSL/TLS & PKI

- ❑ Fixed software restart in process `SSL-map Proprietor` in `ssl_map.dll` at `.text+0x12636`, when attempting to import a Certificate Authority. SR#2-334351112 (B#149260)
- ❑ Fixed software restart in process `SSLW C48BA930` in `cfssl.dll` at `.text+0x2afa5`. SR#2-330214072, 2-332264678, 2-335251242, 2-335339492, 2-337071452, 2-337233212 (B#148374)
- ❑ Resolved issue of the ProxySG appliance hanging caused by Profile push from Director. Please refer to Knowledge Base article FAQ1177 for more information and recommendations <https://kb.bluecoat.com/index?page=content&id=FAQ1177>. SR#2-336840411, 2-341732022 (B#151086)

Storage

- ❑ Fixed software restart in process `ATA Clock` in `ata.dll` at `.text+0x11644`. SR#2-314221237, 2-330116709, 2-334938051 (B#144028)

TCP/IP and General Networking

- ❑ Resolved the issue where the `restore-sgos4-config` command did not restore the static-route-table in a 4x or 5x configurations. SR#2-283894542, 2-302049917, 2-328876712 (B#136270)
- ❑ Resolved the issue where an intermediate device injected packets into the network which triggered the ProxySG appliance to generate a TCP ACK storm. SR#2-289938482 (B#137649)
- ❑ Fixed the issue when the setting: `reflect client IP` was disabled, `trust-dest-mac` did not work and caused the ProxySG appliance to perform a route lookup, leading to use of incorrect source IPs. SR#2-284636164, 2-286901210, 2-312213693 (B#142910)
- ❑ Fixed occasional bridge loop & intermittent packet loss occurrences when using multiple bridge groups (in event-log). SR#2-318192482, 2-330127019, 2-338551011 (B# 147954)
- ❑ Resolved the issue when a multicast address was used in the source IP field on upgrade, In a SGRP implementation. SR#2-339330162 (B#151445)
- ❑ Resolved the issue where the ProxySG appliance at the Core SG dropped 1 packet which caused the Edge to terminate file transfer. SR#2-320448309 (B# 151019)

Section H: SGOS 5.4.6.1, build 54128

- ❑ Resolved issue where the ProxySG appliance often sent back ACK on a different physical port and MAC address, of the software bridge.
SR#2-323871952 (B#146459)
- ❑ Fixed software restart in process `tcipip` in `tcipip.dll` at `.text+0x15554e`.
SR#2-343062032, 2-343070052 (B#151842)

Known Issues in 5.4.6.1

Authentication

- ❑ With the IBM TDS (Tivoli Directory Server) when an AD (Active Directory) user's password expires, the ProxySG appliance does not serve an exception page resulting in an authentication failure. SR#2-299103242 (B#140546)
- ❑ LDAP authentication on the ProxySG appliance does not accept the UTF-8 character set mode; the password filed for LDAP Authorization is rejected. SR#2-348056162 (B# 153412)
- ❑ BCAA occasionally returns `Too many users--won't work` error, when one user logs out of a client computer and another user logs in due to the incorrect Win SSO info provided by a Windows API used by the ProxySG appliance. SR#2-291631132 (B#141759)

Client Manager

- ❑ SGOS restarts in process `mgmt.worker.02227181` in `util.dll` at `.text+0x16413`.
SR#2-340796992 (B#151401)

CIFS Proxy

- ❑ Inability to save MS Word 2010/2003/2007 documentation via CIFS when ADN is enabled. SR#2-335251542 (B#151371)

FTP Proxy

- ❑ MLSD or MLST feature is not supported in the current SGOS implementation of the FEAT command. SR#2-300231892 (B#140467)

HTTP Proxy

- ❑ The ProxySG appliance enters regulation and stops responding to traffic randomly. SR#2-334359062, 2-335149122, 2-343439892 (B#149535)

ICAP

- ❑ Infrequent and non service impacting error messages appear in the event log, for example: `Cannot establish connection to service Vontu`, `Cannot establish connection to service ProxyAV`. SR#2-297064887, 2-319977085, 2-342771072 (B#142662)

Section H: SGOS 5.4.6.1, build 54128

IM Proxy

- ❑ SGOS restarts in process `tcipip` in `tcipip.dll` at `text+0x3ec04`.
The workaround: disable IM logging. SR#2-322402252 (B#147044)

SOCKS Proxy

- ❑ Intermittent failure of FTP data connection in Socks configuration with virtual IP. SR#2-330508002 (B#153180)

SSL Proxy

- ❑ Accessing URL `www.hipassplus.co.kr` from Opera10 or Firefox 3.5 fails with exception error: `SSL Certificate Verification Error (ssl_failed)`. This is caused by the intermediate certificate “SignKorea mCA” which has critical extensions that are not supported by ProxySG appliance - Certificate policies and Policy Constraint.
Workaround: Disable SSL-Proxy for these URLs or disable certificate validation in the SSL layer for the specific URLs. SR#2-195383742 (B#123410)

TCP/IP and General Networking

- ❑ A single bad entry in the static route table can lead to ARP requests for 10.0.0.0, causing problems with sensitive upstream firewalls. This error is fixed as soon as the erroneous IP in the static route table is corrected.
SR#2-332947282 (B#150718)
- ❑ In the TCP/IP routing table, overlapping routes are not properly ordered by subnet mask value when you have multiple gateways.
Workaround: When you have multiple default gateways across different groups, add the default gateways using the CLI. (B#153539)

URL Filtering

- ❑ ProxySG appliance categorizes YouTube URLs as `None` even after downloading the complete BCWF database while the online/site review of the same URL indicates the correct category. SR#2-345267862 (B#152244)
- ❑ The CPU utilization limit for automatic content filtering database updates is preset to 25%. (B#143851)

Windows Media Proxy

- ❑ The ProxySG appliance strips out the referrer header from the client request for streaming Windows Media over HTTP. It does not forward the referrer header on the server side when HTTP handoff is enabled, which causes the OCS to deny the connection.
Workaround: Disable HTTP handoff in the Windows Media proxy.
SR#2-342016457 (B#151870)

Section I: SGOS 5.4.5.1, build 51300

Section I: SGOS 5.4.5.1, build 51300

Release Date: 10/21/2010, build 51300

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.5.1 Contents

- ❑ "Fixes in 5.4.5.1"
- ❑ "Known Issues in 5.4.5.1"

Vulnerability Fixes in 5.4.5.1

CLI Consoles

- ❑ The ProxySG appliance executes commands even if the admin account was set to READ ONLY due to a security vulnerability. See Security Advisory SA45 for more information (<https://kb.bluecoat.com/index?page=content&id=SA45>).
- ❑ Cross site scripting vulnerability fixed. See Security Advisory SA47 (<https://kb.bluecoat.com/index?page=content&id=SA47>).

HTTP Proxy

- ❑ NSA-SG-1-c Transformer does not handle scripts encoded with UTF-8 or Hex encoding. See Security Advisory SA48 (<https://kb.bluecoat.com/index?page=content&id=SA48>)

SSL Proxy

- ❑ The TLS protocol, and the SSL protocol 3.0 (and possibly earlier), does not properly associate renegotiation handshakes with an existing connection. (CVE-2009-3555). See Security Advisory SA44 (<https://kb.bluecoat.com/index?page=content&id=SA44>) SR#2-239523102, 2-252882082, 2-279446222, 2-294222663, 2-315935322

Fixes in 5.4.5.1

Access Logging

- ❑ The ProxySG stops responding while pasting a list of commands through SSH due to improper error handling. SR#2-295590982 (B#139350)
- ❑ The ProxySG automatically reboots due to a page fault. (B#139328, SR#2-296878108)
- ❑ Access log FTP upload fails with a socket error. (B#140113)

Section I: SGOS 5.4.5.1, build 51300

- ❑ Restart Regular ceases to work after access log upload failure over FTPS. SR#2-310593232, 2-319330526 (B#141982)
- ❑ When "client-type" is set to "none" on the Management Console, the ProxySG will do FTP uploading and create a "Not Applicable" file. (B#144730)

Active Sessions

- ❑ The ProxySG appliance crashes due to memory corruption. SR#2-284888792 2-309594602 2-318728296 (B#140304)

ADN

- ❑ Byte-caching tunnel does not close properly because of data corruption. SR#2-271326683 (B#136392)
- ❑ The Management Console does not properly display improperly closed tunnels per peer. SR#2-301341698 (B#142193)

Authentication

- ❑ LDAP authentication (when using LDAP protocol version 3 on Windows Server 2008) causes the ProxySG to restart. SR#2-295259481, 2-296420805 (B#138984)
- ❑ The error "Username could not be converted to Kerberos name" occurs in an IWA realm when authenticating users with names longer than 15 characters from a remote domain. (B#139935, SR#2-293451112, 2-298066622, 2-307456892)
- ❑ The ProxySG appliance reboots when attempting to connect to a BCAAA server due to a issue with authentication policy. (B#140743, SR#2-301043919)
- ❑ The authentication IP address obtained from explicit proxy is not invoked for the transparent proxy request. SR#2-280809302 (B#140104)
- ❑ The ProxySG appliance reboots when comparing an LDAP attribute value to a string. SR#2-262943652, 2-264212140, 2-284242312 (B#133826)
- ❑ Novell SSO logs out users intermittently after a period of inactivity. SR#2-282017183, 2-293271802, 2-306478391 (B#139807)
- ❑ The ProxySG crashes (requiring a manual restart) due to an access violation. SR#2-305857872 (B#141966)
- ❑ The ProxySG reboots when a RADIUS realm is shutting down due to a change in policy. (B#142370)
- ❑ When LDAP server sends invalid network address attribute to Novell SSO, it causes SSO to restart a full LDAP search. The search may find certain users with outdated timestamp and can trigger the SSO to logout those users unexpectedly. SR#2-294515082, 2-311558244 (B#142152)
- ❑ Timing issues due to multiple notifications of the same login and logout events and multiple LDAP servers can cause a "Old logon is newer" problem. As a result, an existing logon is discarded when no new logon exists. SR#2-311558244 (B#142150)

Section I: SGOS 5.4.5.1, build 51300

- ❑ An uninitialized variable causes BCAA to stop performing DCQ under certain conditions. SR#2-314418291 (B#143586)
- ❑ Heavy authentication load on ProxySG may cause a stack overflow if the LDAP server providing the authentication service is very slow to respond. SR#2-312210282 (B#142263)
- ❑ **Page cannot be displayed** is shown on client machines until it is manually refreshed due to redirect limitation on IE 7.0 & 8.0. SR#2-294830476 (B#139377)
- ❑ www.yahoo.com (and a few other sites) do not render correctly when transparent authentication is enabled. SR#2-308447572, 2-317102332 (B#143821)

Build

- ❑ The application's digital signature has an error due to expiration of a valid date. SR#2-311801222, 2-326027635 (B#142697)

Cache Engine

- ❑ Cache engine may choose an invalid disk as the initial master. (B#138316)
- ❑ Large content-filter database replication causes the ProxySG to reboot. SR#2-289800640 (B#137499)

CIFS

- ❑ Reflect client IP via forward policy does not work for CIFS. (B#145792)
- ❑ If CIFS files are deleted on the server, "Invalidated" directory entries can build up on the ProxySG, causing intermittent CPU spikes to 100%. (B#128008, SR#2-218197642, 2-286477322)
- ❑ Old CIFS sessions accumulate and cause active CIFS sessions to experience slowdowns during file transfer until the ProxySG is restarted. (B#139944, SR#2-295359948, 2-296448442, 2-298447612, 2-313665237, 2-317174044)
- ❑ Excel displays a **sharing violation** error while saving a file on a share, even though no other user has opened the same file. (B#140850)
- ❑ Lost connectivity to the ProxySG when "attempting to read a not present page" due to internal error. (B#142147)
- ❑ CIFS log needs to include connection and task pointers. (B#142251)
- ❑ CIFS Share is not accessible on the IBM AS/400. IBM system returns the following error message: **The specified server cannot perform the requested operation.** (B#135371)
- ❑ CIFS connection reading large amounts of server side data can cause intermittent, prolonged CPU spikes to 100%. (B#141746)
- ❑ CIFS proxy is unable to handle file names with special characters, causing file transfers to fail. SR#2-281762995 (B#139995)

Section I: SGOS 5.4.5.1, build 51300

- ❑ The ProxySG reboots while running less than 30 concurrent connections overnight. (B#144850)

CLI Consoles

- ❑ SSH write socket incorrectly displays error messages. (B#143252, SR#2-315974011)
- ❑ Certain Debug URLs not available to Read-Only administrators are accessible to Read-Only administrators. (B#143092, SR#2-313672657)
- ❑ Management Console becomes inaccessible, requiring the ProxySG appliance to be restarted in order to regain access to the Management Console. (B#145430, SR#2-318739292)

DNS Proxy

- ❑ The DNS negative cache entry for an original query yields non-name error while imputing suffix is configured. (B#139756, SR#2-298801338)
- ❑ The ProxySG always queries alternate DNS servers if the first response to SOA query does not contain a CNAME. (B#143272, SR#2-293086553)

FTP Proxy

- ❑ FTP proxy sends PORT or PASV command after REST but before RETR or STOR, causing the entire file to be downloaded from the beginning, instead of just the missing portion specified in the REST being downloaded. (B#136369, SR#2-277260002)
- ❑ Active mode data connections from the ProxySG to the client fails after upgrading from SGOS 4.x to 5.x. (B#141778, SR#2-254787871)

Health Checks

- ❑ When more than 100 health checks are created and a composite member is added, a circular reference error is reported. (B#141923, SR#2-310639642)

HTTP Proxy

- ❑ HTTP client connection is reset before the ProxySG transmits the entire modified ICAP Response from WebWasher. (B# 146166, SR#2-322851591)
- ❑ User randomly receives **500 Internal errors returned** messages when using a patience page. (B#137039, SR#2-285900872)
- ❑ The **HTTP 503 Error message** is not handled consistently by the HTTP proxy. (B#140037, SR#2-295452821)
- ❑ HTTPS traffic over HTTP CONNECT is denied by the policy engine at server-out when protocol detection is enabled without an SSL license. (B#140532, SR#2-295983609)

Section I: SGOS 5.4.5.1, build 51300

- ❑ The ProxySG reboots to a faulting instruction. (B#135105, SR#2-301429652, 2-301864322)
- ❑ The ProxySG might send an incomplete HTTP Response to the browser when the OCS sends a compressed response and the ICAP Server decompresses the content. (B#143860, SR#2-317171186)
- ❑ Safe-search policy is no longer effective for Ask.com, due to changes on their website. (B#140459, SR#2-297638943)

MAPI Proxy

- ❑ The ProxySG reboots due to client behavior resulting from an EPMapper design issue. (B#140433, SR#2-288667572)
- ❑ MAPI leaks memory on the ProxySG that intercepts MAPI connections due to allocation in the active sessions module not being freed after use. SR#2-289470861 (B#139664)

Management Console

- ❑ Error text misleads users into thinking that a transaction currently in process can continue without further ICAP processing. (B#140371, SR#2-296908212)
- ❑ The **Savings** column under **Statistics>Active Sessions** does not correctly sort items when **n/a** values are present. (B#140691, SR#2-300475571)
- ❑ When attempting to apply **Disable Master**, the following message displays: **Error in Committing Changes**. (B#142198, SR#2-310833472)

Network Drivers

- ❑ When the hardware security processor begins to fail, the ProxySG falls back to software encryption. This allows encrypted traffic to continue through the appliance. The following message will be posted to the system event log during that event: “Excessive timeouts on security processor, using software encryption”. (B#139919)

Policy

- ❑ While using the virus detect option in the web access layer with the allow rule to specific URL categories, users are denied access to websites that are should be allowed. (B#137928, SR#2-286885472, 2-291267292)
- ❑ The ProxySG reboots while writing `$(cs-auth-group)` after new policy is installed. (B#139974, SR#2-299071492)
- ❑ The ProxySG attempts to resolve wildcard host names under certain conditions. (B#139623, SR#2-297079193)
- ❑ Policy compilation does not generate any warning messages when `client.address` condition is used in the cache layer. (B#141573, SR#2-308097912)

Section I: SGOS 5.4.5.1, build 51300

SNMP

- ❑ High system memory utilization due to improper memory allocation causes SNMP timeouts. (B#139090, SR#2-295872166)

SSL/TLS & PKI

- ❑ When **SSL intercept** and **Server certificate validation** are enabled, the ProxySG returns a **SSL Certificate Hostname Mismatch (ssl_domain_invalid)** exception. (B#139753, SR#2-298268352)

System Statistics

- ❑ For multi-processor ProxySGs, a trap to trigger warning or critical states when CPU utilization percentage value passes thresholds is sent only for the first CPU (CPU-0). (B#139938, SR#2-295364488)

TCP/IP and General Networking

- ❑ Connect-error trigger for dynamic bypass does not function correctly. (B#141647, SR#2-293597162)
- ❑ High CPU usage in TCP and DNS when using `tcp-fast-finwait2-recycle`. (B#146141, SR#2-324166035)
- ❑ User-configurable options to reduce the number of instances where the TCP source port is reused too soon is not available. (B#139275, SR#2-288605142, 2-292429734, 2-298076102)
- ❑ The standard two hour keep-alive time out used by SGOS may cause problems with protocols that use this for client side keep-alive. (B#140631, SR#2-171190612)
- ❑ The log entry “Cannot establish connection” to the ProxyAV is seen in an event log with a lot of `FIN_WAIT_2` entries in the TCP connection table, due to many `FIN_WAIT_2` entries waiting for AV ICAP communication. (B#137966, SR#2-291526172)
- ❑ The `restore-sg4-config` command does not restore the `static-route-table` in an SGOS 4.x or 5.x configuration. SR#2-283894542, 2-302049917 (B#136270)
- ❑ The ProxySG will RST to CIFS protocol if VLAN tagging (Trunk) is enabled on bridge port. (B#139990, SR#2-294020042)
- ❑ Interfaces 0:0 - 0:3 on the ProxySG 9000 appliance lose connectivity because their ethernet addresses get reversed. (B#143392)
- ❑ The ProxySG reboots due to an internal driver issue. (B#143019, SR#2-312428552)
- ❑ The backup ProxySG in the SGRP group advertises excessively and could result in the backup ProxySG erroneously becoming the master for short periods of time. (B#142649, SR#2-301696882)

Section I: SGOS 5.4.5.1, build 51300

- ❑ When using multiple default gateways and static/RIP routing, the ProxySG switches over to RIP/static route when the interface is down, but it doesn't switch back to the interface route when the interface is back up. (B#126775, SR#2-207446592, 2-282960991, 2-290534592, 2-314313217)
- ❑ Packets are queued even when the interface is down. When the gateway interface is back up, all queued packets go out resulting in a flood of ARP packets. (B# 137338, SR#2-286317472)
- ❑ In the case of a misbehaving server that does not send FIN after the connection has been closed, the connection will hang around in `FIN_WAIT_2` state for 10 minutes. This duration is too long when a lot of connections are going to the same server that is misbehaving, eventually causing port exhaustion. This fix implements a faster timer (60 seconds as in FreeBSD 8.0) to clean up connections in the `FIN_WAIT_2` state. Please use this new CLI command to enable this fast timer:

```
#(config)tcp-ip tcp-fast-finwait2-recycle enable
```

(B#145266, SR#2-320946712, 2-323120232)

URL Filtering

- ❑ The ProxySG reboots due to Websense content-filter database corruption. (B#138210)
- ❑ CPU utilization is reported at 100% during content filtering database update task. (B#141967)

VPM Policy

- ❑ CPL becomes corrupted while performing the **Edit Category** action for policies which use URL Categories in their rules. (B#140020, SR#2-205413592, 2-299020301)

Windows Media

- ❑ Video stream fails to play when opened the first time. (B#133809, SR#2-263296161, 2-294040322, 2-296842170)
- ❑ In a ProxySG chaining deployment or in a forwarding configuration between two ProxySG's on port 554, playing Windows Media video on demand (VOD) files that are not in cache until the end, results in connections being leaked between the ProxySGs, client, and the Origin Content Server. (B#143096, SR#2-311699212)

Known Issues in 5.4.5.1

- ❑ Cookies set at the wrong level causes 'origin-cookie' to not work as expected for '.co.jp' domain URLs. (B#146465, SR#2-321409402)

CIFS Proxy

- ❑ An `assertion error` triggers at random times in the Event Logs. (B#120587, SR#2-314927441)

Section I: SGOS 5.4.5.1, build 51300

HTTP Proxy

- ❑ Internet Explorer 6.x users are unable to access Siebel 8 through the ProxySG unless pipelining to the server is disabled. (B#139572, SR#2-288338322)
- ❑ The ProxySG reboots due to a memory corruption issue. (B# 143612, SR#2-316716962)

ICAP

- ❑ Infrequent and non-service impacting error messages appear in the event log such as `Cannot establish connection to service Vontu` and `Cannot establish connection to service ProxyAV`. (B# 142662, SR#2-297064887, 2-319977085)
- ❑ ICAP weighting does not work correctly when waiting transactions. (B# 143280, SR#2-312673932)

Management Console

- ❑ Cannot select a row in the first column of ADN Inbound located at **Statistics>Sessions>Active Sessions>ADN Inbound**. (B# 144173, SR#2-313686401)

Network Drivers

- ❑ High number of `Input Errors` are seen on the Intel Gigabit dual/quad port passthru card. SR#2-320342602 (B# 145352)
- ❑ When a user-defined exception page is used, a blank page is displayed on the web browser if an exception is hit for a HTTPS URLs. This works fine with built-in exceptions & with HTTP URLs. (B# 146163, SR#2-318029485)

TCP/IP and General Networking

- ❑ The `restore-sg4-config` command does not restore the `static-route-table` in an SGOS 4.x or 5.x configuration. (B#136270, SR#2-283894542, 2-302049917)

VPM

- ❑ When using sequence authentication (IWA+LDAP), the LDAP username cannot be installed through VPM policy. The workaround is to use the LDAP realm only. (B#137588)

Windows Media

- ❑ The `x-duration` field is logged inconsistently for streaming URLs using the Silverlight plug-in on web-browsers due to Silverlight's deviation from normal operating procedures as mandated by the MS-WMSP protocol. (B#139720, SR#2-288378452)

Section J: SGOS 5.4.4.1, build 45872

Section J: SGOS 5.4.4.1, build 45872

Release Date: 5/26/2010, build 45872

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.4.1 Contents

- ❑ ["Fixes in 5.4.4.1"](#)
- ❑ ["Known Issues in 5.4.4.1"](#)

Fixes in 5.4.4.1

Access Logging

- ❑ Fixed a software restart in the "SSLW C40308D0" process in "kernel_shim.dll" at .text+0xcdc on SGOS 5.4.3.1.44023 when attempting to do a file I/O when the file wasn't open. (B#136858, SR 2-287779782, 2-288397389)
- ❑ Fixed a page fault in the "ALOGReader:main" process in "kernel_gcc.dll" at .text+0xa22e3, caused when attempting to log a disk I/O failure before its process configuration was initialized. (B#137384, SR 2-290127341)

Active Sessions

- ❑ Improved several messages in the Active Sessions detail area to show more usable information. (B#136630, SR 2-286530462)
- ❑ Fixed a page fault in the "CAG_Worker 55" process in "active_sessions.dll" at .text+0xa2f9 on an SG9000 running SGOS 5.4.2.30.43244. (B#138965, SR 2-295389832)

Authentication

- ❑ Fixed the BCAA LDAP thread deadlock, resulting in failure with Novell SSO authentication. (B#136279, SR 2-285420651)

Cache Engine

- ❑ Fixed the issue with prolonged high CPU usage due to incorrect handling of truncated objects (objects > 500K without a content-length header). (B#137760, SR 2-290257426)

CIFS

- ❑ Stopped the same CIFS client from being listed numerous times in Errored Sessions when a policy denies its connection. (B#136774)

Section J: SGOS 5.4.4.1, build 45872

CLI Consoles

- ❑ Fixed software restart in process "CLI_Worker_2" in "cli.dll" due to multithreaded, unsynchronized access to shared resources. (B#136730, SR 2-287176333)
- ❑ Fixed the issue when a SSH client errors out or disconnects prematurely causing all sessions to be used and a "CM sshd No more sessions available" message to be displayed and the SSH session on the ProxySG is not closed down. (B#137851, SR 2-281572042, 2-291488130)
- ❑ Fixed a software restart in the "director@ssh" process in "sshd.dll" at .text+0x1388d (buffer_append()). B#138277

HTTP

- ❑ Fixed a software restart in HTTP CW C4F4DEC0" in "transformer_dll.dll" at .text+0xbbf. (B#134756, SR 2-287999062, 2-294812162)
- ❑ Fixed a page fault at 0x86f4b000 in the "HTTP SW C4076F20 for C3C5EF20" process in "http.dll" at .text+0x566fb caused by an HTML page with the "base href" URL set to "http://" and caching turned off. (B#135558, SR 2-281795142)
- ❑ Fixed a software restart in the "tcpip" process in "tcpip.dll" at .text+0x1545fc, or when a corrupt message is sent to the originating content server when an incoming HTTP request has multiple "Cookie:" headers. (B#137789, SR 2-291425792)

ICAP

- ❑ Fixed connecting to a Vontu DCS from the ProxySG resulting in a stale Active Sessions being displayed as active. (B#125422, SR 2-287651282)

Kernel

- ❑ Fixed a page fault in the "osconfig" process in "Kernel.dll" at .text+0x1934 that occurred when a lost interrupt led to the system to get stuck on the serial port. (B#136761, SR 2-286279782)
- ❑ Fixed the issue where short (2 second) livelock events occurred every 10 seconds consistently throughout the day regardless of the traffic load. (B#137327, SR 2-285028590)
- ❑ Fixed a hardware restart (HWE0x2, SWE0x19, PF0x0) in the "Cache Administrator" process in "Kernel.dll" at .text+0x1b67f. SR 2-291765056 (B#138327)

Management Console

- ❑ Fixed the issue where the "Sense Setting" in ICAP Services was not reflecting the modified setting until the Management Console is logged in to again. SR 2-289073164 (B#137493)

Section J: SGOS 5.4.4.1, build 45872

Networkware

- ❑ Fixed the issue where low MTU causing large file transfers to be dropped in a MACH5 install with ADN optimization set to byte-cache while the server still shows the file has been transferred successfully. (B#138038, SR 2-287876221)

Policy

- ❑ Fixed URL rewrite statements being populated erroneously when compiled to policy. (B#136842, SR 2-287029621)

SOCKS

- ❑ Fixed the issue where the SOCKS proxy was terminating half-closed client TCP connections without waiting for response from the originating server. (B#136604, SR 2-279629501)

SSL

- ❑ Fixed the issue where SSL proxy failing when accessing <https://www.red-gate.com/> with Internet Explorer 8 with TLSv1 using Windows Vista. (B#132043, SR 2-219254993, 2-285254482)

TCP/IP and General Networking

- ❑ Fixed symmetric traffic flow preventing internet access due to a newly enabled proxy participating in WCCP and not being included in the assignment mask table. (B#134171, SR 2-257077301, 2-285735503, 2-292732352)
- ❑ Fixed the “restore-sg4-config” command not restoring the static-route-table in a 4x or 5x configuration. (B#136270, SR 2-283894542)
- ❑ Fixed RST packets from the ProxySG not be routed using stored return-to-sender or trust-dest-mac information. (B#137803, SR 2-290829559)
- ❑ Fixed a high memory utilization issue that caused the ProxySG appliance to stop servicing traffic. (B#135712, SR 2-321485462, 2-272524950, 2-280103492, 2-282911531, 2-286914182, 2-288158102, 2-290406579, 2-298503812)

URL Filtering

- ❑ Fixed high CPU utilization as often as every five minutes due to complete database rebuilds during BCWF auto updates. (B#138242, SR 2-286628122)

Windows Media

- ❑ Fixed a page fault in the "HTTP CW BC891EC0" process in "http.dll" caused by parsing corrupted HTTP Pragma headers during HTTP handoff to Windows Media. (B#137652, SR 2-285766752)

Known Issues in 5.4.4.1

Access Logging

- ❑ Uploading FTP client Access Logs to an FTP server fails after changing or toggling between the new and old FTP server IP address on SGOS 5.4.3.3. (B#138833, SR 2-290660564)

ADN

- ❑ Due to a truncated stream issue, the "Tunnel improperly closed" error message is displayed in the session log for CIFS connections that are being accelerated from the edge proxy. (B#136392, SR 2-271326683)

Authentication

- ❑ ProxySG does not use the BCSI_USERNAME value returned by SiteMinder. SR 2-283351865 (B#137658)
- ❑ Using LDAP protocol version 3 on Windows Server 2008 for LDAP authentication causes a software restart in the "LDAP Authenticator" process in "authenticator.dll" at .text+0x7d7e6. (B#138984, SR 2-295259481, 2-296420805)
- ❑ A redirect limitation in Internet Explorer 7.0 and 8.0 causes the 'Page cannot be displayed' message to appear on client machines until the page is manually refreshed. (B#139377, SR 2-294830476)

FTP

- ❑ ProxySG ftp-proxy sends either a PASV or PORT in between the REST and subsequent RETR (or STOR), and the REST is ignored, resulting in the entire file being downloaded from the beginning, instead of just the missing portion specified in the REST. (B#136369, SR 2-277260002)

Management Console

- ❑ Any changes done with the WCCP configuration interface overwrites any Text Editor configurations. (Limitation) (B#138424, SR 2-293602131)

Policy

- ❑ When the virus detect option is enabled in the web access layer and specific URL categories have an allow rule, users are denied access to URLs in the allowed URL categories. (B#137928, SR 2-291267292)

TCP/IP and General Networking

- ❑ Until the default gateway is pinged from SG CLI, and unrecognized host/address, or protocol error is received when attempting to ping hosts with static route defined. (B#126775, SR 2-207446592, 2-282960991)

Section J: SGOS 5.4.4.1, build 45872

SSL

- ❑ OpenSSL does not properly associate renegotiation handshakes with an existing connection, causing a security vulnerability. (B#136944, SR 2-239523102, 2-252882082, 2-279446222, 2-294222663)

VPM

- ❑ Unable to install LDAP username through VPM policy when using the sequence authentication (IWA+LDAP), which can be installed by using the LDAP realm only. (B#137588)

Section K: SGOS 5.4.3.7, build 45225

Section K: SGOS 5.4.3.7, build 45225

Release Date: 4/12/2010, build 45225

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.3.7 Contents

- ❑ "Changes in 5.4.3.7"
- ❑ "Fixes in 5.4.3.7"
- ❑ "Known Issues in 5.4.3.7"

Changes in 5.4.3.7

This section describes important changes in SGOS 5.4.3.7.

- ❑ Fix for CVE-2008-4609 Sockstress TCP Attacks reported in Blue Coat security advisory SA41 (B# 129157). For more information, see <https://kb.bluecoat.com/index?page=content&id=SA41&actp=LIST>
- ❑ Increased the max-cache-size value that can be entered in the ProxySG CLI and Management Console to 8.25 GB. (B# 134613)
Note: The ProxySG does not cache large objects greater than 4 GB when patience page is configured and the max-cache-size is greater than 4 GB. However, caching occurs when trickling is on. This limitation will be removed in a future release. (B#137657)

Fixes in 5.4.3.7

ADN

- ❑ Fixed the decompression errors that caused accelerated connections to fail when compression and byte caching are enabled using CommVault backup software. (B# 134858, SR 2-217479352)

Access Logging

- ❑ Fixed errors reported in the event log when trying to rotate the access log. B# 132411, SR 2-197540128, 2-216142772, 2-231439092, 2-237701062, 2-255184262, 2-268587360
- ❑ Fixed PF crash in process "ALOGAdmin:main" in "ce_admin.dll" at .text+0x30e6 when a new log object could not be created. (B# 135038, SR 2-279586852, 2-290127428)
- ❑ Fixed the failure of continuous access log updates to Websense. This failure was caused when an access log module passes in a zero length buffer to the zlib compression module. (B# 132358, SR 2-201686281, 2-249244073)

Section K: SGOS 5.4.3.7, build 45225

- ❑ Fixed the issue when using LDAP authentication, where the last letter of the username displayed in the access logs and in an exception page, if \$(user.name) is used, would always be truncated. (B# 135940, SR 2-282419503, 2-283016262, 2-285187382, 2-287635502)

Active Sessions

- ❑ Added enhancements to messages in the Active Sessions details to display more usable information. (B# 136630, SR 2-286530462)

Authentication

- ❑ Fixed the issue where SiteMinder authentication requests failed if the policy server was down when BCAAA attempts its initial connection. (B#133505, SR 2-194258912)
- ❑ Fixed the issue where SiteMinder or CoreID realm that is configured with a hostname instead of an IP address caused authentication failure. This was because the ICAP X-Authenticated header sent to the server did not contain the hostname. (B#120232)
- ❑ Fixed the issue that caused the ProxySG to stop processing TCP connections. This issue was caused due to intermittent connectivity problems with the LDAP server that triggered LDAP requests to build up faster than they could be processed. Under heavy load, it is possible to reach the 64 LDAP connection limit, and in this case, SG event logs this message: "The LDAP server is busy. The limit of threads waiting on LDAP operations has been reached." (B#135427)
- ❑ Fixed the restart in process "LDAP Authorizer" in "authenticator.dll" occurred when editing LDAP search & groups settings, changing "Membership" type value from "User" to "Group" and "Username" type from 'FQDN' to 'Relative'. (B#135012, SR 2-279246862)

CIFS

- ❑ Fixed the page Fault in process "CIFS::Worker: Connection 196029 (running)" occurred under heavy CIFS traffic while recovering from a socket error while sending data. (B# 133699, SR 2-262001355, 2-263265604, 2-264423562, 2-264446063, 2-289441472)
- ❑ Fixed the Catia CAD application tried to open a file which was already open from different session which did not allow the open to succeed and save did not complete. (B# 130102, SR 2-213908879)
- ❑ Excel file was corrupted when write back was enabled. This corruption was caused because the write and SFI requests were going out of order from client to server. (B#133071, SR 2-248086565)
- ❑ If CIFS files are deleted on the server "Invalidated" directory entries can build up on proxy. (B# 128008, SR 2-218197642, 2-286477322)
- ❑ Unique files rapidly deleted under load caused memory pressure. (B# 133705 SR 2-261143932)

Section K: SGOS 5.4.3.7, build 45225

- ❑ CIFS shares on NetApp servers become inaccessible due to increasing number of CIFS TCP connections, until the client PC or the SG is restarted. (B# 130960, SR 2-227221042, 2-231231856, 2-274212042, 2-281978232, 2-286785469)

Content Filtering

- ❑ Fixed DRTR background mode memory leak that resulted in memory regulation. (B# 134496, SR 2-265942201, 2-273908332, 2-279182422, 2-284536052, 2-285436649, 2-288233682, 2-288812952, 2-289525765)
- ❑ Fixed a boot up issue on the SG510 following a restart or an upgrade. (B# 136555, SR 2-285321539)

Forwarding

Fixed the issue where the host affinity feature did not function properly with sub domains. B# 127941

HTTP

- ❑ Fixed the issue with the prolonged high CPU usage due to incorrect handling of truncated objects (objects > 500K without a content-length header). (B# 134682, SR 2-250832612, 2-264201033, 2-286565641)
- ❑ Fixed HTTP proxy stops working due to truncation/non-cacheable entries in overflow blocks. (B# 132109, SR 2-237735122, 2-279338122)
- ❑ "Client HTTP requests" OID was not on par with Advanced URL HTTP Client Request statistic because the OID only tracks the GET requests. This issue has been fixed. (B# 136070, SR 2-284572101)
- ❑ WebFTP ignored unchanged modification time and continuously retrieved the file from the FTP server. This issue has been fixed. (B# 134616, SR 2-277385581)
- ❑ Fixed ProxySG reboot in "HTTP::Waiting_room::Handle_remove_entry, assertion at http_waiting_room.cpp:245, CK_Fatal_error (ERR_UNEXPECTED_STATE)" due to inability to remove object from Waiting_room hashmap. (B# 136320, SR 2-285254302)
- ❑ MACH5 Edition license on the ProxySG now has HTTP Compression support. Fixed the issue where the HTTP Compression CPL feature failed to gain client compression in the MACH5 Edition license. (B# 133855)

Health Checks

- ❑ Fixed the inability to revert from TCP back to a Composite for forwarding host's health-check type due to an incorrect equality check. (B# 133510, SR 2-261479001)
- ❑ Fixed the issue with the forwarding host's health check becoming unknown upon restart. This issue occurred when creating a composite health check with two user-defined aliases in it and changing the default forwarding health check from TCP to Composite. (B# 134128, SR 2-268503233)

Health Monitoring

- ❑ Fixed the false warning issue that caused the event log to report the power supply status being low or high on the SG9000. B# 134618

Instant Messaging

- ❑ Fixed the software restart in Process "IM_Admin" in "Kernel.dll" at .text+0x16c96 due to unexpected data sent from MSN client version 7.0. (B# 136393, SR 2-283406222)

Kernel

- ❑ Fixed the issue that caused the SG8100 to become unresponsive. This issue occurred under heavy traffic load, with no cache policy and external ICAP services enabled, causing periodic dips in performance and incomplete transactions. (B#134478, SR 2-262918462)

MAPI

- ❑ ProxySG drops connection in epmapper process while parsing BIND_ACK message that contains new accepted context item combination which was not observed earlier. This issue has been fixed. (B#135334, SR 2-279941305)

Management Console

- ❑ Fixed the issue that prevented sorting of data by Client or Server IP address in **Statistics > Errored Sessions > Bypassed Connections**. (B#134850, SR 2-271815925)

Policy

- ❑ Accessing `https://<SG_IP>:8082/Policy/Settings` from Internet Explorer or Firefox resulted in a software restart. This issue has been fixed. (B# 136570)

Real Media

- ❑ Fixed the page fault in process "RTSP_WM_Dispatcher" in "rtsp.dll" due to the handling of authenticated content that makes use of query-strings-based authorization. (B# 133191, SR 2-256851572)

SNMP

- ❑ Resolved the issue caused by a bug in the third-party net-snmp package with multiple error messages in logs similar to "error on subcontainer '' insert (-1)". (B# 133783, SR 2-262873311, 2-278262219)

SSL

- ❑ SSL contexts were not being flushed properly when modifying the Certificate Revocation Lists (CRL) allowing URL request until the proxy is restarted. This issue has been fixed. (B#132207)

TCP/IP and General Networking

- ❑ Fixed the rare case in the link propagation code that can cause both links into a deadlock state. (B#133513, SR 2-261080062)
- ❑ Fixed CERT-FI Advisory on the Outpost 24 TCP Issues / CVE-2008-4609. (B# 129157, SR 2-230464117, 2-237480705, 2-281438901)
- ❑ Resolved inaccessibility to the Internet with Trust-Destination-Mac enabled. This issue occurred in deployments where two interfaces on the ProxySG were transparently bridged and a third interface served as the Internet gateway. (B# 130608, SR 2-179804472)
- ❑ Increased the held buffer count to at least 4KB to help reduce performance issues that were caused by memory contention. (B#135718, SR 2-260192001)

WCCP

- ❑ Fixed the synchronization issues due to large I_SEE_YOU packets being generated by the WCCP router. (B# 134718, SR 2-257401431)

Known Issues in 5.4.3.7

ADN

- ❑ E-mail attachments are sometimes corrupted when a batch of e-mails with JPG or PDF attachments are sent in very quick succession. B# 137666, SR 2-286639272. This rare issue is not seen in Outlook 2007 or when Outlook cached-mode is disabled.

Authentication

- ❑ BCAA LDAP thread deadlocked resulting in failure with Novell SSO authentication. (B# 136279, SR 2-285420651)
- ❑ The ProxySG does not use the BCSI_USERNAME value returned by SiteMinder. (B# 137658, SR 2-283351865)

CIFS

- ❑ CIFS share is not accessible on IBM AS/400; The IBM system displays the error message, "The specified server cannot perform the requested operation." (B# 135371, SR 2-281541512)
- ❑ The same CIFS client is listed numerous times in **Statistics > Sessions > Errored Sessions** when a policy denies its connection. (B#136774)

Content Filtering

- ❑ At moderate traffic levels, when Websense RTU/RTSU updates are enabled, CPU is consistently high in policy evaluation. (B# 136554, SR 2-28260819)

HTTP Proxy

- ❑ Page fault at 0x86f4b000 in process "HTTP SW C4076F20 for C3C5EF20" in "http.dll" at .text+0x566fb is caused by an html page with a "base href" URL set to "http://" and caching turned off. (B# 135558)
- ❑ **Always-Verify-Source** policy option prevents trickle ICAP setting. (B# 136434, SR 2-284691482)
- ❑ Pressing F5 when downloading EICAR virus from eicar.org rotates between ProxyAV ICAP exception page and ProxySG exception page. (B# 136850 2-251039569)
- ❑ A 500 Internal error is randomly displayed when patience pages are used. (B# 137039, SR 2-285900872)

ICAP

- ❑ The **Sense Setting** in **Configuration > External Services > ICAP Services** does not reflect the modified setting until a you re-login to the Management Console. (B# 137493, SR 2-289073164)

Kernel

- ❑ Page fault in process osconfig in "Kernel.dll" at .text+0x1934 occurred when a lost interrupt led to the system to get stuck on the serial port. (B# 136761, SR 2-286279782)

Policy

- ❑ Memory regulation caused due to high memory usage in HTTP Policy evaluation. (B# 136055, SR 2-252872932)
- ❑ URL rewrite statement is populated erroneously when compiled to policy. (B# 136842, SR 2-287029621)
- ❑ During proxy chaining, FTP over SOCKS does not adhere to the forwarding layer rules configured on the parent proxy. (B# 137095, SR 2-285941116)
- ❑ If policy contains `http.response.apparent_data_type` condition, the request may be denied or stale content may be delivered. (B#137444, SR 2-289226982)
- ❑ When using sequence authentication (IWA+LDAP), LDAP username cannot be installed through VPM policy. The workaround is to use the LDAP realm only. (B#137588)

SNMP

- ❑ SNMP walk times out with a large number of active connections. (B# 135755, SR 2-281694709)

SOCKS

- ❑ SOCKS proxy terminates half-closed client TCP connections without waiting for response from the origin content server. (B#136604, SR 2-279629501)

System Statistics

- ❑ In the Management Console, the **Statistics > Traffic History > Service** tab displays negative bandwidth gain. Server bytes is larger than client bytes. (B#137491, SR 2-287403311)

TCP/IP and General Networking

- ❑ The `restore-sg4-config` command does not restore the static-route-table in a 4.x or a 5.x configuration. (B#136270, SR 2-283894542)
- ❑ Configuration and IP address on interface 2:0 does not display within the system configuration information. (B#135809, SR 2-282922553)
- ❑ An intermediate device injecting packets into the network can trigger the ProxySG to generate a TCP ACK storm. (B#137649, SR 2-289938482)

Windows Media

- ❑ Page fault in process "HTTP CW BC891EC0" in "http.dll" resulted from parsing corrupted HTTP Pragma headers during HTTP handoff to Windows Media. (B#137652, SR 2-285766752)

Section L: SGOS 5.4.3.3, build 44321

Release Date: 2/16/2010, build 44321

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.3.3 Contents

- ❑ "Fixes in 5.4.3.3"
- ❑ "Known Issues in SGOS 5.4.3.1"

Fixes in 5.4.3.3

ADN

- ❑ Fixed hardware restart in process "tcpip" in "tcpip.dll" that was caused by a race condition in which an internal process was returned as NULL, prohibiting the proxy from accepting new connections. (B#132607, SR#2-250828022)

Access Logging

- ❑ Fixed the page fault in process "libnet_admin" in "tcpip.dll" when enabling DNS imputing. (B#133413, SR#2-263659732, 2-263947432, 2-264509061, 2-274113752)
- ❑ Unable to upload access logs due to improperly deletion of access logs objects from hard drive disk. (B#133706, SR#2-238105042, 2-254711167, 2-260942512, 2-261833482, 2-263686038, 2-264065544, 2-264422431, 2-266258055, 2-274170723, 2-274472292, 2-277434542)

Authentication

- ❑ Read-only Admin access failed if the user didn't belong to the first authentication realm within a Sequence Realm list. (B#124908, SR# 2-204522405)
- ❑ The installer for BCAA version bcaa_5.4.2.2.41580.exe, wrote the Registry Key incorrectly into Window Registry, causing Event ID 1001 to be logged into the Windows Eventlog. (B#131523, SR#2-227406976)
- ❑ Fixed hardware restart 0xE in process "ALOGAdmin:main" in "access_log.dll" that occurred when the LDAP server returned a length longer than the original DN. (B#131076, SR#2-230403572)
- ❑ Windows server hosting the BCAA version 5.5.1.1.43412 became unresponsive and had to be restarted due to the increase of bcaa-130.exe's handle count. This particular problem was only seen by customers using Windows SSO with client query enabled and under heavy load. (B#132338, (SR#2-245989422, 2-263865146, 2-264462212)
- ❑ Resolved a race condition and two deadlock conditions in BCAA's domain Controller Query (DCQ) functionality. The race condition occurred when a user accessed resources in more than one domain at a time, and BCAA was querying both domains. (B#132804, SR#2-246343441)

- ❑ "Username could not be converted to Kerberos name" when the domain name contained a "@" symbol. (B#133651, SR#2-208501232)

CLI Console

- ❑ Removed SSH message `Read from socket failed: Return code zero(0) SEVERE_ERROR` from logging to system-level event logs. This message was not a "SEVERE_Error". (B#132442, SR#2-250790611)
- ❑ Fixed restart in process "admin@ssh" in "cli.dll" when the SSH client session was improperly closed. (B#132845, SR#2-253104604)

Content Filtering

- ❑ Slow performance occurred during BCWF update when the default option "The Automatically Check for Updates" is enabled. (B#133012, SR#2-239679305, 2-255385822, 2-256212332, 2-257980002, 2-261046872)
- ❑ Fixed the issue that caused a failure to load the Websense content-filtering database after upgrading to 5.4.3.1. This failure to load the database rendered all URL categorization requests to be "unavailable". (B#133906, SR 2-262965812, 2-263370782, 2-263512532)

Documentation

- ❑ Documented the CLI command `return-to-sender overwrite-static-route`. (B#133825, SR#2-262956266)

HTTP Proxy

- ❑ When Two-Way URL rewrites with Authentication enabled were done, cached content was not compressed when a 304 response code was returned from the origin content server. (B#134023, SR#2-261918621)

Policy

- ❑ Fixed the problem of multiple hardware restarts in process "tcpip" in "" at .text+0x0 when the access log attempted to retrieve the source IP. address at that time. (B#132071, SR#2-239513438, 2-244559007)

Services

- ❑ SNMP manager received error message "Destination unreachable" when Source UDP port was MMS (1755). (B#132876, SR#2-254093012)

Streaming Media

- ❑ Windows Media Proxy: Fixed a hardware restart in process "RTSP_WM_Dispatcher" in "rtsp.dll" that occurred on multi-processor ProxySG's, when playing RTSP and HTTP based Media. (B#134075, SR#2-263799088)

TCP/IP and General Networking

- ❑ Network_Driver: Fixed hardware restart in process "Idler 0" in "tcpip.dll" at .text+0xb948f due to a race condition. (B#127295, SR#2-216014353)
- ❑ Fixed restart in process "closesocket::req::process()" that occurred when a peer closed the connection before it was properly accepted. (B#132354, SR#2-255766981)
- ❑ The external interface of the ProxySG responded to ICMP packets when the “**Firewall Incoming Traffic**” was enabled. (B#133101, SR#2-255682342)
- ❑ Fixed a problem that caused asymmetric traffic flows which prevented internet access. The problem was caused by a race condition in which a newly enabled proxy participating in WCCP was not included in the assignment mask table. (B#134171, SR#2-257077301)

Known Issues in 5.4.3.3

Access Logging

- ❑ Continuous Access Log upload via FTP client fails with a 426 Response Code from the FTP server. Periodic uploading works fine. (B#130366, SR#2-185938257)
- ❑ Errors reported in the event log when trying to rotate the access log. (B#132411, SR#2-231439092, 2-237701062)

CIFS_Proxy

- ❑ CIFS file save takes longer than expected when ADN and CIFS are both enabled. (B#129279, SR#2-193675919)
- ❑ Page Fault in process "CIFS::Worker: Connection 196029 (running)" occurs under heavy CIFS traffic while recovering from a socket error while sending data. (B#133699, SR#2-262001355, 2-263265604, 2-264423562, 2-264446063)

CLI Console

- ❑ Local Database content filtering auto update with FTP ignores unchanged modification time and continuously downloads the file. (B#134616, SR#2-277385581)
- ❑ Console does not accept max-cache-size larger than 2047 MB. (B#134613, (SR#2-277200197)

Documentation

- ❑ The help documentation in the management console displays "**The DNS System Cache dialog appears**" message for the DNS, object, and byte cache; the message should be specific to each type of cache. The PDF documents (on BlueTouch Online) have been updated though the online help continues to display the error (until there is a new help build). (B#132412, SR#2-246008602)

Health Checks

- ❑ Unable to revert from TCP to Composite-result for forwarding host's health-check type. (B#133510, SR#2-261479001)
- ❑ When a composite health check is created with two user-defined aliases in it and the default forwarding health check is changed from TCP to Composite, the health check changes to unknown upon reboot. (B#134128, SR#2-268503233)

HTTP Proxy

- ❑ HTTP Compression CPL feature fails to gain client compression in MACH5 Edition proxy. (B#133855, SR#2-261824973)

Streaming Media

- ❑ Page Fault in process "RTSP_WM_Dispatcher" in "rtsp.dll" due to the handling of authenticated content that makes use of query-strings-based authorization. (B#133191, SR#2-256851572)

TCP/IP and General Networking

- ❑ Internet traffic stops working after upgrade to 5.4.1.1 because of "Trust-Destination-MAC" behavior. (B#130608, SR#2-179804472)

Section M: SGOS 5.4.3.2, build 44285

Release Date: 1/26/2010, build 44285

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.3.2 Contents

- ❑ ["Fixes in 5.4.3.2"](#)

Fixes in 5.4.3.2

Content Filtering

- ❑ Fixed the issue that caused a failure to load the Websense content-filtering database after upgrading to 5.4.3.1. This failure to load the database rendered all URL categorization requests to be "unavailable". (SR 2-262965812, 2-263370782, 2-263512532) (B#133906)

TCP/IP

- ❑ Page Fault in process "libnet_admin" in "tcpip.dll" when enabling DNS imputing. (SR# 263659732, 2-263947432) (B#1334132)

Section N: SGOS 5.4.3.1, build 44023

Release Date: 1/12/2010, build 44023

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.3.1 Contents

- ❑ "New Features in 5.4.3.1"
- ❑ "Fixes in 5.4.3.1"
- ❑ "Known Issues in SGOS 5.4.3.1"

New Features in 5.4.3.1

No new features are introduced in SGOS 5.4.3.1.

Fixes in 5.4.3.1

Access Logging

- ❑ Access logs now display usernames when Sequence-Realms are used for authentication with Websense content filtering. SR 2-205703131 (B#125103)
- ❑ The default early upload threshold is set to 80% of the maximum access log file size. The maximum access log file size is restricted to 25% of the smallest disk size or is capped at 20GB for ProxySG appliances with large storage capacity, such as the SG9000. Therefore, on the SG9000, the early upload threshold value translates to 16GB. (B#125695)

ADN

- ❑ Fixed the issue with metadata file corruption when ADN data streams exceeded the maximum limitation. SR 2-209068553 (B#125141)
- ❑ Fixed the hardware restart that occurred under heavy load causing numerous events (Check_update_history_impl) within the syslog. SR 2-219669522 (B#128616)
- ❑ Fixed the open managed ADN issue where an ADN control connection was not established after the core or ADN manager was upgraded to 5.5. (B#126809)

Authentication

- ❑ Fixed the issue that prevented archives from being restored in a sequence realm that contained an IWA realm. The show config command incorrectly displayed the iwa-only-once enable property as ntlm-only-once and prevented archives from being restored. SR# 2-194294432 (B# 122052)
- ❑ Fixed proper table updates when TCP client connection reach the maximum limitation. SR 2-215726252 (B#124465)

- ❑ Fixed high CPU utilization and system restarts caused when BCAAAs “novell_primary_file” data file was locked by another application process, which caused a large volume of log entries to the hard disk. SR 2-202912011(B#124653)
- ❑ Fixed memory leaks in the LDAP Authentication and Authorization process. SR 2-199034692, 2-243987672 (B#126389)
- ❑ Fixed the memory regulation issue caused by BCAA-130.exe continuously consuming server memory. SR 2-227093371, 2-236586822, 2-240057232 (B#130505)

CIFS

- ❑ Browsing a folder occasionally displayed an error in sg_5_4 Fileserver - Novell Netware with ADN enabled. This issue has been fixed. SR 2-189415752. (B#122785)
- ❑ Resolved the corruption of PDF files when uploaded over CIFS by a Multifunction Printer for WAN optimization. SR 2-210072022 (B#127073)
- ❑ Fixed the Active Session error, "Read length 65435 is larger than connection max 61440" for clients transferring PACS (Picture Archive and Communication System) files due to the custom application reading more than 60K of data. SR 2-199295631. (B#123713)
- ❑ Excel files no longer display a read-only error when accessed over ADN with writeback enabled. SR 2-209144102 (B#127405)
- ❑ Resolved the inability to transfer PDF files through ADN using the “write-back none” function. SR 2-220921666. (B#128695)
- ❑ Fixed the race condition that caused CIFS connection workers to block system processes rendering the Management Console and CLI inaccessible. SR 2-218526982, 2-220784682, 2-222432032, 2-223455792. (B#128831)
- ❑ Fixed the logging of numerous entries that read “Can't find session <number>” in the access logs. SR 2-222654498 (B#129716)

CLI Console

- ❑ Fixed the error that displayed There was 1 error and 0 warning, when installing an SGOS build image which already resided on the system. (B# 109470)
- ❑ Connectivity issues when accessing the SSH console have been resolved. SR 2-187139753, 2-217239013, 2-238216421. (B#119021 and 129428)
- ❑ Fixed restart error when the client closed and reopened an SSH connection. SR 2-203413841, 2-203437060. (B#119778)

Content Filtering

- ❑ Fixed the error where the `exception.category` field did not display the category that caused the exception message to display. SR 2-190914662 (B#122872)

- ❑ Fixed the condition that stopped the processing of HTTP traffic while checking the size of the DRTR cache. SR 2-237963662 (B#131735)
- ❑ Fixed high CPU usage when Dynamic Real Time Rating (DRTR) is enabled. (B#129689)

Documentation

- ❑ Updated the Advanced Networking volume of the CMG and the online help to fix the error in the `client attack-detection` configuration values. SR 2-203531362. (B#124427)
- ❑ Updated information on the traffic statistics displayed on the **Statistics > Summary** page of the Management Console. SR 2-223120781 (B#130600)
- ❑ The maximum number of DNS suffixes that can be configured on the ProxySG is 6. The CMG has been updated; This information is not included in the online help. 2-236672162 (B#131315)

Event Logging

- ❑ Fixed the corruption in the RAM logging structures that caused page faults and infinite loops. (B#124741)

FTP

- ❑ Fixed the issue that caused the 501 Not Implemented error message for HTTP HEAD request for objects on FTP servers. SR 2-201553692 (B#125799)

Health Checks

- ❑ Fixed the health checks issue that caused artificially high numbers for DNS resolution. This was triggered by the proxy looking for the AAAA record for an entry rather than the A record. SR 2-218061560. (B#128932)

Hardware

- ❑ Fixed the system restart caused by a race condition when the kernel accessed the hardware real time clock. SR 2-231383672, 2-238917792 (B#131109)

HTTP Proxy

- ❑ Fixed the page fault that was caused by a multi-thread race condition between two HTTP client workers attempting to update the same form-based authentication object. SR 2-213819062, 2-238375062 (B#127404)
- ❑ Fixed Sharepoint application behavior, where MS Office Sharepoint check-in procedure did not accelerate as expected. SR 2-195858292 (B#122061)
- ❑ Fixed the restart that occurred when the cache engine fails to cache response headers greater than 8K. (B#125781)

- ❑ Fixed the application error that was caused when a patience page was delivered for a large object using ICAP response modification. The application error was triggered by the termination of the request by the server.
SR 2-194499202, 2-200005532 (B#127667)
- ❑ Fixed a software restart issue that was caused due to a conflict between duplicate retrieval workers while processing transaction objects.
SR 2-214593193 (B#130854)
- ❑ Fixed the software restart that was caused due to a conflict between multiple server workers operating on different CPUs in a multi-processor system, while updating an SSL transaction object. SR 2-236731528 (B#131637)
- ❑ Fixed the TCP timeout from the OCS that occurred during a large file download. SR 2-211011392 (B#131725)

ICAP

- ❑ The multi-thread race condition that occurred when two different processes access and change the content of the same service object simultaneously has been fixed. SR 2-224376367. (B#122289)
- ❑ Fixed the ICAP error that occurred when downloading a file larger than 1MB and preview is enabled. SR 2-205901652. (B#122389)
- ❑ Fixed the error in restoring the ICAP REQMOD (request mode) configuration. SR 2-197395082. (B#122713)
- ❑ ICAP policy was not applied when executed using F5 function until the object is removed from cache. This issue has been fixed. SR 2-214714158, 2-218274212, 2-218466768 (B#127501)
- ❑ Fixed the issue where the ICAP server dropped connections when the ICAP deferred threshold was set to 0 manually, instead of being configured using “sense-setting” function. SR 2-216133840 (B#127900)

IM

- ❑ Fixed the MSN server connection time out that was caused by inactivity. The connection was RST by the server without sending any data. SR 2-197146401. (B#122285)
- ❑ Fixed the restart that occurred when attempting to read a non existing page. SR 2-196749802, 2-206879291. (B#122384)
- ❑ Fixed a restart in process "tcpip" in "tcpip.dll" at .text+0x38c11 caused by an invalid socket being retrieved after the IM session was closed. SR 2-216146882 (B#124107)
- ❑ Fixed the system restart in process "RTSP_WM_Dispatcher" in "rtsp.dll" at .text+0x82ced (Parse_play_params) caused by the improper handling of Unicode files. SR 2-216035399 (B#127291)
- ❑ Fixed IM memory consumption that caused the proxy to hang and stop processing traffic. SR 2-225199775 (B#130227)

- ❑ Fixed the network error issue when Windows Media client failed to recover from TCP-retransmission due to bandwidth limitation on an 800/kbit live stream. SR 2-214014595 (B#131287)
- ❑ Fixed the Yahoo file transfer failure when IM was tunneled and HTTP handoff was enabled. (B#121977)

IP v6

- ❑ Fixed the issue where a transparent DNS proxy to an IPv6 DNS server requests the source IP address instead of the server IP address. (B#120693)

Policy

- ❑ Fixed the error in the policy exception page that gets generated for the client-facing HTTP response. This issue manifested as an incorrect HTTP response code in the access log. SR 2-207420733, 2-208094422, 2-218357049. (B#125699)
- ❑ Fixed the issue with the VPM menu not displaying as a scrollable list. When using Director running SGME 5.4.2.4, the action items in the Online VPM were not visible. SR 2-222823932, 2-230469532, 2-238137592 (B#131224)
- ❑ Fixed the policy re-evaluation error that caused a system restart. SR 2-239035459 (B#131771)

Services

- ❑ SNMP service was unresponsive after certificates are imported and or removed. This issue has been fixed. SR 2-240392041 (B#123722)

Storage

- ❑ Fixed the repetitive read block error messages reported in the event log. This error was caused by the failure to track input output errors on the hard disk. (B#124690)
- ❑ Fixed the HTTP transaction failure that resulted in an ICAP communication error (internal error code 51). This error was caused by an empty cache object being passed from HTTP to ICAP scanning. SR 2-217823831 (B#127799)

SOCKS

- ❑ Fixed the issue where SOCKS authentication succeeded when using a valid username with a blank password. SR 2-224710502 (B#130218)

TCP/IP and General Networking

- ❑ Fixed the issue with static routes not displaying CIDR notation. SR 2-241096552 (B#117903)
- ❑ DNS imputing names were missing from the **post setup archive** configuration option. This issue has been fixed. SR 2-197625295 (B#122864)

- ❑ Fixed the rare race condition whereby the Proxy interface entered into a temporary disable mode resulting in packet delays between WCCP processing and transmission on the wire. SR 2-197275783, 2-199781725, 2-201497621, 2-203281302, 2-209123381, 2-210974172, 2-220824917. (B#122931)
- ❑ Resolved issue where the Gigabit Fiber interface on the ProxySG 810 did not link up after a software restart. SR 2-203694201. (B#124699)
- ❑ Fixed the software restart in process "tcpip" in "tcpip.dll" at .text+0xBF411 when a TCP Tunnel is setup by the HTTP worker. SR 2-200749132. (B#125751)
- ❑ DNS imputing suffixes stops working when the total number of characters of all the entries of the imputing list exceeds 76. This issue has been fixed. SR 2-209081151, 2-218239495 (B#126442)
- ❑ Fixed restart in process "tcpip" in "tcpip.dll" at .text+0x64738 that occurred when return-to-sender inbound is enabled on a bridged VLAN. SR 2-209392372 (B#126548)
- ❑ Repeated WCCP port numbers are not retained if WCCP was configured from the Management Console. SR 2-222682503 (B#129362)
- ❑ Fixed EMCP health checks that sent multiple ARP requests causing network latency. SR 224703353. (B#130067)
- ❑ Fixed a page fault in process "tcpip" in "tcpip.dll" at .text+0xe9f30 when the proxy received an incorrect TCP option length. SR 2-225374991 (B#130086)
- ❑ Fixed the software restart in process "HC Watchdog" in "kernel_shim.dll" at .text+0xcde when issuing 'show health-checks'. SR 2-224412625 (B#130309)
- ❑ Fixed a memory leak that caused the ProxySG to hang and stop processing any service after upgrading to SGOS 5.4.2.2. SR 2-227371342 (B#130394)
- ❑ Fixed a memory regulation issue that was due to excessive DNS memory consumption when DNS recursion is enabled. SR 2-209827822, 2-221642501, 2-236765474, 2-237497321 (B#131244)

Time

- ❑ Fixed the severity of the error message that is logged when the ProxySG detects a minor discrepancy between the system clock and the NTP server time update.(B#131977)

WCCP

- ❑ Fixed the issue with WCCP when the ProxySG reported WCCP status as ready although the home router was inaccessible. This issue occurred if the WCCP home-router IP address was modified from a valid IP address to an unresponsive IP address after the WCCP negotiation was completed. (B#122748)
- ❑ Fixed the inability to configure WCCP web-cache for WCCP version 2 using the Management Console. SR 2-204657491 (B#125258)

Known Issues in SGOS 5.4.3.1

Access Logging

- ❑ Streaming access-logs are not generated when HTTP Handoff is enabled. SR 2-236824972 (B#131587)
- ❑ Continuous access log upload using an FTP client fails with a 426 Response Code from the FTP server. Periodic uploading works fine. SR 2-185938257 (B#130366)
- ❑ Errors are reported in the event log when the access log is rotated. SR 2-231439092, 2-250665526 (B#132411)

Authentication

- ❑ Read-only Admin access fails if the user doesn't belong to first authentication realm within a Sequence realm list. SR 2-204522405 (B#124908)
- ❑ SOCKS authentication succeeds when a blank password is provided for a valid username. SR 2-224710502 (B#130218)
- ❑ The BCAA installer for SGOS version 5.4.2.2. (bcaa_5.4.2.2.41580.exe), writes the registry key incorrectly in the Window registry causing Event ID 1001 to be logged in the Windows eventlog. SR 2-227406976 (B#131523)
- ❑ When restoring a configuration to a ProxySG, the realms contained within Sequence realms are displayed out of order. SR 2-227798182 (B#131956)
- ❑ The Windows server hosting the BCAA version 5.4.3.1 or 5.5.1.1.43412 becomes unresponsive and must be restarted in networks that are under heavy load and are using Windows SSO realms with client query enabled. This is due to an increase in the handle count for bcaa-130.exe. For IWA, SiteMinder, or COREid realms this issue does not occur.
Workaround: To prevent this issue, set the MaxSSOThreads to zero in BCAA's sso.ini file. SR 2-245989422 (B#132338)

CLI Console

- ❑ The CLI displays **NTP enabled instead of NTP is enabled using Blue Coat's NTP servers.** This message is erroneous because NTP is enabled only for Bluecoat NTP server. B#131726, SR 2-233867949
- ❑ The ProxySG does not display a warning message when installing the same policy rule twice from the text editor. B#131079, SR 2-230908952

Documentation

- ❑ The online help records the Clear Object Cache dialog incorrectly as Clear DNS Cache. This error displays in the instructions for Clearing the Object Cache task in **Maintenance > System and disks > Tasks.**
Note: This error has been fixed in the PDF of the Configuration and Management Guide which is posted on the Blue Touch Online portal.
SR 2-246008602 (B#132412)

- ❑ The screenshot for the Add Permit Authentication Error Object in the VPM Reference Guide does not match the user interface.

Network Drivers

- ❑ Hardware restart in Process "Idler 0" in "tcpip.dll" at .text+0xb948f due to a race condition. SR 2-216014353 (B#127295)

Policy

- ❑ Multiple hardware restarts occur when the access log attempts to retrieve the source IP address. SR 2-244559007 (B#132071)

Streaming

- ❑ Windows Media over HTTP fails when the URL format is `http://<Proxy_SG_IP>/redirect?mms://<streaming_server>/<filename>.wmv`
The workaround is to use `http://<Proxy_SG_IP>/redirect?http://<URL>` instead of using `http://<Proxy_SG_IP>/redirect?mms://<URL>`
SR 2-198319392 (B#124346)

TCP/IP and General Networking

- ❑ CERT-FI Advisory on the Outpost24 TCP issues / CVE-2008-4609.
SR 2-230464117, 2-237480705 (B#129157)

Section O: SGOS 5.4.2.11, build 42967

Release Date: 11/23/2009, build 42967

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.2.11 Contents

- ❑ "Changes in 5.4.2.11"
- ❑ "Fixes in 5.4.2.11"

Changes in 5.4.2.11

No new features are introduced in SGOS 5.4.2.11.

Fixes in 5.4.2.11

ADN

- ❑ After a restart, a priority condition between initial ADN dictionary loading and HTTP traffic caused a temporary delay in URL response time when loading large byte-cache dictionaries. (SR# 2-205737189, B#125638)
- ❑ The ProxySG occasionally stopped responding to new ADN connections when connectivity between ProxySG appliances was lost for more than three minutes, or when one of the ProxySG appliances rebooted while a stream deletion was taking place. The ProxySG could run into a deadlock after it came back online, which triggered an dictionary re-sync. Stream deletion can take place as a result of a full dictionary or the clear-cache byte-cache command. (SR#2-217795492, 2-218165942, B#128108)

Authentication

- ❑ The BCAA service's "novell_primary_file" data file was locked by another application process causing events to fill the hard disk, resulting in high CPU utilization and system restarts. (SR# 2-202912011, B#124653)
- ❑ Novell SSO: The novell_primary_inc.sso file grew too large. The Novell SSO code scans the list of logged-in users and initiates an update of logged-in sessions whenever users have recently logged out. Under certain conditions, a thread could get stuck in an infinite loop repeatedly updating the same set of login events. Each of these events caused a new entry to be written to novell_primary_inc.sso, which caused this file to rapidly increase in size.
(SR# 2-191653613, 2-193582722, 2-202912011, 2-203795112, 2-204291792, 2-210225452, 2-217073672, 2-217128811, 2-223771168, 2-227306458, 2-227798162, 2-236711570, B#129775)

CIFS Proxy

- ❑ Clients transferring PACS (Picture Archive and Communication System) files received the following error under Active Session: "Read length 65435 is larger than connection max 61440." This was due to the custom application reading more than 60K of data. (SR# 2-199295631, B#123713)
- ❑ A race condition caused CIFS connection workers to block system processes, rendering the Management Console and CLI inaccessible. (SR#2-218526982, 2-220784682, 2-222432032, 2-223455792, B#128831)

Content Filtering

- ❑ Disk failures could have caused the loss of categorization service. (B#122152)
- ❑ SmartFilter databases failed to build when using an SL database. (SR#2-221830522, B#123593)

HTTP Proxy

- ❑ Malformed characters found in ICAP e-mail alerts when using the "notify_email" property and \$(icap_error_details) variable. (SR#2-177493371, B#120747)

ICAP

Setting the "Deferred ICAP threshold" to 0 did not scan as expected, causing slow scanning performance and exceeding the maximum queued connection on the ProxyAV. (SR# 2-196941842, B#122900)

Kernel

Boundary condition existed in which small NTP correction could corrupt internal timers. Could manifest as 'stuck' transactions, DNS lookups, and exhaustion of client workers. (SR#2-189457002, B#120624)

MSN Instant Messenger

When the MSN server connection timed out because of inactivity, it was closed (RST) by the server without any data sent. (SR# 2-197146401, B#122285)

Networking

- ❑ TCP connection timeout values are configurable between 10 and 90 seconds using the "tcp-ip tcp-connect-timeout" command within CLI. (B#124446)
- ❑ Due to a rare race condition, the Proxy interface entered into a temporary disable mode, resulting in packet delays between WCCP processing and transmission on the wire. (SR#122931, 2-197275783, 2-199781725, 2-201497621, 2-209123381, B#122931)

SSH Console

Session leak on failed SSH console access. (SR#2-187139753, B#119021)

SSL Proxy

Mozilla Firefox 3.5 rejected the CA certificate generated by the ProxySG, resulting in the following error: “This is not a certificate authority certificate,” thus prohibiting the certificate from being imported. (SR#2-201459052, B#123865)

Storage

- ❑ Software restart in process "Cache Administrator" in "ce_admin.dll" occurred when the Cache Engine processed large list queues under heavy load conditions. (SR#2-201851132, B#123724)
- ❑ Failure to track IO errors on hard disk could result in repetitive read block error messages reported in the event log. (B#124690)

Section P: SGOS 5.4.2.2, build 41580

Release Date: 08/10/2009, build 41580

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x and Reporter 9.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.2.2 Contents

- ❑ "Changes in 5.4.2.2"
- ❑ "Fixes in 5.4.2.2"
- ❑ "Known Issues in SGOS 5.4.2" on page 89

Changes in 5.4.2.2

No new features are introduced in SGOS 5.4.2.2. SGOS 5.4.2.1 was made available as a pre-release and includes new features. See [Section Q: "SGOS 5.4.2.1, build 40763"](#) on page 91.

Fixes in 5.4.2.2

ADN

- ❑ Corrected an issue that caused a duplicate serial number detection *false alarm*. (B#121748)

Authentication

- ❑ BCAA failed to free SSPI Context Handle when Kerberos is selected, resulting in Handle leaks. (B#123959, SR# 2-198120386)

Content Filtering

- ❑ Memory error when downloading the Websense database caused a restart. (B#123190)

Known Issues in SGOS 5.4.2

Network

- ❑ Relying on **auto-sense** where both the ProxySG and its link partner are not both set up for auto-negotiation is problematic and can cause down interface links. Blue Coat recommends manually setting the speed and duplex appropriately. (B#108779)

Doc Errata in SGOS 5.4.2

- ❑ Post-production, an error was discovered in the documentation section regarding Attack Detection. This error was corrected in *Volume 5: Advanced Networking*, Chapter 3: Preventing Denial of Service Attacks, but the Online Help System still contains the incorrect information. Specifically, erroneous information is in some of the CLI help text. As accessed from the ProxySG, the CLI help text is correct. The Online Help should read:

- SGOS#(config client) **default connection-limit**
integer_between_1_and_65534

Online Help displays 65535.

- Table 3-1: default connection-limit description: Indicates the number of simultaneous connections between 1 and 65534.

Online Help displays 65535.

- Step 4:

SGOS#(config client ip_address) **connection-limit**
integer_between_1_and_65534

Online Help displays 65535.

SGOS#(config client ip_address) **failure-limit**
integer_between_1_and_500

Online Help displays 1_and_65535.

SGOS#(config client ip_address) **unblock-time** *minutes*

Online Help displays 1_and_65535.

SGOS#(config client ip_address) **warning-limit**
integer_between_1_and_100

Online Help displays 1_and_65535.

- Table 3-2 displays similar errors in the Online Help.

Section Q: SGOS 5.4.2.1, build 40763

Release Date: 07/29/2009, build 40763

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.2.1 Contents

See the following sections for information on this release.

- ❑ ["Changes in 5.4.2.1" on page 91](#)
- ❑ ["Fixes in 5.4.2.1" on page 92](#)
- ❑ ["Known Issues in 5.4.2.1" on page 100](#)
- ❑ ["Access Logging" on page 138](#)
- ❑ ["Doc Errata in 5.4.2.x" on page 102](#)
- ❑ ["SGOS 5.4.x — Limitations and Support for Other Products" on page 138](#)

Changes in 5.4.2.1

This section describes important changes introduced with SGOS 5.4.2.1.

Content Filtering

New Management Console Feature

The new feature enables you to select the new Category 3 map set (not selecting retains the default: the Category 2 map set). This option is on the **Configuration > Content Filtering > SmartFilter** Management Console page. If you select **Specify Category Map Version** and select **Version 3**, you must re-download the database and re-evaluate the policy (the same applies if you in time re-select **Version 2**). A dialog displays that informs you that because of differences in category names and contents, ensure that your current policy meets your corporate regulations and alter if necessary.

New CLI Commands

There are new CLI command that accomplish what was described in the previous section:

```
#(config smartfilter) category-map-version default
#(config smartfilter) category-map-version 2
#(config smartfilter) category-map-version 3
```

Category Support

On May 28, 2009, McAfee released Category Set 3 for their TrustedSource Web Database (also known as SmartFilter). This release includes the addition of two new categories and the deprecation of two categories. You can review McAfee's release document regarding the Category Set 3 release at:

<https://kc.mcafee.com/corporate/index?page=content&id=PD21783&actp=LIST>

Health Checks (MACH5)

When running SGOS with a MACH5 license, the following Health Check pages are now available in the Console:

- ❑ **Configuration > Health Checks > General**
- ❑ **Configuration > Health Checks > Background DNS**

Note: The CLI equivalents to these options are also available.

The following VPM objects are also now available:

- ❑ **SSL Access Layer > Service > Health Check**
- ❑ **Web Access Layer > Service > Health Status**
- ❑ **Forwarding Layer > Service > Health Check**
- ❑ **Forwarding Layer > Service > Health Status**

User-defined health checks are also supported. All of the functionality is the same as the ProxyEdition license. Refer to the Help pages.

Fixes in 5.4.2.1

This section describes fixed issues in SGOS 5.4.2.x.

Access Logging

- ❑ The ProxySG restarted when uploading the access log to a Websense server. (B# 117572, SR# 2-181663987, 2-186108108, 2-189163912, 2-191624684)
- ❑ The MAPI access log field `x-mapi-user-dn` did not record the value of the `userDN` string, and set the value as `-`. (B#109425)

Active Sessions

- ❑ Memory management problem caused system crashes. (B# 122363, SR# 2-195872011, 2-199947807, 2-200162653)
- ❑ When ADN was enabled, accessing **Management Console > Active Sessions > ADN Inbound Connection** and clicking the **Show** tab twice, caused the proxy to hang and stop passing traffic. This also occurred when accessing the serial console and executing the `show cpu` and `show configuration` commands. (B# 118986)
- ❑ HTTP proxied sessions were not displayed under **Statistics > Sessions > Active sessions > Proxied Sessions**. (B# 119075)
- ❑ A restart issue due to a race condition in the output dumping logic in Active Sessions through the Advanced URL has been fixed. (B# 116166, SR# 2-174829522)

ADN

- ❑ In the **Active Sessions** panel, the byte-caching status of a connection reflected the selected policy for that connection. If byte-caching is manually disabled in the **Statistics > ADN History > Peer Dictionary Sizing** tab, its byte-caching status in **Active Sessions** panel still displays as **enabled**. (B# 109679)
- ❑ ADN did not recognize the leading 0 from the peer-ID string, which had the effect of creating duplicate peer entries with different peer-IDs. (B# 118971, SR# 2-187041242)
- ❑ The `Max-peer-limits` limitation size is no longer imposed on any platforms. (B# 110102)

Authentication

- ❑ IWA Authentication failed when the username is not in NetBios form. (B# 116236, SR# 2-174163402, 2-175340523)
- ❑ Authentication hangs when IWA and Window SSO (with the client queries only option enabled) use the same thread process within the BCAA agent. The problem occurs when the main domain controller is down, the process for IWA hangs causing delays for new client Windows SSO authentication requests connections. This issue has been fixed in this release. (B# 116610)
- ❑ When LDAP, Certificate and Guest authentication is configured within policy, a restart might occur when clients are forced to authenticate with guest access. This issue has been fixed in this release. (B# 116757, SR# 2-176920392)
- ❑ Some Novell SSO users might be denied access with the exception **The user could not be determined by the Single Sign-on agent** due to a restart of the Novell eDirectory servers. This issue has been fixed by adding persistence and agent synchronization features to Novell SSO. (B# 117574, SR# 2-181192560)
- ❑ LDAP authentication users, on rare occasions, had system crashes due to incorrect buffer allocation using LDAP authentication. (B# 117680, SR# 2-173822122, 2-176341712)

CIFS Proxy

- ❑ The ProxySG occasionally crashed when CIFS acceleration was enabled. The crashes occurred when the ProxySG encountered unexpectedly large packets while setting up the CIFS session. (B# 115990, SR# 2-174925212)
- ❑ A page fault that resulted in occasional connection failures with shares and folders while browsing using Windows Explorer has been fixed. (B# 116343, SR# 2-176493803, 2-177124481, 2-177540541, 2-177540579, 2-177541210)
- ❑ CIFS Proxy caused. PPT files that have imbedded pictures to become corrupted. Corrupted files would display red crosses, instead of a valid image. (B# 117750, SR# 2-181456522, 2-189888942, 2-192230078)
- ❑ The ProxySG kept the CIFS connection open when the client shut down unexpectedly. As a result, a file that was re-opened after an unexpected shutdown opened in a read-only mode. (B# 118783)

- ❑ The ProxySG kept the CIFS connection opens when the Apple MAC OS client shut down unexpectedly. (B# 119317)

CLI Consoles

- ❑ SSH client key configuration: Deletion of a specific client key might also delete other client keys that have been configured. (B# 107675)
- ❑ SSH client sessions leaked memory when they were closed. (B# 110113, SR# 2-176444691)
- ❑ When managing the ProxySG through a Director, pagination occurred when issuing `show interface all` regardless of the `line-vty length 0` setting. This issue has been fixed by removing forced pagination. (B# 117366, SR# 2-176848622, 2-177615317, 2-178637230, 2-183537992, 2-184803302, 2-189420584)
- ❑ System crashes resulting from a rare race condition, caused by a null worker after repeatedly pressing the enter key for prompts that have not come up, have been fixed in this release. (B# 118412, SR# 2-184069872)
- ❑ A high number of failed attempts at SSH console access caused the ProxySG's memory utilization to increase. The memory utilization and the PESVC34.03 did not decrease even after several hours have passed since the failed attempts. This issue has been fixed in this release. (B# 118063, SR# 2-184783701)
- ❑ Loopback connections were rejected when the internal communication slots (array) became full. (B# 119168, SR# 2-186401534)
- ❑ A restart issue that occurred when retrieving a large policy using the `show config` command through SSH has been fixed. (B# 116107, SR# 2-167689069)
- ❑ A rare restart issue that occurred when executing the `show conf expanded noprompts` command via an SSH connection to the CLI has been fixed in this release. (B# 109724, SR# 2-187009632, 2-187016882, 2-188678011)

Client Manager

- ❑ When the Windows location setting was set to any non-US setting, the date/time passed to the Java `DateTime` parser assumed that it was formatted in the local format. The expiration date passed from the ProxySG is always US formatted, so the date did not parse correctly and appears to be expired. (B# 116142, SR# 2-176478832)

Content Filtering

- ❑ A system restart issue caused by invalid memory de-allocation when background DRTR is enabled has been fixed in this release. (B# 118222, SR# 2-184989164)
- ❑ A BCAA authentication client process issue, causing the ProxySG to disconnect after numerous authentication failures, has been fixed in this release. (B# 118569, SR# 2-182281243, 2-184238852, 2-184824602)
- ❑ SmartFilter mis-categorized embedded URLs with decimal numbers in the path or query strings. (B# 118856, SR# 2-184238092)

FTP Proxy

- ❑ The ProxySG restarted when a user attempted to retrieve multiple files from an FTP server without logging out. This issue has been resolved and the ProxySG now allows downloading of multiple files using one control connection. (B# 116364, SR# 2-176333411)

HTTP Proxy

- ❑ Transparent HTTP in `http strict-expiration serve` configuration: When a type M (an object with no cache control header, but has a last modified time) object was cached, the configuration switch `http strict-expiration serve` did not check if refresh with the OCS is necessary. This fix makes type M objects be subject to the same refresh configurations that type T objects are (therefore it responds to the setting `http strict-expiration serve`). (B# 116023)
- ❑ Non-current WebFTP directory listings were downloaded for future requests because the ProxySG serves the listing from the cache. This issue has been fixed in this release. (B#116420)
- ❑ When reflect client IP is enabled on the ProxySG and the client uses persistent connections, the server-side ProxySG reuses the same source port as previous TCP connection even when the OCS has sent back a connection-close within the http header. (B#117770)
- ❑ A restart occurred when a Patience Page parses a URL that does not contain flags to parse authentication information and is then propagated to the cache engine. (B#117853, SR 2-183055232, 2-183276098)

ICAP

- ❑ The ProxySG sent out an incorrect exception page when using Secure ICAP. (B# 118847, SR# 2-183492142)
- ❑ Using Secure ICAP the ProxySG reports that the ProxyAV has closed the connection when a file being scanned is larger than the maximum file size. Sending a 503 exception instead of Max File Size Exceeded exception. This is observed using both FTP over HTTP and direct HTTP on the client side. This also occurs when the AV is set to serve the file rather than block it.
- ❑ A restart issue caused by a de-referencing NULL pointer after memory allocation failure has been fixed in this release. (B# 115908, SR# 2-175718191)

IM Proxy

- ❑ AIM 6.8 failed to login when HTTP forwarding was enabled. (B#106263)
- ❑ When MSN IM users use custom emoticons between two proxied clients with `IM.Reflection` enabled, the emoticon shows up as the pre-defined text of the shortcut name. This issue has been fixed in this release. (B# 116912)
- ❑ IM Tunneling failed with Windows Live Messenger 2009. IM tunneling now supports 100 Continue HTTP responses. (B# 116439, SR# 2-176137825)

- ❑ An issue where IM clients remain in IM statistics after HTTP handoff is disabled has been fixed in this release. (B# 116529)
- ❑ Sharing photos using Yahoo Instant Messenger caused a page fault, leading to a software crash. (B# 117753, SR# 2-179677079, 2-184998442, 2-188210432, 2-188798947, 2-188832103, 2-189420259)
- ❑ A restart issue caused when IM Tunnel attempts to release an HTTP Request object twice has been fixed in this release. (B# 120621, SR# 2-191567542, 2-193299202, 2-196398231)
- ❑ A restart that occurred when load balancing between two ProxySG appliances (where one proxy processes login sessions and the second proxy processes chat sessions) has been fixed in this release. (B# 115937, SR# 2-175488050, 2-176477771, 2-186061212)
- ❑ MSN file transfer failed for MSN clients running on hosts with multiple network interfaces. (B#121910)

Kernel

- ❑ On multiprocessor systems, printing output to the serial console at the same time on different processors caused unexpected behavior. Also changed handling of disk read I/O failures to no longer print these errors to the serial console. (B# 116131)
- ❑ A page fault resulting in a crash after a soft restart due to upper memory corruption issues has been fixed in this release. (B# 116449)
- ❑ The ProxySG restarts after running out of physical memory due to a memory allocation error. This issue has been fixed in this release by adding a spinlock to prevent other processes from running at the same time. (B# 116736)
- ❑ The ProxySG might hang or produce throughput variations when the kernel runs out of memory. This issue has been fixed in this release. (B# 117318)

Management Console

- ❑ Statistics Network WCCP: The `state` column of the packet forwarding mismatch is not fully displayed. (B# 108031)
- ❑ Upon upgrading from SGOS 4.3 to 5.4 Mach5 Edition trial license, services that use the following proxy types: Telnet, SOCKS, AIM/Yahoo/MSN IM, continue to exist and are not editable in the Management Console. (B# 109794)
- ❑ Some special characters such as backslashes and double quotes were not detected properly in user entered fields for FTP **Remote Upload** settings, located under **Configuration > General > Archive > Archive Storage**. (B# 118224, SR# 2-184965092)
- ❑ The LDAP access-log field `x-ldap-attribute(name)` was not displayed in the `#Fields` ELFF header-line. (B# 117995, SR# 2-180654357)
- ❑ A discrepancy between the auto-sense settings located in **Statistics > Summary** compared to **Configuration > Network > Adapters** has been fixed in this release. (B# 120296, SR# 2-175928530)(B# 109337)

MAPI Proxy

- ❑ The access log field `x-mapi-user-dn` did not properly record values. (B# 109425)

Policy

- ❑ The proxy HTTP rewrite policy failed to handle content properly because of an invalid `Content-Encoding` header value (for example, binary). It returned the following error to the client: `url_rewrite: headers only -- wrong content type`, and closed the connection to the OCS. (B# 109858)
- ❑ A policy compilation was caused by the policy compiler when it failed to detect a late condition `'condition'` guards `early action` error. The issue occurred when the late condition was nested in multiple levels of condition definitions. A warning is now issued when attempting to compile policies containing this problem. (B# 116491, SR# 2-173459252)
- ❑ CPL gestures to control HTTP connection persistence have been added to `http.client.persistence` and `http.server.persistence` with the addition of the `client` and `server` values. (B# 118440)
- ❑ Memory fragmentation issues when running complex policy combined with high traffic loads (including SSL traffic) caused performance degradation. (B# 119494, SR# 2-188003942)
- ❑ Policy was rejected with the error: **RDNS Policy restriction "WARNING: this restriction has no effect** after upgrading from SGOS 5.2x to 5.4. (B# 121313, SR# 2-192904314)
- ❑ Policy statistics for all active sessions were not synchronized with the actual session in use. (B# 103296, SR# 2-168890491)

Proxy Forwarding

- ❑ When a host with multiple IP addresses was added to a load balance group, new connections were not always sent to the host with the fewest number of connections. (B# 109676)

Quicktime Proxy

- ❑ When a Quicktime stream is delivered over HTTP (RTSP tunneled over HTTP), the ProxySG proxy terminated the server side connection for the POST (keep-alive) after 3 minutes, which caused the stream to fail. (B# 117971, SR# 2-173705202)

Services

- ❑ Editing services when the ProxySG is at 100% CPU utilization caused the Management Console to freeze. (B#107242)
- ❑ One busy service could starve off other services when the client continues to connect. For instance if FTP connections appear to come in faster than the FTP handler can process, only new incoming FTP connections are accepted, starving off other services. (B# 109751)

- ❑ After invoking a `restore-defaults` and configuring through the CLI, users could no longer telnet and SSH to the ProxySG. (B# 121762, SR# 2-197990423)
- ❑ After running `restore-defaults` and the ProxySG Configuration Wizard via CLI, the user could not use Telnet and SSH to connect with the ProxySG. This issue has been fixed in this release. (B# 121762, SR# 2-197990423)

SSL Proxy

- ❑ An issue where users are unable to visit certain Web sites that use invalid UTF-8 characters within a server certificate has been fixed. (B# 116896, SR# 2-177529512, 2-184797902)
- ❑ A secure Firefox/Gmail connection caused an error due to a lack of TLS SessionTicket extension support within SSL-Proxy. SSL-Proxy now supports this extension. (B# 116966, SR# 2-177136871, 2-178804022)

SNMP

- ❑ Because of a set of unrecoverable errors, the ProxySG did not notify SNMP when a disk became bad or unusable and could no longer be used. No traps were sent when a disk was invalid, which should be recoverable or unsupported. (B# 109573)

SSL/TLS and PKI

- ❑ OCSP requests that used the HTTP protocol employed a POST request that was *not* compliant with the HTTP RFC. This caused failures when:
 - The associated OCSP responder strictly complied with the HTTP RFC.
 - The OCSP request was routed through an HTTP RFC-compliant proxy (for example, another ProxySG) before it reached the OCSP responder.(B# 107733, SR# 2-166367540, 2-181198482) (B# 107608)
- ❑ The OpenSSL vulnerability listed in advisory CVE-2009-0590 has been fixed in this release. (B#116017)

Storage

- ❑ A reboot issue caused by a bug in the code, which affected some users after upgrading from SGOS 4.2.9.3 to SGOS 5.4.1.3, has been fixed in this release. (B# 117373, SR# 2-182186924)
- ❑ A restart error caused when the disk process encounters a read error of an internal object during the initialization phase has been fixed. (B# 116274)

TCP/IP and General Networking

- ❑ Occasional interface resets occurs on a ProxySG 8100 when it is overloaded. (B# 110344)
- ❑ Outbound return to sender broke TCP connection-forwarding. (B# 110560)

- ❑ Upgrading to SGOS 5.4 with a configuration that does not contain `forwarding-type` caused a packet return mismatch error during WCCP negotiation. (B# 117444, SR# 2-177862022, 2-178486332)
- ❑ The `clear-arp` command did not work for certain IP address ranges. (B# 121888, SR# 2-191570562)
- ❑ When a multicast address is configured as a home router, the L2 WCCP router table was not correctly populated, resulting in dropped bypassed traffic. (B# 117751, SR# 2-170857742)
- ❑ Static Routes did not properly display CIDR Notation. (B#117903)
- ❑ A static route installed going through the loopback interface was marked down after some time. (B# 118904, SR# 2-171069702)
- ❑ SMTP error handling held onto socket resources, which caused **503 Address Not Available** and **Internal Protocol** error messages. (B# 118925, SR# 2-185110012)
- ❑ When shutdown (FIN) was used to close a connection, the connection remained in the `FIN_WAIT_2` state indefinitely unless a FIN was received from the peer system. (B# 118949, SR# 2-176803872, 2-185116424, 2-185353542, 2-193346832)
- ❑ WCCP configuration becomes disabled after every restart due to a parsing error generated on `primary-hash-weight` configuration, which did not work with any interface other than `0:0`. (B# 119368, SR# 2-186412681)
- ❑ When **DNS recursion** was enabled, some Web sites were not be resolving properly. (B# 120078, SR# 2-189521552)
- ❑ When configuring the ProxySG to be on the same subnet as one of the predefined Management Console addresses, the ProxySG deleted the default gateway IP configured on the appliance. (B#116327, SR# 2-177136812)
- ❑ A ProxySG restart issue caused by TCP/UDP checksum errors has been fixed in this release. (B# 116007, SR# 2-175928522)
- ❑ When `reflect-client-IP` was enabled in a WCCP configured environment, RCIP caused traffic delays on a Cisco 2621. (B# 115744, SR# 2-169669552)
- ❑ The ProxySG 8100 series displayed a misleading warning message on systems with multiple bridges during bootup. (B# 109984)

VPM (Visual Policy Manager)

- ❑ VPM policy cannot be installed when configuring the rule's **Track** parameter using either **Event Log**, **E-mail** or **SNMP** objects in certain layers. This issue has been fixed in this release. (B# 117036, SR# 2-176807022, 2-195585912)
- ❑ A **Track** column object in the VPM reverted to **Any** instead if **None** in the **Forwarding Layer** when objects were deleted. (B# 119661, SR# 2-189108171)

Windows Media Proxy

- ❑ An issue where the WMP hangs after a live stream switches to the audio only mode has been fixed by adding full thinning support to TCP. It also enables video streams to be switched to the key frame mode upon client requests. (B# 116477)

Known Issues in 5.4.2.1

This section describes known issues in SGOS 5.4.2.x that might impact your environment.

Authentication

- ❑ Radius realm configuration refresh time `rejected-credential-refresh` functionality might not work if the refresh time is configured for less than 10 seconds. (B# 107016)
- ❑ Disabling or enabling failover while the **Session-Monitor** is enabled causes **500 Read Timeout** errors. (B# 110139)
- ❑ If a SiteMinder or CoreID realm is configured with a hostname instead of IP addresses, the ICAP `X-Authenticated` header sent to the server does not contain the hostname. (B# 118976)
- ❑ The `show config` command incorrectly displays the `iwa-only-once enable` property as `ntlm-only-once` in sequence realms which contains one IWA realm. This issue prevents archives from being restored. (B# 122052, SR# 2-194294432)

CIFS Proxy

- ❑ Browsing a folder occasionally reports the following error when ADN is enabled: **Fileserver - Novell Netware**. (B# 122785, SR# 2-189415752)

CLI Consoles

- ❑ Administrator login and read/write events are repeating every second in the event log. (B# 106455)
- ❑ Manually entered `line-vty` timeout settings are not saved after a reboot. (B# 107122)
- ❑ Configuring the `exclude-ports` from a client acceleration configuration does not remove the `include-ports` command. (B# 108262)
- ❑ The `config proxy-client web-filtering warn` setting in the CLI cannot be properly negated. (B# 108264)
- ❑ Attack detection `block` and `unblock` settings are not reflected within the system configuration. (B# 109452)
- ❑ Installing an SGOS build image which already resides on the system results in the following error message: **There was 1 error and 0 warning**. (B# 109470)

Hardware Diagnostics

- ❑ SGOS fails to detect the removal of the hardware bridge. (B# 119333)

Hardware Drivers

- ❑ The network interface card (NIC) is unable to establish a connection when set to 1Gb/half duplex mode. (B# 108063)

HTTP Proxy

- ❑ Malformed characters are found within ICAP e-mail alerts when using the `notify_email` property and the `$(icap_error_details)` variable. (B# 120747, SR# 2-177493371)

IM Proxy

- ❑ When a MSN server connection times out because of inactivity, it becomes closed (RST) by the server without any sent data. (B# 122285, SR# 2-197146401)

Management Console

- ❑ Leap year dates for February 29 cannot be set in the Management Console. (B# 119314)
- ❑ When the NTP server list is empty and the Acquire UTC time command is executed, it displays `UTC time was successfully acquired even when there is no NTP server.` (B# 122335)
- ❑ A memory error is encountered on **Statistics > Proxy Client > Details** page during an 11,000 client stress run. (B# 122553)

Kernel

- ❑ NTP time slewing can cause the delay service to stop firing close timers and delays, resulting in system hangs. (B# 120624, SR# 2-189457002)

Network Security

- ❑ The `attack-detection server` command for limiting the number of server connection requests does not properly function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B# 109184)

Policy

- ❑ The **bypass cache** property in the CLI is configured within the `<proxy>` and `<DNS-Proxy>` layers using the following inline command: `bypass_cache(yes)`. (B# 117481)
- ❑ The **deny.unauthorized (no)** property in the CLI is configured within the `<proxy>` and `<ssl>` layers using the following inline command: `deny.unauthorized(no)`. (B# 117482)

SOCKS Proxy

- ❑ The upstream proxy might display the **SOCKSHistory>ClntComp.Gain** calculation as **100%** instead of **0%** within proxy chain environments. (B# 107429)

Storage

- ❑ The CLI command `content revalidate regex.regex` might not work properly when regular expressions are used. (B# 107056)
- ❑

Streaming

- ❑ WM-RTSP: When there are multiple files in a playlist for live streaming, RTSP live split clients go into a waiting state on stream change in a proxy chaining ProxySG setup. (B#109745)

TCP/IP and General Networking

- ❑ Poor performance might be experienced when a hardware bridge is re-enabled to fail-open or fail-closed because the bridge settings might revert to inconsistent settings. (B# 108065)
- ❑ Configuring additional static route entries prompts the incorrect warning message. (B# 120931)
- ❑ Modifying WCCP home-router IP addresses from a valid IP to an unresponsive IP address might cause the proxy to incorrectly report readiness. (B# 122748)

Time Zones and NTP

- ❑ UTC time acquisitions return a success message even when the NTP server cannot be reached. (B# 119260)

Windows Media Proxy

- ❑ An **Object not found** message is sometimes encountered after pulling a file from the media server. (B# 119290)

Doc Errata in 5.4.2.x

The new SmartFilter version— Category map 3— was added to the Management Console and CLI after *Volume 7: Managing Content* was produced. For more information, see "[Content Filtering](#)" on page 91.

Section R: SGOS 5.4.1.12, build 40038

Release Date: 06/19/2009, build 40038

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.1.12 Contents

See the following sections for information on this release.

- ❑ ["Changes in 5.4.1.12"](#) on page 103
- ❑ ["Fixes in 5.4.1.12"](#) on page 103
- ❑ ["Known Issues in 5.4.1.12"](#) on page 106
- ❑ ["SGOS 5.4.x — Limitations and Support for Other Products"](#) on page 138

Changes in 5.4.1.12

This section describes important changes in SGOS 5.4.1.12.

- ❑ OpenSSL vulnerability fix for the advisory CVE-2009-0590. (B#116017)
- ❑ OpenSSL advisory: Incorrect checks for malformed DSA signatures.
- ❑ The ProxySG reuses the TCP source port too quickly for server side connections when IP reflection is enabled on the ProxySG and the OCS does not want connection persistence but the client does. This occurred even when the OCS sent back a connection-close in the HTTP header (SR 2-114584741, 2-173704461, B#117770). To correct the problem, new CPL was added to control connection persistence. With this change, the *preserve* value was added to the `http.client.persistence` CPL gestures to reflect the server persistence on the HTTP client connection persistence.

```
; <Proxy> layer only
http.client.persistence(yes|no|preserve)
```

Fixes in 5.4.1.12

This section describes fixed issues in SGOS 5.4.1.12.

Active Sessions

- ❑ ProxySG restarts because process "CAG_Worker 58" in "active_sessions.dll" at `.text+0xc8d3` because of a race condition while dumping sessions through the Advanced URL. (B#116166, SR 2-174829522)
- ❑ With ADN enabled, accessing the **Management Console > Active Sessions > ADN Inbound Connection** and clicking the **Show** tab twice, causes the ProxySG to hang and stop passing traffic. This might also occur when accessing the serial console and executing the `show cpu` or `show configuration` commands. (B#118986)
- ❑ HTTP Proxied sessions are not displayed under **Statistics > Active Sessions**. (B#119075)

Authentication

- ❑ When LDAP, Certificate, and Guest authentication is configured in policy, a restart might occur when clients are forced to authenticate with guest access. (B#116757, SR 2-176920392)
- ❑ A rare page fault occurs because of incorrect buffer processing using LDAP authentication. (B#117680, SR 2-173822122, 2-176341712)
- ❑ In BCAA authentication, the ProxySG loses the connection when trying to authenticate users. This results in authentication failure. (B#118569, SR 2-182281243, 2-184238852, 2-184824602)
- ❑ Authentication: Authentication hangs when IWA and Window SSO (client queries only option) use the same thread process within the BCAA agent. The problem occurs when the main domain controller is down—the process for IWA hangs, causing delays for new client Windows SSO authentication requests connections. (B#116610)

CIFS Proxy

- ❑ ProxySG keeps the CIFS connection open when the client shuts down arbitrarily. After restarting, if the client opens the same file again, the file opens in read-only mode. (B#118783)

CLI Console

- ❑ Deletion of specific SSH client key might also delete other configured client keys. (B#107675)
- ❑ SSH client sessions leak memory after they are closed, causing high memory pressure over long periods of time. (B#110113, SR 2-176444691)
- ❑ Error occurs when retrieving a large policy by invoking the `show config` through SSH. (B#116107, SR 2-167689069)
- ❑ When managing an ProxySG through Director, pagination occurs when executing the `show interface all` command, regardless of `line-vty` settings. (B#117366, SR 2-176848622, 2-177615317, 2-178637230, 2-183537992)
- ❑ Session memory leaks upon failed SSH console connections. (B#118063, SR 2-184783701)
- ❑ Errors occurs because of a rare race condition that causes the CLI to close the SSH connection. (B#118412, SR 2-184069872)

HTTP Proxy

- ❑ When an object with no cache control header, but has a last modified time is cached, the configuration switch `http strict-expiration serve` does not check if a refresh with the OCS is necessary. These objects are now subject to the same refresh configurations as other objects and will respond to the `http strict-expiration serve` setting. (B#116023)

IM Proxy

- ❑ Statistics incorrectly show MSN IM clients after HTTP handoff configuration is disabled. (B#116529)
- ❑ In MSN IM with reflection enabled, the pre-defined text of the shortcut emoticon's name appears when using customer emoticons between two proxied users. (B#116912)
- ❑ A page fault occurs in Yahoo IM when sharing photos over IM. (B#117753, SR 2-179677079, 2-184998442, 2-188210432, 2-188798947, 2-188832103, 2-189420259)

Kernel

- ❑ On multiprocessor systems, printing output to serial console at the same time on different processors causes unexpected behavior. Changed handling of disk read I/O failures to no longer print these errors to the serial console. (B#116131)
- ❑ Page fault sometimes occurs after a soft restart because of upper memory corruption. (B#116449)
- ❑ Software restarts when the system runs out of physical memory. (B#116736)
- ❑ When the kernel runs out of memory, the system may not to process packets for a period of time or some throughput variations. (B#117318)

Policy

- ❑ Because of an invalid `Content-Encoding` header value, the proxy HTTP rewrite policy fails to properly handle content. The policy returns a `url_rewrite: headers only -- wrong content type` error to the client and closes the OCS connection. (B#109858)

SSH

- ❑ Page Fault at 0x00000CB4 in process Process "CLI_Worker_2" in "sshd.dll" when displaying the expanded configuration through SSH. (B#109724)

SSL Proxy

- ❑ If there is a server certificate that has an invalid UTF-8 character, SSL Proxy fails while processing "`v3 SERVER HELLO`". (B#116896 SR 2-177529512, 2-184797902)
- ❑ Secure Firefox/Gmail connection caused an error because of a lack of TLS SessionTicket extension support in the SSL Proxy. The SSL Proxy now supports this extension. (B#116966, SR 2-177136871, 2-178804022)

Storage

- ❑ Disk failures caused ProxySG restarts. (B#116171, SR 2-179690582)
- ❑ Page fault occurred in "`ce_admin.dll`" when the disk process encountered a read error of an internal object during the initialization phase. (B#116274)

TCP General Networking

- ❑ 8100 series ProxySG interface occasionally reset when it was operating under extreme loads. (B#110344)
- ❑ Upgrading to SGOS 5.4 with a configuration that did not contain `forwarding-type` causes a packet returned mismatch error during WCCP negotiation. (B#117444, SR 2-177862022, 2-178486332)
- ❑ The L2 WCCP router table did not correctly populate when a multicast address was configured as a home router. (B#117751, SR 2-170857742)
- ❑ A static route installed through the loopback interface is marked down after a given interval. (B#118904, SR 2-171069702)
- ❑ When shutdown (FIN) is used to close a connection, the connection remained in the `FIN_WAIT_2` state indefinitely unless a FIN is received from the peer system. (B#118949, SR 2-185116424, 2-185353542)

WCCP

- ❑ WCCP configuration disabled after every restart because of a parsing error generated on primary-hash-weight configuration for valid interfaces. (B#119368, SR 2-186412681)

Known Issues in 5.4.1.12

This section describes known issues in SGOS 5.4.1.12 that might impact your environment.

Authentication

- ❑ SSH authentication fails with SSH access `zmalloc: zero size` when the banner length is 0 in size. Blue Coat recommends having a banner. (B#120541)
- ❑ SSHv1 authentication with RSA key fails with Cygwin. Setting the SSH host to use SSHv2 solves this problem. (B#120616)

CIFS

- ❑ Proxy keeps CIFS connection open when MAC OS client shuts down. (B#119069)

Content Filtering

- ❑ After upgrading to SGOS 5.x from 4.x, ADP connection limit counts connections in all TCP states. In SGOS 4.x, ADP connection limit only counts established connections. In SGOS 5.x, connections in all TCP states are counted. After upgrading, clients that used to work fine now keep hitting the ADP connection limit. Therefore, before upgrading, plan for the correct ADP connection limit. (B#119932, SR 2-181118142)

Downgrade

- ❑ Downgrade limitation: you must clear the byte and object caches after downgrading from SG 5.3 or 5.4 to 5.2. (B#116791)

Management Console

- ❑ Early versions of Firefox and Java Plug-in 1.6.0_11: After logging in from the Landing page, clicking **Home** at the top of the browser pane results in a Java exception. Blue Coat recommends using Internet Explorer if you do not have any minimally-required JRE installed. (B#109031)
- ❑ With a Copperhead programmable 4-port bridge card, the drop down menu is not present and cannot be edited. You can use the CLI to edit the bridge. (B#119427)
- ❑ Upon upgrading from 4.3 Proxy Edition to 5.4 MACH5 Edition trial license, services using Telnet, SOCKS, AIM/Yahoo/MSN IM proxy types still exist and cannot be edited in the Management Console. (B#109794)

Network

- ❑ Blue Coat Web Filtering does not work in Trial mode. The evaluator must obtain trial credentials from Blue Coat, which then allows the download of the Blue Coat Web Filter database. The evaluator can then enable Web filtering in the Client Manager. (B#116596)
- ❑ When creating an OCSP responder, any capital letters used in the name of the OCSP responder service will be changed to lower case by the OS. (B#117192)

TCP/IP General Networking

- ❑ Page Fault occurs due TCP/UDP checksum errors. (B#116007, SR 2-175928522)

Section S: SGOS 5.4.1.3, build 38863

Release Date: 04/16/2009, build 38863

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.1.3 Contents

See the following sections for information on this release.

- ❑ ["Fixes in 5.4.1.3"](#)
- ❑ ["Known Issues in 5.4.1.3" on page 109](#)
- ❑ ["SGOS 5.4.x — Limitations and Support for Other Products" on page 138](#)

Fixes in 5.4.1.3

This section describes fixed issues in SGOS 5.4.1.3.

Authentication

- ❑ IWA Authentication failed in certain network configurations and the error message **Username could not be converted to Kerberos name** was displayed. The issue was caused by a dependency on a Microsoft service that was not always available. This dependency has been removed and the issue is fixed. The user will now be successfully authenticated by the ProxySG. (B#116236, SR# 2-174163402, 2-175340523)

Connection Forwarding

- ❑ Connection forwarding could not be configured for VLAN interfaces. The **Local IP** drop-down menu in the **Configuration > Network > Advanced > Connection Forwarding** tab lists IP address that are associated with a physical interface only. This issue has been fixed, and connection forwarding can now be configured for VLAN interfaces. (B#106949)

CIFS

- ❑ If CIFS acceleration was enabled and large packets (larger than 8K) were received while setting up the CIFS session, the ProxySG restarted. This issue has been fixed. (B#115990, SR 2-174925212)
- ❑ When browsing using Windows Explorer, the user would occasionally be disconnected from shares or folders. This issue is now fixed. (B#116343, 116633, SR 2-176493803, SR 2-177124481, SR 2-177540541, SR 2-177540579, SR 2-177541210)

Event Logging

- ❑ If you upgraded from SGOS 4.3 and then downgraded again, some cached objects became invalid and needed to be removed. Each deleted object used to generate an event log message. This issue has been fixed and event log messages for invalid objects are not generated. (B# 107934)

FTP

- ❑ The ProxySG restarted when a user attempted to retrieve multiple files from an FTP server without logging out. This issue has been resolved and the ProxySG now allows downloading of multiple files using one control connection. (B#116364, SR 2-176333411)

ICAP

- ❑ In low memory conditions, memory allocation on the ProxySG would fail and cause the ProxySG to restart. This issue has been fixed. When a low memory condition occurs, the ProxySG will display an error message in the client's browser window. The error message will read **Internal error: Out of system resources**. (B#115908, SR 2-175718191)

IM

- ❑ When IM tunnel mode was enabled for unsupported IM versions and two ProxySG appliances were used for load balancing, the ProxySG handling the chat would restart. This occurred in cases where MSN login was handled by one ProxySG and the chat session was handled by the other ProxySG, which implemented a more restrictive policy. This restart issue has been resolved and both the log in and the chat sessions will be tunneled through the load balanced ProxySG appliances. The IM client should no longer experience any interruptions. (B#115937 SR 2-175488050, SR 2-176477771)
- ❑ Tunneling failures with Windows Live Messenger 2009 has been fixed. (B#116439, 116415, SR# 2-176137825)

Proxy Client

- ❑ On the Proxy Client, web filtering can now be enabled regardless of the operating system's locale setting. (B#116142, SR 2-176478832)

Known Issues in 5.4.1.3

This section describes known issues in SGOS 5.4.1.3 that might impact your environment.

Access Logging

- ❑ The MAPI access log field `x-mapi-user-dn` does not record the value of the `userDN` string, and sets the value as `-`. (B#109425)

Active Sessions

- ❑ Some errored sessions display their active sessions status as **Active** (in the **Age** column) and the duration increases although the sessions are inactive. To view the errored sessions that are active, access the **Sessions > Active sessions** tab. (B#103519)

Authentication

- ❑ When a Windows SSO realm that has been configured to perform **Query Client** is being used for authenticating a client to the BCAA agent and a Domain Controller is taken offline, the realm may process requests very slowly, causing some requests to timeout.(B#116610) The workaround to prevent this delay is:

a. Use **Query Domain Controller** or the **Query Domain Controller and Client** option in the **Query type** drop-down menu (in the **Configuration > Authentication > Windows SSO > Agents** tab).

b. Increase the `NumThreads` parameter in BCAA.ini. `NumThreads` is the Number of threads per realm. The default value for this setting is two. Increasing the `NumThreads` parameter allows BCAA to process more concurrent requests, and increases the throughput of the Windows SSO realm.

Important: Blue Coat recommends keeping the value under eight because the `NumThreads` parameter is applied to each realm configured on the ProxySG.

If, for example, your ProxySG contains a Windows SSO realm and an IWA realm, setting `NumThreads` to four causes the BCAA agent to create eight threads. Also, increasing `NumThreads` will not increase the throughput of IWA realms because Active Directory enforces a limitation on the number of concurrent authentication requests per client.

- ❑ In the RADIUS realm configuration, credential-refresh time may not work if the refresh-time configured is less than 10 seconds. (B#107016)
- ❑ If Session Monitor is enabled, and failover is switched from disabled to enabled or enabled to disabled, you may receive **500 Read Timeout** errors when attempting to access the Session-Monitor Lookup page. (B#110139)
- ❑ LDAP authentication using an iPlanet LDAP server that is configured with nested groups causes errors in the VPM. (B#102008)

ADN

- ❑ In the **Statistics > Sessions > Active Sessions** panel, the byte-caching status of a connection reflects the policy applied for that connection. If byte-caching is manually disabled in the **Statistics > ADN History > Peer Dictionary Sizing** tab, the byte-caching status in **Statistics > Sessions > Active Sessions** still displays as enabled. (B#109679)

CLI Console

- ❑ The `line vty timeout` setting, when entered manually, is not preserved after reboot. (B#107122)

- ❑ The archive configuration file, `archconf_post_setup.txt` contains configuration for content filtering with MACH5 Edition license. Since the MACH5 edition license does not include the content filtering features, this issue can cause a failure of the configuration install process when restoring with the `archconf_post_setup` file.(B#108552)
- ❑ The `attack detection server` command for limiting the number of server connection requests does not function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B#109184)

FTP

- ❑ If you are logged in as an anonymous user, the first download attempt of a file larger than the `max-cache-size` fails. Subsequent download attempts will be successful. (B#99917)

Forwarding

- ❑ When a host with multiple IP addresses is added to a load balance group, new connections are not always sent to the host with the least connections. (B#109676)

HTTP Proxy

- ❑ WebFTP directory listings can be stale because the ProxySG serves the request from cache. To obtain a current listing, click the reload button on the web browser to force a page refresh. (B#116420)

Health Checks

- ❑ After you upgrade from a Mach5 license to a ProxySG license, you must reboot the ProxySG before health-checks become active/available. (B#110098)

ICAP

- ❑ When ICAP scanning is set to deferred scanning mode, the object count displayed for scanned objects (in the **Statistics >ICAP >Completed Requests** tab) is higher on the ProxySG than the count on the ProxyAV user interface. This is because the object count mechanism on both devices are different; the bytes scanned is displayed accurately.(B#107403)

IM

- ❑ Non-ASCII character replacement policy does not work with Yahoo IM. (B#85278)
- ❑ AIM 6.8 fails to login when HTTP forwarding is enabled on the ProxySG. SOCKS forwarding works correctly, and can be used instead. In the following example `upsocks` is the defined SOCKS proxy:(B#106263)

```
<forward>
socks_gateway(upsocks)
```

- ❑ When the Yahoo client is not using the same proxy settings as the browser, file transfers are not supported.
- ❑ Yahoo IM: Socks Forwarding policy combined with im.transport (HTTP) property is not supported. (B#109762)
- ❑ The **Statistics > Protocol details > IM History > IM Clients** tab in the Management Console, erroneously displays MSN IM clients over HTTP even after HTTP handoff configuration is disabled. To fix the issue, you must restart the ProxySG. (B#116529)
- ❑ AIM connections get disconnected when transferring large (greater than 8K) buddy icons over the AIM proxy. (B#116236)

Management Console

- ❑ JRE 1.6.0_11 and 1.6.0_12 with Firefox 2.0.0.20 and Firefox 1.5.0.12 intermittently display a Java exception when you click **Home** while another page loads. (B#109032)
- ❑ After an upgrade or downgrade of the SGOS version, the Management Console might hang or throw a Java exception upon reboot. Close the browser page and launch it again to resolve the problem. (B#110413)
- ❑ Rapid context switching between or within the Statistics, Configuration and Maintenance Tabs, may lead to an out of memory condition in the Java Virtual Machine. Click the tab again for the page to load. (B# 108726 and 108791)

Networking

- ❑ If you configure the ProxySG to be on the same subnet as one of the predefined Management Console addresses, for example 192.168.1.x, 192.168.0.x, or 172.16.x.x during the initial configuration, the ProxySG deletes the default gateway IP configured on the appliance. (B#116327, 2-177136812)

The workaround is to:

1. Remove and re-add the default gateway, using the serial console as follows:

```
SGOS# conf t
SGOS# no ip-default-gateway <gateway IP>
SGOS# ip-default-gateway <gateway IP>
```

2. Reboot the ProxySG.

- ❑ The 1Gbps Copper Network Interface Card does not support a half-duplex connection. (B#108063)
- ❑ Changing duplex configuration on the Integrated NIC on the ProxySG8100 causes link connectivity failure. (B#108779)
- ❑ Changing the duplex configuration, on the pass-through card of the ProxySG 510 or 810 appliance, to half-duplex causes the link speed to drop from 1Gbps to 100 Mbps. (B#108783)
- ❑ Gateway load balancing distribution is not consistently equal across gateways. (B#107839)

- ❑ On boot up, the warning message displayed on duplex, speed, or link speed mismatch might be inaccurate for a hardware bridge. Verify the configuration in the Summary>Efficiency tab in the Management Console. (B#109984)
- ❑ If a bridge is disabled, you can configure different settings for the ports on the bridge. When the bridge is re-enabled to fail-open or fail-closed the settings are maintained and so you could have a hardware bridge with manual 100/half on one side, and auto on the other. This can potentially cause performance problems. (B# 108065)
- ❑ Connection forwarding does not function properly when the **Return-to-Sender Outbound** configuration is enabled. The ProxySG forwards server traffic to the MAC address of the ProxySG peer performing connection forwarding rather than to the server next hop. (B#110559,110560)

Policy

- ❑ Reflect Client IP policy for CIFS cannot be implemented in the Forward layer. `Client.protocol=cifs reflect_ip(client)` must be defined under the Proxy Layer. (B#109532)

ProxyClient

- ❑ Currently, the ProxyClient Web filtering can be used with the 60-day SGOS trial license only after you do any of the following:
 - (Recommended.) Enable ProxyClient Web filtering from the command line using the following commands:

```
Blue Coat SG200 Series#(config)proxy-client
Blue Coat SG200 Series#(config proxy-client)web-filtering
Blue Coat SG200 Series#(config proxy-client web-
filtering)enable
ok
```
 - Contact your Blue Coat representative to get temporary Blue Coat Web Filtering database credentials, then in the Client Manager's Management Console, click **Configuration > Content Filtering > Blue Coat**.

In the **Username** field, enter the user name provided to you by your Blue Coat representative. Click **Change Password** and in the provided fields, enter the password provided by your Blue Coat representative into the provided fields.

You can then enable and use ProxyClient Web filtering. (B#115694, 116424)

SSH Client Key Configuration

- ❑ Deletion of a specific client key deletes other client keys that are configured on the ProxySG. (B#107675)

SSL

- ❑ The HTTP POST request generated by the ProxySG for OCSP fails when the request goes through another ProxySG appliance. (B #107608)

In a proxy chain, the workaround is to:

- a. Create a custom port and use it for TCP-Tunnel on the ProxySG(#2) fronting the OCSP responder.
 - b. Configure OCSP setting on the downstream ProxySG(#1) to use the custom port in the responder's URL.
 - c. Create a TCP forwarding host with server port as 80, on ProxySG(#2).
- ❑ An SSL Device Profile cannot be deleted after deleting the authentication realm that uses that **ssl-device-profile**. (B#106438)

Streaming

- ❑ Pre-population of RealMedia content from web servers does not work. (B#109339)
- ❑ WM-HTTP: A Windows Media client streaming multi-bitrate live content sourced from a playlist might get disconnected under low bandwidth conditions. (B#109029)
- ❑ WM-RTSP: The Windows Media client hangs after the live stream switches from audio and video mode to audio-only mode. This problem occurs because thinning might not work when the client is using TCP Transport. (B#116477,62453)
- ❑ Windows Media player might enter a buffering state near the end of the stream when using `rtspt://url`. (B#64430)
- ❑ Some Windows Media content files cannot be pre-populated from a HTTP web server. The workaround is to use streaming speed pre-population instead of line speed pre-population. (B#104035)

Storage

- ❑ Regular expressions in `content revalidate` command do not work. (B# 107056)

WCCP

- The **State** column in the **Statistics > Network > WCCP** tab does not display the complete error message. For example, the **Packet Forwarding Mismatch** error is not fully displayed. Use the `show wccp statistics` CLI command for a listing. (B#108031)
- ❑ When upgrading from earlier versions to SGOS 5.4, the WCCP configuration fails if the `forwarding-type` information is not defined. To prevent a packet return mismatch error during WCCP negotiation, you must explicitly define `forwarding-type` in the WCCP configuration. (B#117444) For example, the configuration should read:

```
wccp enable
wccp version 2
service-group 9
forwarding-type GRE
```

```
assignment-type hash
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 80 443 0 0 0 0 0 0
interface 0
home-router 172.16.11.1
```

Section T: SGOS 5.4.1.1, build 38147

Release Date: 03/15/2009, build 38147

BCAAA Version: 130

Compatible with: SGME 5.4.x, Reporter 8.x, ProxyAV 3.x and 2.x, and ProxyClient 3.1.x

SGOS 5.4.1.1 Contents

See the following sections for information on this release.

- ❑ ["SGOS 5.4.x Feature Matrix"](#)
- ❑ ["Known Issues in SGOS 5.4.1.1" on page 130](#)
- ❑ ["SGOS 5.4.x — Limitations and Support for Other Products" on page 138](#)

SGOS 5.4.x Feature Matrix

The following table lists the features introduced in this release (SGOS v5.4.1.1) with cross-reference links to feature descriptions.

Table 1–1 SGOS 5.4.1.1 Feature Matrix

Component	Feature
ADN	"Open ADN"
Authentication	"HTTP Header Changes"
	"Kerberos Authentication Enhancement"
	"Kerberos Constrained Delegation"
	"LDAP Group Check Performance Improvement"
	"Processing LDAP Attributes Locally"
CIFS	"MSISDN"
	"Overlapping Opens"
	"Browsing Performance"
Content Filtering	"Blue Coat WebPulse"
	"SmartFilter"
	"Websense"
HTTP	"WebFTP"
Instant Messaging (IM)	"AIM 6.8 Support"
	"Unsupported IM Client Policy"
MAPI	"Compression Handling"

Table 1–1 SGOS 5.4.1.1 Feature Matrix

Component	Feature
Management Console	"Browser Configuration using PAC Files"
	"Force Bypass Switch"
	"Configuring WCCP Settings on the ProxySG"
	"JRE Support"
	"New Landing Page"
	"Updated Proxy Services Interface"
Networking	"Change in Default List of Bypassed Services"
	"Displaying Duplex Mismatch"
	"Enforce LAN/WAN Concept in WCCP Deployment"
	"Handling Non-Routable Addresses"
	"Configuring Private Networks"
	"Change in Defaults for TCP/IP Loss Recovery Mode"
ProxyClient	"ProxyClient"
Web-Anti Virus or ICAP	"Web Anti-Virus (ICAP) Features"

Descriptions of Features Introduced In This Release

This section describes new functionality introduced in the SGOS 5.4.1.1 release.

Application Delivery Network (ADN)

Open ADN

In an application delivery network (ADN), ProxySG appliances form tunnel connections over which they accelerate application requests and responses. In previous SGOS releases, each ProxySG appliance had to connect to an ADN Manager in order to be part of the ADN. In SGOS 5.4, an ADN Manager is no longer required in transparent ADN deployments. In this configuration, called *Open ADN*, an ADN peer is allowed to form a tunnel connection with any other ADN peer. An acceleration network that does not have any ADN Managers is called an *open unmanaged ADN*.

Because the ADN Management functions are not available in an unmanaged ADN, the following are not supported in this configuration:

- Explicit tunnel connections (including ProxyClient and out-of-path deployments)
- Load balancing (explicit or transparent)
- Internet Gateway
- Manager authorization in secure ADN

To enable any of these services, you must configure an ADN Manager and connect the ProxySG appliances that require the services to it. You do not need to connect all ProxySG appliances to the ADN Manager. Mixed acceleration networks in which some open nodes connect to a manager and some do not is called an *Open, managed ADN*.

If you only want ADN nodes to establish transparent tunnels with peers in this ADN, you can configure a *Closed ADN*. In this configuration, participating ADN nodes can only establish accelerated tunnel connections with peers in its ADN.

By default, a transparent acceleration network is in Open, unmanaged mode. Therefore, to set up a new ADN, you deploy the ADN nodes in-path or virtually in-path and enable acceleration; no further configuration is required.

To configure an Open, managed or a Closed acceleration network, you must configure the ADN Manager settings from the Management Console on all ProxySG appliances that require ADN Manager services as well as on the ADN Manager appliance itself:

1. Select **Configuration > ADN > General**.
2. In the **Primary ADN Manager** field, define the **IP Address** of the ADN Manager to which this ProxySG should connect, or select **Self** if you are configuring the box as manager.
3. To enable ADN, select the **Enable Application Delivery Network** option.
4. Click **Apply**.

To have ADN operate in Closed mode, you must also perform the following steps on the ADN Manager:

1. Select **Configuration > ADN > Manager > Peer Authorization**.
2. Select the **Allow transparent tunnels only within this managed network** option.

Authentication

HTTP Header Changes

The `Authorization` and `Proxy-Authorization` HTTP headers are now writable.

The `Authorization` request-header field is used in an HTTP request when a user agent wishes to authenticate itself with a server. And the `Proxy-Authorization` request-header field allows the client to identify itself or its user to a ProxySG, which requires authentication.

In a proxy chain, administrators can now, also control the upstream authorization headers using `server.authenticate.basic` which allows substitutions for the username and password.

Kerberos Authentication Enhancement

SGOS 5.4 supports Kerberos authentication for explicit proxy connections.

Kerberos Constrained Delegation

Kerberos Constrained Delegation (KCD) allows a secure and reliable method of single sign on within Microsoft Windows networks. KCD uses extensions to the Kerberos protocol found in Microsoft Server 2003 which enables a trusted process to acquire Kerberos tickets for a user. A single Kerberos ticket authenticates a user to a specific service or server.

The ProxySG uses these new extensions to give authenticated users access to a preconfigured set of services. KCD configuration is performed by access administrators who manage policy.

LDAP Group Check Performance Improvement

Lightweight Directory Access Protocol (LDAP) group check performance improvement allows LDAP group comparison operations to be offloaded onto the ProxySG, thereby improving performance. This feature minimizes the number of server queries when performing a comparison because a single search can retrieve all appropriate entries. Once the ProxySG receives the relevant entries, it performs the group membership check on the ProxySG without placing additional load on the LDAP server.

An LDAP search uses simplified DN comparison rules and might have differing results to LDAP comparisons. This issue is expected to be a very rare occurrence. However, to maintain accuracy, the ability to use LDAP compares is retained.

Processing LDAP Attributes Locally

LDAP attributes comparisons are now offloaded and are performed locally by the SGOS LDAP client. The new functions include the ability to:

- ❑ Substitute the value of an LDAP attribute into a character string or block of text; for example into headers, exception pages, and access log records.
- ❑ Reduce the number of LDAP server queries by offloading LDAP attribute comparisons onto the ProxySG, thus minimizing the impact on the LDAP server.

- ❑ Test LDAP attributes using string comparisons, existence, list count, and numeric checks.

Note: The existing **attribute** trigger behavior has been left unchanged. As a result, existing policies will continue to function without any policy updates.

However, to take advantage of the expanded comparison tests and perform them locally on the ProxySG, the policy writer must use the new **ldap.attribute** trigger.

MSISDN

The ProxySG allows mobile operators to charge for value-added content such as video streaming and music based on mobile phone numbers (MSISDNs). To enable billing integration for voice and data content, the ProxySG maps IP addresses to MSISDNs. The administrator can now configure the ProxySG to send the MSISDN in hexadecimal format in addition to ASCII.

The new CPL modifier to support hex-encoding of bytes is: `encode_hex`

The MSISDN is available in the `$(session.username)` substitution, so to encode the MSISDN in hexadecimal format, the substitution is `$(session.username:encode_hex)`

The `encode_hex` modifier can optionally take a separator string which will be substituted between each byte of the original substitution. For example, for an MSISDN number `"*#911#"` the `encode_hex` modifier can be used as follows:

- `$(session.username:encode_hex)` produces `2A2339313123`
- `$(session.username:encode_hex(,))` produces `2A,23,39,31,31,23`
- `0x$(session.username:encode_hex(0x))` produces `0x2A 0x23 0x39 0x31 0x31 0x23`

Like other CPL modifiers, `encode_hex` can be used anywhere a CPL substitution can be used.

CIFS

Overlapping Opens

For applications such as Microsoft Word and Microsoft Excel, the ProxySG now improves access times when these applications open the same file multiple times, even if the end user opens the file only once (a type of file contention referred to as *overlapping opens*).

Browsing Performance

Two new CIFS proxy options improve the user's experience when browsing remote folders in Windows Explorer:

- ❑ Remote Storage Optimization: Enabled by default. When enabled, Windows Explorer modifies the icons of uncached folders on remote servers, indicating to users that the contents of the folder have not yet been cached by the ProxySG. See [Figure 1–1](#).

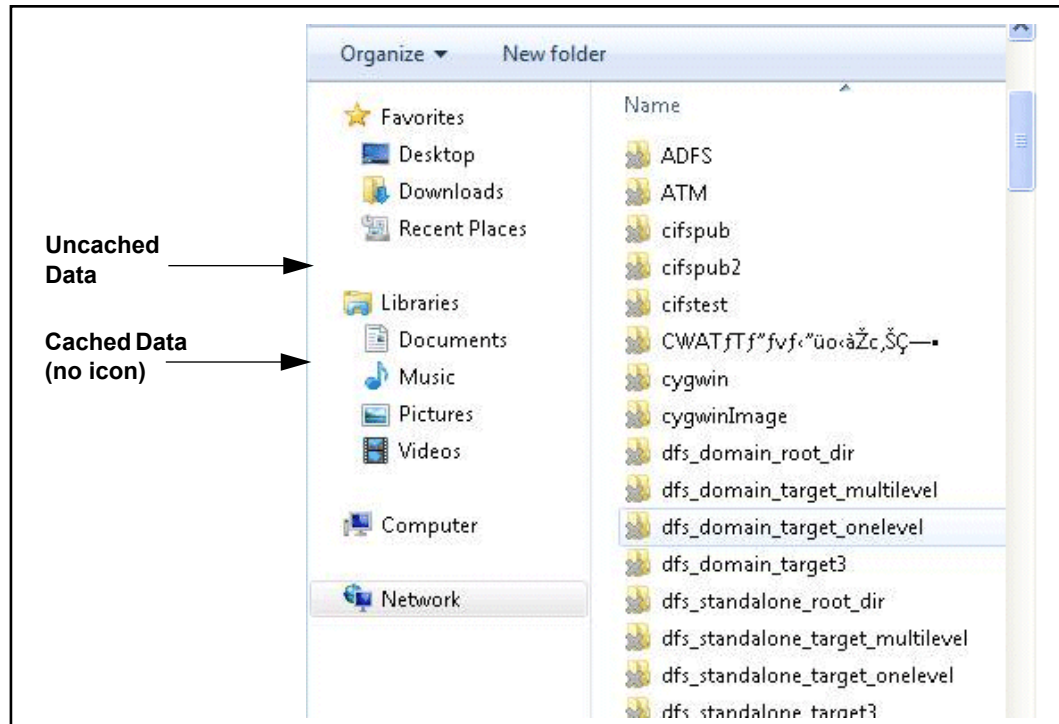


Figure 1–1 CIFS Remote Storage Optimization Explorer Icon

In Vista and Windows 7, the uncached data icon displays as a gray “X”, as shown in [Figure 1–2](#).

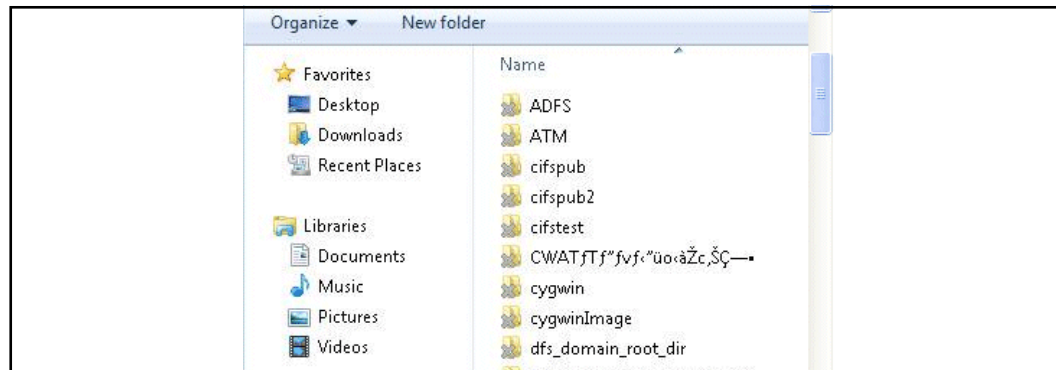


Figure 1–2 Uncached Data Icon in Vista and Windows 7

- ❑ **Suppress Folder Customization:** Disabled by default. When a remote folder is customized (for example, the style of icon and the display of folder contents as icons or thumbnails), Windows Explorer checks for `desktop.ini` file inside the folder to determine how to display its contents. On slow links, however, the extra transactions required by this check result in sluggish performance. To speed the display of remote folders, enable Suppress Folder Customization to skip the extra transactions and always display remote folders in the default view.

Content Filtering

Blue Coat WebPulse

Blue Coat offers WebPulse services to customers using Blue Coat Web Filter (BCWF). As a real-time cloud service (SaaS), WebPulse leverages the collective knowledge of millions of users in an Internet-based *community watch* program consisting of participating BCWF, K9, and ProxyClient customers. The WebPulse service also provides dynamic real-time rating (DRTR, also known as *Dynamic Categorization*) of web content on the ProxySG.

DRTR has been renamed as WebPulse in the **Configuration > Content Filtering > BlueCoat** tab in the Management Console.

WebPulse service leverages information on threat analysis, malware, and web content ratings for a very large community of users. Information collected and analyzed only moments ago is pro-actively shared as category updates to all users within the WebPulse community.

Other enhancements include:

- ❑ Malware notification to the WebPulse service when the ProxySG is connected to a Web AV scanning device, and has an ICAP service configured and BCWF enabled.
- ❑ The ProxySG checks for BCWF updates every few minutes. Frequent updates provide you with the most current and comprehensive database categories, and inhibit malware and phishing attacks. You can schedule the interval for checking updates and for retrieving content from the download server(s) — it can vary from an hour per day up to 24 hours per day.
Frequent content-filter updates are also available for all on-box databases with a valid content-filtering license.

Change in CPL Syntax

- ❑ **Deprecated CPL Syntax:** `category.dynamic.mode(none | realtime | background | default)`
- ❑ **Replacement CPL Syntax:**
`webpulse.categorize.mode(none | realtime | background | default)`

SmartFilter

SmartFilter offers reputation-based categorization of URLs. When reputation-based categories are enabled, SmartFilter assigns every URL a reputation score. The ProxySG interprets these reputation scores as five possible categories— Malicious, Suspicious, Unverified, Neutral, Trusted. Reputation-based categories are fully accessible in policy, and function like normal categories.

SmartFilter also provides embedded URL categorization and supports SmartFilter Category Set 2, as defined by Secure Computing at <http://www.securecomputing.com/filteringdb.cfm?db=XL>

Websense

Websense features Real-time updates (RTU) and Real-time security updates (RTSU). RTU/RTSU allow the ProxySG to frequently update the database with new information from the Websense servers. By default, RTU is enabled and your database may be updated several times each hour. Even if RTU is disabled, your database will be updated at least once per day.

HTTP

WebFTP

When ADN is enabled, Web FTP connections in explicit and transparent proxy deployments now use the ADN tunnel when the server-side connection is set to auto or passive mode. ADN tunnel support for Web FTP connections enhance the byte-caching and compression benefits derived by deploying ProxySG appliances in your network.

The server-side connection is controlled by the CPL property `ftp.server_data{auto|passive | port}`. When in auto mode, the ProxySG supports the ADN tunnel only if the ProxySG is able to connect in passive mode.

Instant Messaging

AIM 6.8 Support

SGOS 5.4.x supports AIM 6.8 client traffic. Configuring AIM 6.8 support on the ProxySG slightly differs from the AIM 5.x configuration. AIM 6.8 connections are explicit (where the clients believe the ProxySG is the native AIM service host) and require a keyring and a signed certificate. The certificate must be installed on the ProxySG and is used by the AIM proxy service to communicate with the AIM client. Certificates signed by the `rapidssl.com` CA and Thawte are accepted by the AIM 6.8 client.

Note: While trial certificates from `Rapidssl.com` are supported by AIM 6.8, Thawte trial certificates are not supported.

Unsupported IM Client Policy

By default, SGOS 5.4.x detects an unsupported IM client version (Windows Live Messenger and Yahoo only) and blocks connection attempts. When Blue Coat releases an updated SGOS version that supports new IM clients, the policy automatically allows the traffic to proceed. If you elect to allow unsupported IM connections at the expense of no policy checks against the transactions, you can create policy that allows (tunnels) unsupported clients. For more detailed information about this policy, see the Instant Messaging chapter in *Volume 3: Web Communication Proxies*.

MAPI

Compression Handling

The ProxySG can now cache and accelerate data encoded or compressed by Microsoft Outlook and Exchange. For example, when an e-mail with an attachment is sent using Microsoft Outlook, the encoded (or compressed) data is decoded (or decompressed) by the branch office proxy. The ProxySG sends it across the WAN in a plain data format. Because the data is in a plain data format, it can be byte cached with all other supported protocols (such as CIFS, HTTP, FTP), thus increasing cross-protocol hits.

Currently, MAPI compression handling supports improved byte caching for MAPI 2000/2003. It also improves general performance, bandwidth and, in certain cases, application-level latency. Both the branch and concentrator ProxySG appliances must run the same version of SGOS for MAPI compression functionality.

Management Console

New Landing Page

After you have logged in to the ProxySG, the Management Console displays the **Statistics > Summary** page. The Management Console banner displays across the top of the Web browser and includes information on the ProxySG appliance name, hardware model, hardware serial number, and the software version. You can also view information on the health status, license status, and license edition.

The new **Statistics > Summary** page monitors and reports information on your network traffic and applications, and displays the role of the ProxySG in boosting the performance of traffic within your network using its acceleration, optimization, policy control, and caching techniques.

- ❑ The **Statistics > Summary > Efficiency** tab displays the bandwidth gain achieved within your network in the Savings panel, and the performance of each interface in the Interface Utilization panel on the ProxySG.
- ❑ The **Statistics > Summary > Device** tab displays a snapshot of the key system resources, identification specifics, and the status of external devices that are connected to the ProxySG.

JRE Support

ProxySG 5.4 is officially supported on JRE 1.5.0_15 and above, and 1.6 (except 1.6_05, which causes VPM Help problems). JRE 1.4x is no longer supported.

Lowest Allowed JRE: 1.5.0_15

Default Downloaded JRE: 1.5.0_15 is the default for IE; the latest JRE version available is the default for Firefox.

Browser Configuration using PAC Files

The ProxySG no longer supports browser configuration for Explicit Proxy deployments through an HTML page on the Management Console.

If your network does not use transparent proxy, clients on the network must configure their browsers to use either an explicit proxy server or a Proxy Auto-Configuration (PAC) file.

Two PAC files ship with the ProxySG:

- ❑ Default PAC file, which can be accessed at
`https://ProxySG_IP_Address:8082/proxy_pac_file`
- ❑ Accelerated PAC file, which can be accessed at
`https://ProxySG_IP_Address:8082/accelerated_pac_base.pac`

Only the `accelerated_pac_base.pac` file can be edited. Any text editor can be used to edit and customize the accelerated PAC file to meet your needs.

After editing the file, you can load a PAC file only through the CLI:

```
SGOS#(config)inline accelerated-pac 123
-paste PAC file here-
123
```

Then set the browser to use the following URL to access the automatic configuration script:

```
http://ProxySG_IP_Address:8082/accelerated_pac_base.pac
```

Deprecated CLI command:

```
SGOS#(config interface interface_number) instructions {accelerated-pac |
default-pac | proxy}
```

Force Bypass Switch

A new CLI command and **Temporarily bypass all proxy services** check box has been added to bypass all proxy services, without impacting any configuration or interface settings. The check box is located at the top of the **Proxy Services** tab (**Configuration > Services > Proxy Services**). If the check box is enabled, the check box label displays in red to highlight that the configured proxy services are being bypassed. When force bypass is disabled, the ProxySG resumes normal proxy services.

When the **Force Bypass** switch is enabled, existing connections will continue to be tunneled; only new data connections are bridged. When a ProxySG is used as a concentrator, no new ADN connections will be negotiated.

Force bypass mode is specific to SGOS 5.4. Downgrading while running in bypass mode will result in a restoration of proxy services.

Configuring WCCP Settings on the ProxySG

WCCP settings can now be configured using the Management Console on the ProxySG. The new **Configuration > Network > WCCP** tab allows you to configure WCCP versions 1 and 2.

For WCCP version 2, you can add and edit service groups and assign an interface, select the forwarding and returning type, select hash or mask assignment type, add weights for load balancing, select the ports and protocols to redirect, and choose unicast or multicast addressing.

The forwarding and return methods supported on the ProxySG are:

Forwarding type	GRE	L2	L2
Returning Type	GRE	L2	GRE

You can also configure passwords for service groups; the password is encrypted.

To review WCCP service-group status and statistics go to the **Statistics > Network > WCCP** page.

Updated Proxy Services Interface

The services GUI has been updated to include a drop-down menu to toggle **Intercept All** and **Bypass All** at the service-group level. This feature allows users a simplified method of changing listener settings at the service-group level. This toggle will change all listeners in a particular service. Selecting individual listeners within a service changes the drop-down menu to **Mixed**. Services with a single listener no longer have a drop-down menu at the listener level. Instead, a service level down-down will control the listener.

To assist in readability, listener configuration drop-down menus are indented by listener level. The change makes it easier to switch the listener setting to the desired level.

Networking

Change in Default List of Bypassed Services

Because interactive and encrypted traffic cannot benefit from optimization, these service groups are now set to be bypassed, using the **Bypass All** setting. Although you can manually set individual services to be intercepted, it is not recommended unless you have a specific reason for doing so (for instance, the port usually associated with the service is used for a custom application on your network). In addition, a number of new predefined services have been added to the Interactive and Encrypted service groups.

The new services added to the Interactive service group are: Echo, Time, Remote Telnet, BGP, Remote Login/Shell, NetMeeting, H.323, ICU-II, MGCP, pcAnywhere, and SIP.

The new services added to the Encrypted service group include: TACACS, IMAP4S, LDAPS, FTPS, L2TP, PPTP, Oracle over SSL, IBM DS, Tivoli DS, and SIP over SSL. In addition, an Other SSL service is predefined with a set of SSL-related ports.

Displaying Duplex Mismatch

The **Interface Utilization** panel in the **Statistics > Summary > Efficiency** tab displays whether the interface is in use and functioning. It also displays the duplex settings and includes the following information:

- ☐ **Up or Down:** **Up** indicates that the link is enabled and can receive and transmit traffic. **Down** indicates that the link is disabled and cannot pass traffic.
- ☐ **Auto or Manual:** Indicates whether the link is auto-negotiated or configured manually.

- ❑ **10Mbps, 100 Mbps, or 1Gbps:** Displays the speed of the link.
- ❑ **FDX or HDX:** Indicates whether the interface uses full duplex or half duplex connection, respectively. In some cases, if a duplex mismatch occurs when the interface is auto-negotiated and the connection is set to half-duplex, the display icon changes to a yellow warning triangle. If you see a duplex mismatch, you can adjust the interface settings on the ProxySG in the **Configuration > Network > Adapters** tab.

Enforce LAN/WAN Concept in WCCP Deployment

In an in-path, bridged deployment, the ProxySG can distinguish traffic coming from the LAN from traffic coming from the WAN based on the interface on which it receives a packet. However, in a WCCP deployment, traffic from the LAN and WAN are both redirected to the ProxySG from the WCCP router over a single, physical interface. In previous SGOS versions, the ProxySG would not be able to distinguish LAN and WAN traffic for WCCP, therefore the ProxySG could not handle LAN traffic differently from WAN traffic. For example, you could not elect to bypass all traffic coming in from the WAN.

SGOS 5.4 allows you can extend the interface definition for the ProxySG to include VLAN interfaces. By creating two separate VLAN interfaces on the ProxySG—one for LAN traffic and one for WAN traffic—the ProxySG can now distinguish inbound and outbound traffic and make the appropriate forwarding decision.

To use this feature, you must create a VLAN trunk between the ProxySG appliance's WCCP interface and the network device to which it is connected. You must then ensure that the appropriate VLANs for ProxySG traffic are created on the ProxySG and all other network devices in-path to the WCCP router.

When creating the WCCP configuration on the ProxySG and the WCCP router, you must create separate service groups—one for LAN traffic and one for WAN traffic—and apply them to the corresponding VLAN interfaces that you defined for your LAN and WAN traffic.

On the ProxySG, the syntax of the WCCP interface parameter has been extended to include a VLAN identifier (*<VLAN_ID>*) as follows:

```
interface 0:1.2
```

where the .2 represents VLAN 2. You must create the VLAN before referencing it in a WCCP service group configuration.

The VLAN interfaces that you have defined are also available from the **WCCP** tab in the Management Console (**Configuration > Network > WCCP**). You can now select a physical interface (0:0 for example) or a virtual interface (0:0.2 for example) from the **Interface** drop-down list.

Handling Non-Routable Addresses

To increase stability within internal networks, a TCP tunnel proxy service is now used to access internal sites and servers. As a result, the HTTP service has been split into three services:

Proxy Service		Listener(s)	
Service Name	Default Proxy	Supported IP Addresses	Port
External HTTP	HTTP Proxy	Transparent	80
Explicit HTTP	HTTP Proxy	Explicit Explicit	8080 80
Internal HTTP	TCP tunnel	Private Subnets <ul style="list-style-type: none"> • 10.0.0.0/8:80 • 172.16.0.0/12:80 • 192.168.0.0/16:80 • 169.254.0.0/16:80 • 192.0.2.0/24:80 	80

New ProxySG appliances or those that have been restored to factory defaults, will use the split HTTP services. Customers who upgrade from earlier SGOS versions will not experience any functionality impact—all settings and services are retained from the previous version. Should the new services be required, you can manually import them. You can also edit the HTTP service to use either the TCP tunnel or the HTTP proxy and add custom listeners to suit your particular needs.

Important: The **Internal HTTP** service uses the TCP tunnel for handling all traffic destined for the private subnets listed above. However, the TCP tunnel does not support proxy functionality. If you wish to use proxy functionality, you must edit the Internal HTTP service to use the HTTP proxy instead of the TCP tunnel.

Explicit Listener Filter

Multiple listener matching behavior has been updated to maximize compatibility. Explicit proxy service listeners now have priority over a subnet match. Only explicitly matching destination IP addresses are considered a better match. For example, look at the following listeners:

Listener	Setting
L1	Explicit:80
L2	10.0.0.0/8:80
L3	10.9.59.226 (ProxySG IP address)

An HTTP connection to a ProxySG might match all the listeners in the above table. In such a case, the connection is handled by the most specific listener that matches the request. In this example, L3 is a specific match to a ProxySG appliance's IP address and is considered the best match.

When there is only a subnet and explicit proxy service listener match (L1 and L2), the explicit listener (L1) is the better match. Only listeners with a specific destination IP address are considered better matches to explicit listeners.

Configuring Private Networks

A private network is an internal network that uses private IP addresses that are usually not routed over the public Internet. The ProxySG is pre-configured with private subnets that use non-routable IP addresses. You can delete or add to this list of private subnets in the **Configuration > Network > Private Networks > Private Subnets** tab, and configure private domains on the **Configuration > Network > Private Networks > Private Domains** tab.

This security feature allows you to manage private information within your network. If, for example, you have configured a private domain on the ProxySG, the WebPulse service will not attempt to dynamically rate content for the private network host or URL. Thereby, information about your private network does not traverse the Internet.

Change in Defaults for TCP/IP Loss Recovery Mode

The TCP loss recovery mode algorithm helps recover throughput efficiently after random packet losses occur over networks, such as in wireless and satellite paths. It also addresses performance problems due to a single packet loss during a large transfer over long delay pipes, such as transcontinental or transoceanic pipes.

The TCP loss recovery mode is now set to *Normal*, by default. Blue Coat recommends that you consider non-normal loss modes — *Enhanced* or *Aggressive*, only when you experience packet losses of 0.5% or greater.

For more information, see TCP/IP Configuration in *Volume 5: Advanced Networking*.

ProxyClient

SGOS 5.4 introduces several usability and statistical reporting enhancements, for the Blue Coat ProxyClient solution.

The Blue Coat ProxyClient solution provides security to mobile users and enables systems that do not reside behind a gateway Blue Coat ProxySG to achieve accelerated performance and ensure users abide by company Web usage policies.

ProxyClient usability enhancements include:

- ❑ The status of ProxyClient acceleration and ProxyClient Web filtering features is now displayed in the **Configuration > ProxyClient > General** tab.
- ❑ ProxyClient Web filtering can be enabled in the **Configuration > ProxyClient > Web Filtering > Policy** tab. To enable ProxyClient Web filtering, Blue Coat Web Filter must be enabled and a valid Blue Coat Web Filter database must be downloaded to the Client Manager.
- ❑ You cannot enable acceleration until the Client Manager is enabled and you specify a Primary ADN Manager and Backup Manager, if any.

Enhancements to ProxyClient statistics include:

- ❑ **Statistics > ProxyClient** now has two menu items: **History** and **Details**. The **Statistics > ProxyClient > Details > Client Details** has four tab pages— **General**, **Acceleration**, **Filtering**, **All**.

- ❑ Maintains information on the number of active and inactive ProxyClients connected to the ProxySG across system reboots. After a reboot, the **Statistics > ProxyClient> Details > Client Version Count** panel will accurately display the number of clients (both active and inactive) the Client Manager has seen.

Web Anti-Virus (ICAP) Features

SGOS 5.4 includes several enhancements to Internet Content Adaptation Protocol (ICAP) support on the ProxySG:

- ❑ The Active Sessions page contains a new filter for displaying per-connection statistics for ICAP traffic. All active ICAP-enabled sessions can be displayed, or you can filter by ICAP status (Transferring, Deferred, Scanning, Completed). Additional ICAP filters are available as well: type of ICAP service (REQMOD or RESPMOD), service name, and status (for example, display only the deferred connections).
- ❑ The new ICAP statistics page displays graphs of historical ICAP data and tables of ICAP statistics. You can view graphs of active ICAP requests, plain vs. secure ICAP connections, completed ICAP transactions, and bytes sent to and received from the ICAP service. The ICAP statistics screen also displays a concise table containing the number of successful and failed requests and number of bytes sent and received for each service or service group during the selected time period.
- ❑ The ProxySG features a new load balancing algorithm that determines which ICAP service receives a scanning request. Previously, a round robin algorithm was used. In SGOS 5.4, the ProxySG calculates an index for each service by dividing the number of waiting transactions by the weight assigned to the server. The ICAP service with the lowest index value will handle the new ICAP action, assuming that the service has an available connection to use. If it doesn't, it will send the request to the service with the next lowest index value that has a free connection. Load will be distributed among services proportionally according to their configured weights until the maximum connection limit is reached on all services.

Known Issues in SGOS 5.4.1.1

This section describes known issues in SGOS 5.4.1.1 that might impact your environment.

- ❑ Access Logging: The MAPI Access log field `x--mapi-user-dn` does not record the value of the userDN string, and sets the value as -. (B#109425)
- ❑ Active Sessions: Some errored sessions display their active sessions status as **Active** (in the **Age** column) and the duration increases although the sessions are inactive. To view the errored sessions that are active, access the **Sessions > Active sessions** tab. (B#103519)
- ❑ Authentication
 - In the RADIUS realm configuration, credential-refresh time may not work if the refresh-time configured is less than 10 seconds. (B#107016)
 - If Session Monitor is enabled, and failover is switched from disabled to enabled or enabled to disabled, you may receive “500 Read Timeout” errors when attempting to access the Session-Monitor Lookup page. (B#110139)

- LDAP authentication using an iPlanet LDAP server that is configured with nested groups causes errors in the VPM. (B#10)
- ❑ ADN
 - In the **Statistics > Sessions > Active Sessions** panel, the byte-caching status of a connection reflects the policy applied for that connection. If byte-caching is manually disabled in the **Statistics > ADN History > Peer Dictionary Sizing** tab, the byte-caching status in **Statistics > Sessions > Active Sessions** still displays as enabled. (B#109679)
 - When you add a peer and set the dictionary size manually for that peer, the ProxySG appliance does not display a warning if you exceed the maximum number of peers that can be configured on the hardware platform. Refer to the *WAN Optimization Sizing Guide* for information on the maximum number of peers for each hardware platform. (B#110102)
- ❑ Connection Forwarding: Connection forwarding cannot be configured for VLAN interfaces. The **Local IP** drop-down menu in the **Configuration > Network > Advanced > Connection Forwarding** tab lists IP address that are associated with a physical interface only. (B#106949)
- ❑ CIFS
 - Visio encounters a file corruption error when saving a .vsd file to an EMC filer through a CIFS proxy over ADN. To resolve this issue, install SP3 for Microsoft Visio 2003. (B#109420)
 - CIFS: MacOS 10.5.6 clients and later will not be able to connect to CIFS Shares on EMC servers. (B#109212)
- ❑ CLI Console
 - The `line vty timeout` setting, when entered manually, is not preserved after reboot. (B#107122)
 - The archive configuration file, `archconf_post_setup.txt` contains configuration for content filtering with MACH5 Edition license. The MACH5 edition license does not include the content filtering features.(B#108552)
 - The `attack detection server` command for limiting the number of server connection requests does not function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B#109184)
 - Issuing the `restart regular with restart mode hardware enabled` produces an erroneous message that an uncompressed core image is being written. No such core is created when issuing a restart command from the CLI. (B#105131)
- ❑ Event Logging: If you upgrade from SGOS 4.3 and then downgrade again some cached objects are invalid and must be removed. Each deleted object generates an event log message. The message reads, for example, `HTTP Object information corrupted, deleting the object`. These messages can be ignored. (B# 107934)
- ❑ FTP: If you are logged in as an anonymous user, the first download attempt of a file larger than the `max-cache-size` fails. Subsequent download attempts will be successful. (B#99917)

- ❑ Forwarding: When a host with multiple IP addresses is added to a load balance group, new connections are not always sent to the host with the least connections. (B#109676)
- ❑ HTTP Proxy: Emule login is not supported on the SOCKS5 proxy. (B#107875)
- ❑ Health Checks
 - After you upgrade from a Mach5 license to a ProxySG license, you must reboot the ProxySG before health-checks become active/available. (B#110098)

- Health checks are not supported with the Mach5 license. Although some health checks display in the Statistics tab of the Management Console, they cannot be edited. (B#110095)
- DNS health check issues(B#110541):
 - If a DNS server cannot resolve www.bluecoat.com, it is marked as unhealthy. In instances where multiple DNS servers are configured but only one DNS server can resolve www.bluecoat.com, only this server is deemed healthy and used for resolving DNS queries. However, if all the DNS servers in the group are deemed unhealthy, the health status is ignored and each server is tried in order to resolve user driven DNS queries.
 - Root DNS servers always report unhealthy because they cannot resolve hostnames.
 - A user defined DNS forwarding group (**Configuration > Network > DNS > Groups**) uses the longest domain as the default hostname for the group. In case the longest domain name is not the appropriate default hostname for the DNS servers in the group, the health check will fail.
- ❑ ICAP: When ICAP scanning is set to deferred scanning mode, the object count displayed for scanned objects (in the **Statistics > ICAP > Completed Requests** tab) is higher on the ProxySG than the count on the ProxyAV user interface. This is because the object count mechanism on both devices are different; the bytes scanned is displayed accurately.(B#107403)
- ❑ IM
 - Non-ASCII character replacement policy does not work with Yahoo IM. (B#85278)
 - AIM 6.8 fails to login when HTTP forwarding is enabled on the ProxySG. SOCKS forwarding works correctly, and can be used instead. In the following example upsocks is the defined SOCKS proxy:(B#106263)

```
<forward>
socks_gateway(upsocks)
```
 - When the Yahoo client is not using the same proxy settings as the browser, file transfers are not supported.
 - im.reflect policy does not work for MSN IM. (B#109044)
 - Yahoo IM: Socks Forwarding policy combined with im.transport (HTTP) property is not supported. (B#109762)
 - If WLM 8.5 is configured using SOCKS, chat room messages are not sent. The workaround is to use the HTTP proxy instead of SOCKS. (B#109546)
- ❑ Management Console:
 - JRE 1.6.0_11 and 1.6.0_12 with Firefox 2.0.0.20 and Firefox 1.5.0.12 intermittently display a Java exception when you click Home while another page loads. (B#109032)

- After an upgrade or downgrade of the SGOS version, the Management Console might hang or throw a Java exception upon reboot. Close the browser page and launch it again to resolve the problem. (B#110413)
 - Rapid context switching between or within the Statistics, Configuration and Maintenance Tabs, may lead to an out of memory condition in the Java Virtual Machine. Click the tab again for the page to load.(B# 108726 and 108791)
- ❑ Networking
- The 1Gbps Copper Network Interface Card does not support a half-duplex connection. (B#108063)
 - Changing duplex configuration on the Integrated NIC on the ProxySG8100 causes link connectivity failure. (B#108779)
 - Changing the duplex configuration, on the pass-through card of the ProxySG 510 or 810 appliance, to half-duplex causes the link speed to drop from 1Gbps to 100 Mbps. (B#108783)
 - A VLAN interface that is part of a failover group cannot be deleted. When you attempt to delete the VLAN interface, the Management Console does not issue an error message, however, the VLAN interface is not deleted. To delete the VLAN interface, you must delete the failover group that is associated with the VLAN and then remove the VLAN interface. (B#110050)
 - Gateway load balancing distribution is not consistently equal across gateways. (B#107839)
 - On boot up, the warning message displayed on duplex, speed, or link speed mismatch might be inaccurate for a hardware bridge. Verify the configuration in the Summary> Efficiency tab in the Management Console. (B#109984)
 - If a bridge is disabled, you can configure different settings for the ports on the bridge. When the bridge is re-enabled to fail-open or fail-closed the settings are maintained and so you could have a hardware bridge with manual 100/half on one side, and auto on the other. This can potentially cause performance problems. (B# 108065)
 - Connection forwarding does not function properly when the **Return-to-Sender Outbound** configuration is enabled. The ProxySG forwards server traffic to the MAC address of the ProxySG peer performing connection forwarding rather than to the server next hop. (B#110559)
- ❑ Policy: Reflect Client IP policy for CIFS cannot be implemented in the Forward layer. `Client.protocol=cifs reflect_ip(client)` must be defined under the Proxy layer. (B#109532)
- ❑ ProxyClient
- The allowable range of values in the **Configuration > ProxyClient > Web Filtering > Log** in the **Upload settings** is 0-99 hours, 0-59 minutes, 0-9999 megabytes. If you enter a value outside this range, the extra digits are truncated and no error message is generated. (B#108048)
 - Currently, the ProxyClient Web filtering can be used with the 60-day SGOS trial license only after you do any of the following:

- (Recommended.) Enable ProxyClient Web filtering from the command line using the following commands:

```
Blue Coat SG200 Series#(config)proxy-client
Blue Coat SG200 Series#(config proxy-client)web-filtering
Blue Coat SG200 Series#(config proxy-client web-
filtering)enable
ok
```

- Contact your Blue Coat representative to get temporary Blue Coat Web Filtering database credentials, then in the Client Manager's Management Console, click **Configuration > Content Filtering > Blue Coat**.

In the **Username** field, enter the user name provided to you by your Blue Coat representative. Click **Change Password** and in the provided fields, enter the password provided by your Blue Coat representative into the provided fields.

You can then enable and use ProxyClient Web filtering. (B#115694)

- ❑ Serial Console: If you accidentally press Ctrl-S and the console becomes unresponsive, use Ctrl-Q to resume. (B#106993)
- ❑ Services: While editing services when the ProxySG appliance is at a 100% CPU utilization the Management Console might freeze. (B#107242)
- ❑ SNMP: SNMP traps are not sent for disk failures. (B#109573)
- ❑ SSH client key configuration: Deletion of a specific client key deletes other client keys that are configured on the ProxySG. (B#107675)
- ❑ SSL:
 - The HTTP POST request generated by the ProxySG appliance for OCSP fails when the request goes through another ProxySG appliance. (B #107608)
In a proxy chain, the workaround is to:
 - a. Create a custom port and use it for TCP-Tunnel on the ProxySG appliance (#2) fronting the OCSP responder.
 - b. Configure OCSP setting on the downstream ProxySG(#1) to use the custom port in the responder's URL.
 - c. Create a TCP forwarding host with server port as 80, on ProxySG appliance(#2).
 - Access log fields `x-cs-ocsp-error` and `x-rs-ocsp-error` are not part of the `ssl` format by default, when upgrading from SGOS 4.x or 5.2 to 5.4. These two fields must be added manually. (B# 107494)
 - An SSL Device Profile cannot be deleted after deleting the authentication realm which uses that SSL Device Profile. (B#106438)
 - When `sslsv2` and `rc4-64-md5` are selected as the cipher in an SLL client, SSL fails to initialize. (B#107847)
 - SSL Proxy does not support connecting to a server using DSA encryption; use TCP Tunnel proxy instead. (B#109099)

- Even if the **Verify Peer** option is disabled in any HTTPS Access Log uploads a certificate mismatch error is logged in the event log. (B#107579)
- ❑ Streaming
 - Pre-population of RealMedia content from web servers does not work. (B#109339)
 - A Windows Media client streaming multi-bitrate live content might get disconnected under low bandwidth conditions. (B#109029)
 - WM-RTSP: The Windows Media client hangs after the live stream switches from audio and video mode to audio-only mode. This problem occurs because thinning might not work when the client is using TCP Transport. (B#116477,62453)
 - Windows Media player might enter a buffering state near the end of the stream when using `rtspt://url`. (B#64430)
 - Some Windows Media content files cannot be pre-populated from a HTTP web server. The workaround is to use streaming speed pre-population instead of line speed pre-population. (B#104035)
- ❑ Storage: Regular expressions in content revalidate command do not work. (B#107056)
- ❑ WCCP
 - The **State** column in the **Statistics > Network > WCCP** tab does not display the complete error message. For example, the **Packet Forwarding Mismatch** error is not fully displayed. Use the `show wccp statistics` CLI command for a listing. (B#108031)
 - When upgrading from earlier versions to SGOS 5.4, the WCCP configuration fails if the `forwarding-type` information is not defined. To prevent a packet return mismatch error during WCCP negotiation, you must explicitly define `forwarding-type` in the WCCP configuration. (B#117444) For example, the configuration should read:

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


Documentation Errata

The following documentation issues could not be fixed before production cut-off:

- ❑ The MMS and RTSP proxies are not included in the list of proxies that support Protocol Optimization. The list should include CIFS, HTTP, HTTPS, MAPI, MMS, and RTSP in the **Statistics > Active Sessions** tab of the online help. This error is fixed in the PDF (Vol 9: Managing the *Volume 9: Managing the Blue Coat ProxySG Appliance* > Chapter 5 > Statistics).
- ❑ The online help documentation states that you can add 10 custom DNS server groups. This is incorrect. You can add up to eight custom entries only, in addition to the primary and alternate DNS server groups. If you attempt to add a ninth custom entry you receive an error message. This error is fixed in the PDF (*Volume 1: Getting Started* > Chapter 7 > Configuring DNS).
- ❑ The Internal HTTP IP subnet 172.16.1.1—172.31.255.255 is incorrect. It should read 172.16.0.0—172.31.255.255. This error is fixed in the PDF (*Volume 2: Proxies and Proxy Services* > Chapter 13 > TCP-Tunnel Proxy Services Supported).
- ❑ Further, the following note has been expanded to include a recommendation to delete the existing HTTP service when upgrading from SGOS version 5.3 to 5.4. The note is fixed in the PDF and it reads:

SGOS version 5.4 and later has three HTTP proxy services by default: External HTTP, Explicit HTTP, and Internal HTTP. Previous versions and upgraded systems have a single HTTP service. Upon upgrade to SGOS 5.4, the new HTTP proxy services are not automatically enabled and must be manually imported should they be required.

If you decide to use the split HTTP services, Blue Coat recommends deleting the existing HTTP service before importing the new services.

Failure to delete the existing HTTP service results in errors, such as a Listener Conflict.

This error is fixed in the *Volume 2: Proxies and Proxy Services* > Chapter 3 > Importing a Service from the Service Library, Chapter 8 > Configuring the HTTP Proxy Service Options, and Chapter 13 > TCP-Tunnel Proxy Services Supported)

- ❑ Kerberos Constrained Delegation: The CPL examples do not use the correct wraparound indicator for extended lines of code. The “/” character does not compile correctly when inserted into the CPL text editor. Those instances have been replaced with “\” which the CPL text editor can properly compile.

This error is fixed in the PDF (*Volume 4: Securing the Blue Coat ProxySG Appliance* > Chapter 18 > Creating the CPL and Chapter 3 > Creating the CPL).

Section U: SGOS 5.4.x — Limitations and Support for Other Products

This section lists support for other products that integrate with the ProxySG and records the limitations of this version of the SGOS. They might be caused by general network limitations or non-ProxySG equipment or applications. Workarounds are provided when applicable.

Limitations

Access Logging

When upgrading from SGOS 4.x or 5.2 to 5.4, Access Log fields `x-cs-ocsp-error` and `x-rs-ocsp-error` are not part of the `ssl` format by default. These two fields must be added manually. (B# 107494)

ADN

- ❑ CIFS uploads over ADN via a 1Gbps/4ms latent WAN link become slower over time. The workaround is to disable byte caching, this seems to resolve the issue; SGOS 5.4.3.7. SR#2-296178771 (B#139477)
- ❑ ADN connections are not re-established after downgrading from 5.5 to 5.4. This issue occurs only in cases where both the ADN tunnel and the ADN Manager are listening on the same port. The workaround is to apply a different port number for either the ADN tunnel or the ADN Manager, before or after downgrading to 5.4.x. This modification will allow the listeners to restart and establish the ADN connection.(B#132461)
- ❑ E-mail attachments are corrupted when a batch of e-mails with JPG or PDF attachments are sent in quick succession. (B#137666, SR 2-286639272)

Authentication

- ❑ Disabling or enabling failover while the **Session-Monitor** is enabled causes **500 Read Timeout** errors. (B# 110139)
- ❑ Radius realm configuration refresh time `rejected-credential-refresh` functionality might not work if the refresh time is configured for less than 10 seconds. (B# 107016)
- ❑ The `New Pin` and `Query` forms are only supported (and only required) for specific versions of RSA (RADIUS) ACE Server. SR#2-209163742 (B#126838)
- ❑ VPM browsing of nested iPlanet referral groups will result in errors (`Unable to obtain search results`). If these referral groups have sub-groups then those groups are not visible in VPM. (B# 102008)
- ❑ The BCAAA service is not supported on Windows NT and Windows Vista.(B#79719)
- ❑ Microsoft only supports Kerberos Constrained Delegation with Windows 2003 native domains. Although Windows Server 2000 supports the Kerberos protocol, it does not support constrained delegation and the protocol transition extensions, both of which are necessary to authenticate with Kerberos Constrained Delegation.

- ❑ When creating and configuring an IWA realm to handle Kerberos, the IWA Realm must use SSL to connect to the BCAA server. Further, the IWA Realm must provide a certificate that BCAA can verify.
- ❑ For Certificate Realms, when using a substitution to construct a Username or Full Username, the new certificate parser supports the following attributes only: `serialNumber`, `subject`, `issuerAltName`, and `subjectAltName` fields.
- ❑ When the Management Console is launched on multiple tabs in the Web browser, only one tab remains active. (B#106942)
- ❑ LDAP authentication users receive a policy denied exception page if the ProxySG appliance detects a loop in the nested groups on the LDAP server.

Refer to *Volume 4: Securing the Blue Coat SG Appliance* > Chapter 9 > Configuring LDAP Properties on the ProxySG appliance > LDAP Search & Group Tabs > About Authenticated LDAP Realm Searches for additional information on nested LDAP groups.
- ❑ Health checks are not supported when using the Mach5 license. (B# 110095)
- ❑ High CPU utilization is noted when LDAP authentication policy contains numerous user conditions.
The workaround is to use LDAP groups rather than individual users. SR 2-224197931 (B#130313)
- ❑ The IBM TDS password expired response is not used by the ProxySG appliance , causing it to not serve an exception page as in the case of AD authentication failure. 2-299103242 (B#140546)
- ❑ BCAA occasionally returns **Too many users--won't work** when one user logs out of and another user logs in due to incorrect Win SSO info provided by the Windows API used by the ProxySG appliance . 2-291631132 (B#141759)
- ❑ URLs longer than 4096 characters result in a 'Parse Error' and, as a result, must go around the ProxySG appliance in order to resolve the URL. SR#2-310461732 (B# 144175)

CIFS

- ❑ Windows Explorer search on CIFS shares does not display folders when the origin server is NetApp, EMC, or Atlas. The workaround is to search with the option **Search tape backup** enabled in Windows Explorer. (B#106514)
- ❑ MacOS 10.5.6 clients and later will not be able to connect to CIFS Shares on EMC servers. (B#109212)
To resolve this issue, login to the MacOS client as a *root* user and mount the CIFS share in the terminal prompt as follows:

```
#mount -t smbfs//<user>:<password@<server>/<share>/<mount-point>
```


This step will help you to access the CIFS share on the finder menu.
- ❑ Visio encounters a file corruption error when saving a `.vsd` file to an EMC filer through a CIFS proxy over ADN. To resolve this issue, install SP3 for Microsoft Visio 2003. (B#109420)

- ❑ `Reflect-client-ip` policies for CIFS does not work from the Forward layer. The `Reflect-client-ip` policies for CIFS must be defined in the Proxy layer. (B# 109532)
- ❑ When ADN is enabled, CIFS file save takes longer than expected. SR# 2-193675919 (B#129279)
- ❑ When managing an OCS through the proxy with SMB signing required, access is denied. (B#135124)

CLI Console

- ❑ The `config proxy-client web-filtering warn` setting in the CLI cannot be properly negated. (B# 108264)
- ❑ Configuring the `exclude-ports` from a client acceleration configuration does not remove the `include-ports` command. (B# 108262)
- ❑ Attack detection `block` and `unblock` settings are not reflected within the system configuration. (B# 109452)
- ❑ The ProxySG appliance's Java GUI didn't show any warning message when installing the same policy rule from the text editor. SR#2-230908952 (B#131079)
- ❑ The CLI displays `NTP enabled` instead of `NTP is enabled` using Blue Coat's NTP servers. This message is erroneous because NTP is enabled only for Bluecoat NTP server. SR# 2-233867949 (B#131726)

Content Filtering

- ❑ The maximum number of categories any single URL can have is 16. (B#104403)
- ❑ Content filtering supports at most 16 categories per url (B# 136593, SR 2-277513242)

FTP

MLSD or MLST are not supported in the current SGOS implementation of the FEAT command. SR#2-300231892 (B# 140467)

Hardware Diagnostics

The ProxySG appliance 210 appliance OS fails to detect the removal of the hardware bridge. (B# 119333)

Hardware Drivers

The network interface card (NIC) is unable to establish a connection when set to 1Gb/ half duplex mode. (B# 108063).

Health Checks

Health checks are not supported with the Mach5 license. Although some health checks display in the Statistics tab of the Management Console, they cannot be edited. (B#110095)

Health Monitor

Health Monitor displays a CPU critical warning in the event log when downloading the SmartFilter database. SR 2-222655015 (B#129709)

HTTP

- ❑ In the case of an HTTP request, when you have a URL rewrite policy, the URL search patterns must be described in lowercase. The ProxySG appliance will always perform a case insensitive search. SR 2-337857952 (B#151206)
- ❑ A crash occurs caused by download of a particular text file in reverse-proxy mode, on two of the customer's SG's. The crash appears to be in function `Transform_handle: : Configure`. SR#2-272652382 (B#136612)
- ❑ Firefox (3.0.10 and higher) and Internet Explorer 8 fail to display HTML exception pages sent from the ProxySG when accessing HTTPS Web sites through exception pages due to browser behavior updates. SR# 2-190436632 (B#121066)
- ❑ Emule login is not supported on the SOCKS5 proxy. (B#107875)
- ❑ If upgrading from SGOS 3.2.8 to SGOS 5.3 or later, clear the cache after upgrading to prevent a restart of the ProxySG appliance. SR 2-186276332 (B#118952)
- ❑ When adding custom headers to the CONNECT request, in case of HTTP CONNECT requests, x-forwarded-for header is not added in second or third request in an authentication handshake. (B# 134674)
- ❑ If a policy contains "http.response.apparent_data_type" condition, this can cause a denied request to succeed or cause stale content to be delivered. (B#137444)

Initial Configuration

While performing initial configuration using the initial configuration wizard, modifying the default gateway from an incorrect IP address/ subnet mask to a valid entry causes ping to fail.

Workaround: Wait to perform any configuration change until the configuration summary screen displays. This summary displays after you answer all the on-screen prompts. (B# 120422)

IPv6 Stack and IPv6 Proxies

The `display` command in CLI does not work using the link-local URL. (B#120765)

Browser/Management Console

- ❑ Infinite loop of authentication popups occurs with older versions of Firefox browser (B# 109433)
- ❑ The Monitoring tab refreshes once per minute. There is a possibility to make a change in configuration and see outdated information, before the system performs a refresh. (B# 108407)
- ❑ When the NTP server list is empty and the Acquire UTC time command is executed, it displays `UTC time was successfully acquired even` when there is no NTP server. (B# 122335)

- ❑ Leap year dates for February 29 cannot be set in the Management Console. The workaround is to change the `1 Mar 2012` again to `29 Feb 2012`. (B# 119314)
- ❑ The Management Console hangs on first access with Internet Explorer 7 when the Phishing filter is set to default. The JRE - Java Plug-in 1.6.0_12 exception occurs. (B#110413)
- ❑ When policy is set to intercept HTTPS traffic, Firefox often displays a message about an untrusted CA. This also causes Firefox to send an alert back to the ProxySG and that event is echoed in the event log. This is not a break in SSL; it is the ProxySG reporting what Firefox sent to it. To bypass the message in Firefox, add an exception for the requested secure page. To avoid having to add an exception for each visited secure Web site, you can add the certificate that the ProxySG uses to sign the Web site certificate into the Firefox trusted root CA. (B#122022)
- ❑ An `Out of memory` error is encountered on **Statistics > Proxy Client > Details** page during a 11,000 client stress run. (B# 122553)
- ❑ Any changes done with the WCCP configuration interface overwrites any Text Editor configurations. SR# 2-293602131 (B#138424)

Network Drivers

- ❑ Changing the duplex on ProxySG appliance 8100 Cobra to HDX switches the speed from Gigabit to 100MB. (B#108783)

Network Security

- ❑ The `attack-detection server` command for limiting the number of server connection requests does not properly function and the `show attack-detection server statistics` command does not correctly display the number of active requests. (B# 109184)

Networking

- ❑ When both the ProxySG and its directly connected device are not set up for auto-negotiation, relying on *auto sense* for a Gigabit Ethernet interface might not sense the speed and duplex of the link. (B#119562)
- ❑ The ProxySG210 platform does not support the configuration of Gigabit speed capacity on interface ports. (B#120156)
- ❑ In SGOS 5.4.x and higher, when an interface is down, the ProxySG appliance responds to ARP Request with the MAC address of the receiving interface instead of the interface on which the target IP address is configured. To ensure that the proxy returns the MAC address of the interface, invoke the following CLI command (in enable mode):

```
tcp-ip-arp-strict-matching
```


SR# 2-192155074 (B#122054)
- ❑ Changing the duplex setting on the ProxySG 8100 Cobra to HDX results in a lowered speed setting, from 1Gb to 100Mbps. (B# 108783)
- ❑ In high latency environments, such as Satellite links, the ProxySG does not fill the TCP pipe. SR 2-196516352, 2-198038592, 2-205807029, 2-210041372 (B#124519)

- ❑ In a split-DNS, chained-proxy environment, the child proxy continues to send lookups to the primary DNS server after health-check reports it as unhealthy. A work-around is to add a condition `url.host.is_numeric=yes` in front of any condition. SR 2-161499392 (B#121987)
- ❑ On the ProxySG 800, interface 2:0 does not respond to incoming requests after upgrading to SGOS 5.x. SR 2-171069702 (B#117121)
- ❑ TCP Tunneled connections that are in the established state take between 2-4 hours before they are terminated. SR 2-225187609 (B#130014)

Policy

- ❑ The `deny.unauthorized (no)` property in the CLI is configured within the `<proxy>` and `<ssl>` layers using the following inline command: `deny.unauthorized(no)`. (B# 117482)
- ❑ When new Content Policy Language (CPL) gestures are introduced to a maintenance release, a system downgrade to an earlier release causes policy compilation error message because the new gesture is not supported in the previous version. (B#122705)
- ❑ The **ftp.server_connection (immediate)** property in the CPL is configured within the `<proxy>` and `<cache>` layers using the following inline command: `ftp.server_connection(immediate)`. (B# 117484)
- ❑ Using "virus_detected=yes" test in policy always triggers an exception page. (B# 136334) Use the following workaround:

```
;-----
<Exception>  condition=sslexception
            action.mycookie (yes)
<Proxy>
            url.substring=xyzallow request.header.cookie="sslallow"
action.rewtohttps (yes)
            request.header.cookie="sslallow" action.red (yes)
<ssl>
            url.substring=xyzallow server.certificate.validate.ignore(all)
define condition sslexception
            exception.id="ssl_server_cert_untrusted_issuer"
            exception.id="ssl_server_cert_expired"
            exception.id="ssl_domain_invalid"
end
define condition sslallow
            url.substring=xyzallow
end
define action rewtohttps
            rewrite( url, "(.*)\?xyzallow", "$ (1)" ) end
define action mycookie
            set(exception.response.header.Set-Cookie,
"sslallow$(url.cookie_domain)") end
define action red
            redirect(307, "(.*)", "$ (1)?xyzallow") end
```

```
;-----
```

And replace it with the following:

```
;-----
```

```
<ssl>
    client.protocol=https url.substring=bluecoat-ssl-allow
    server.certificate.validate.ignore(all)

<proxy>
    client.protocol=https url.substring=bluecoat-ssl-allow
    action.rewtohttps(yes)

define action rewtohttps
    rewrite(url, "(.*)bluecoat-ssl-allow", "${1}") end
;-----
```

Note: Each of the 3 exception pages on the ProxySG need to be adjusted to work properly with this changed policy.

Instead of the "exception.ssl_server_cert_untrusted_issuer",
"exception.ssl_server_cert_expired",
and "exception.ssl_domain_invalid" exceptions containing: action="\${url}"

Replace with:

action="\${url}bluecoat-ssl-allow"

- ❑ Ask.com has changed its SafeSearch mechanism from a cookie-based one to a query-string based mechanism. If you are using the SafeSearch policy in your network, to ensure that undesirable mature content is blocked, please update the SafeSearch policy as shown below (B#140459):

Replace

```
; === SafeSearch for Ask ===
;
; === BC_SafeSearch_Ask Domains/Hostnames ===
define condition BC_SafeSearch_Ask_Domains
    url.domain=ask.com url.host=!wzus.ask.com
    url.host=!mystuff.ask.com
    url.domain=ask.co.uk url.host=!wzus.ask.com
    url.host=!mystuff.ask.com
end
;
; === BC_SafeSearch_Ask Rules ===
<proxy BC_SafeSearch_Ask_cookies>
condition=BC_SafeSearch_Ask_Domains
    request.header.cookie="adt=|adlt="
action.BC_SafeSearch_Ask_Cookie_Rewrite(yes)
    action.BC_SafeSearch_Ask_Cookie_Addition(yes)
;
```



```
; === BC_SafeSearch_Ask Defines ===
define action BC_SafeSearch_Ask_Cookie_Addition
    append(request.header.cookie, "gset:adlt=0")
end
define action BC_SafeSearch_Ask_Cookie_Rewrite
#if release.version=5.4..
    rewrite(request.header.cookie, "(.*)adt=(.*)", "$ (1)adt=0$ (2)")
#endif
    rewrite(request.header.cookie, "(.*)adlt=(.*)",
"$ (1)adlt=0$ (2)")
end
;
```

With

```
; === SafeSearch for Ask ===
;
; === BC_SafeSearch_Ask Domains/Hostnames ===
define condition BC_SafeSearch_Ask_Domains
    url.domain=ask.com url.host=!wzus.ask.com
url.host=!mystuff.ask.com
    url.domain=ask.co.uk url.host=!wzus.ask.com
url.host=!mystuff.ask.com
end
;
; === BC_SafeSearch_Ask Rules ===
<proxy BC_SafeSearch_Ask_cookies>
condition=BC_SafeSearch_Ask_Domains
    url.query.regex="adt="
action.BC_SafeSearch_Ask_Query_Rewrite(yes)
;
; === BC_SafeSearch_Ask Defines ===
define action BC_SafeSearch_Ask_Query_Rewrite
    rewrite(url, "(.*)adt=(.*)", "$ (1)adt=0$ (2)")
end
;
;
```

- ❑ On occasion, the PAC/WPAD redirection failed with 400-invalid_request when policy was used. Blue Coat recommends using policy gesture request_redirect instead of redirect. This was first introduced in SGOS 5.5.7.1. (B#145454, SR 2-307668872)

Proxy Client

The allowable range of values in the **Configuration > ProxyClient > Web Filtering > Log** in the **Upload settings** is 0-99 hours, 0-59 minutes, 0-9999 megabytes. If you enter a value outside this range, the extra digits are truncated and no error message is generated. (B#108048)

SOCKS Proxy

The upstream proxy might display the **SOCKSHistory>ClntComp.Gain** calculation as **100%** instead of **0%** within proxy chain environments. (B# 107429)

Streaming

- ❑ In an proxy chain environment, with log forwarding enabled (on the downstream proxy), where multiple clients are requesting the same live streaming from a playlist with multiple files. Their requests are going into a `waiting` state causing delays or errors. (B# 109745)

- ❑ Pre-population of RealMedia content from Web servers does not work. (B#.109339)

- ❑ In transparent proxy mode, Windows Media Player 10 can not access:

```
http://financialserv.edgeboss.net/wmedia/financialserv/
committeemeeting010509.wvx
```

The MMS server returns `ErrorCode: (0x80070002)`. This is an isolated case caused by third party software that is unable to comprehend or tolerate the information sent between the ProxySG and the Origin Content Server (OCS). (B#109805)

- ❑ When an explicit proxy chain environment with authentication is enabled, live stream requests hang when streaming WM-HTTP content. (B# 118032)

SSL

- ❑ By default, hostname mismatch certificate validation will not occur unless the full SSL interception is enabled. (B#119542)

- ❑ Certain ciphers can not be set as the only cipher on HTTPS-Console. (B#138254)

- ❑ Even if the **Verify Peer** option is disabled in any HTTPS Access Log uploads, a certificate mismatch error is logged in the event log. (B#107579)

- ❑ SSL fails to initialize when `sslsv2` and `rc4-64-md5` are selected as the cipher in an `ssl-client`. (B#107847)

- ❑ SSL Proxy does not support connecting to a server using DSA encryption; use TCP Tunnel proxy instead. (B#109099)

- ❑ SSL access to the URL `www.hipassplus.co.kr` fails when using from Opera10 or Firefox 3.5. The ProxySG reports an SSL Certificate Verification Error because the intermediate certificate "SignKorea mCA" uses critical extensions that are not supported by ProxySG appliance.

The workaround is to disable the SSL proxy for the URL or disable certificate validation in the SSL layer for the specific URL(s). SR 2-195383742 (B#123410)

- ❑ On SGOS v5.3 and later, self signed ProxySG appliance generated certificates have a validity of 2 years. This includes `default` and `passive-attack-protection-only-key` certificates. (B# 132809)

TCP/IP and General Networking

- ❑ Configuring additional static route entries prompts the incorrect warning message. (B# 120931)

- ❑ Poor performance might be experienced when a hardware bridge is re-enabled to fail-open or fail-closed because the bridge settings might revert to inconsistent settings. (B# 108065)

Windows Media Proxy

- ❑ Windows Media over HTTP fails when the URL format is `http://<Proxy_SG_IP>/redirect?mms://<streaming_server>/<filename>.wmv`. The workaround is to use `http://<Proxy_SG_IP>/redirect?http://<URL>` instead of using `http://<Proxy_SG_IP>/redirect?mms://<URL>`. SR 2-198319392 (B#124346)
- ❑ An **Object not found** error message is sometimes encountered after pulling a file from the media server and saving it with a false name. (B# 119290)
- ❑ The `x-duration` field is logged inconsistently for streaming URLs using the Silverlight plug-in on web-browsers due to Silverlight's deviation from normal operating procedures as mandated by the MS-WMSP protocol. 2-288378452 (B#139720)

Support for Other Products

This section provides the required versions of other products that interact with the ProxySG.

Supported Clients and Browsers

The following are the combinations of OS, browser, and Sun Java Runtime Environment (JRE) versions supported for the Web-based Management Console (MC) and the Visual Policy Manager (VPM).

Supported Operating Systems

The supported operating systems for the Management Console and VPM are as follows:

- ❑ Microsoft Windows™ 2000 Pro (SP4 or later)
- ❑ Windows XP (SP2 or later)
- ❑ Windows Vista

Supported Browser Versions

Blue Coat tested the following browsers. Others might work, but Blue Coat cannot guarantee their functionality. The supported browser versions for the MC and VPM are as follows:

- Internet Explorer 7.0
- Internet Explorer 6.0 (SP1 or later)
- Firefox 3.6
- Firefox 5.0--9.0

Supported JRE Versions

Supported Java JRE versions:

- 1.5.0_15 and later
- 1.6 (except 1.6_05, which causes VPM Help problems)

Version 1.4.1_07, which was supported in SGOS 5.3.x, is not supported in SGOS 5.4.x.

Notes

- ❑ On the Sun download page, Sun naming conventions refer to JRE 5.0 and JRE 1.5 interchangeably. JRE 5.0 is Sun's new name for JRE 1.5.
- ❑ You might experience a problem downloading the latest supported JRE through the Management Console if:
 - The browser does not support automatic download.
 - The automatic download hangs.
 - The Java Installer displays an error: HTTP Status Code=302 followed by a popup that java 1.5.x cannot be downloaded.

If you experience any of these issues, 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 delays and/or slow processor speeds might affect JRE performance, slowing the display of Management Console menu selections and options.
- ❑ 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.
- ❑ If your system is running JRE 1.6_05, the VPM Help system does not display or function correctly.

Blue Coat Director, Reporter, and ProxyClient

Director

SGOS 5.4 is compatible with SGME 5.4.x. If you are using Blue Coat Director to manage your ProxySG appliances, use overlays to fine-tune configuration specifics after upgrade. Do not push a device profile created in an earlier SGOS version to a ProxySG appliance that has been upgraded. For more information on profiles and overlays, refer to the Director documentation.

Consult the following table before attempting to manage ProxySG appliances:

Director Version	Manages SGOS versions....
6.x and 5.5.x	SGOS 6.1.x, 6.2.x, and 6.3.x SGOS 5.3.x, SGOS 5.4.x, and SGOS 5.5.x SGOS 4.3.x

Director Version	Manages SGOS versions....
5.4.2.x	SGOS 5.3.x and SGOS 5.4.x
5.4.2.5	SGOS 4.3.x Exception: Director V 5.4.2.5 manages SGOS 5.5.1.1 in addition to the above versions.
5.4.1.x	SGOS 5.4.x, SGOS 5.3.x, SGOS 5.2.x, SGOS 5.1.x SGOS 4.2.9 and later, including 4.3.x Limitation: You can use VPM in SGME 5.2.x and later to push policy to devices running SGOS 4.2.x, where $x > 9$ or SGOS 5.2.2.x or later only. If a device runs SGOS 4.2.9 or earlier or 5.2.1 or earlier, use the SGOS Management Console on each device to change policy on the device.

Reporter

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

Note: Beginning with SGOS 5.4.2.x, Reporter 9.x is supported for SGOS 5.4.x.

ProxyClient

ProxyClient versions 3.1.x and 3.2.x are compatible with SGOS 5.4. To download the latest version, refer to the *Blue Coat ProxyClient Release Notes*.

Anti-Malware

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

This release is compatible with AVOS 3.x and AVOS 2.x.

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

Instant Messaging

This section details the Instant Messaging proxy support for English language versions. While some versions of AIM and Windows Live Messenger (WLM) are not officially supported, they work in most situations.

Video and audio are not supported with any of the Instant Message protocols: MSN, Yahoo, AIM and WLM.

English Language Versions Supported

Table 1-1. IM Client Compatibility Matrix

Client Version	SGOS 5.4 Support	Comments
AIM 5.9	Yes	
AIM 6.1	N/A	No longer available. See "Partially Supported IM Protocol Versions" below.
AIM 6.5	Limited	This version was not officially tested, but full proxy support should work. See "Partially Supported IM Protocol Versions" below.
AIM 6.8	Yes	AIM 6.8 is supported in explicit SOCKSv5 and HTTP/HTTPS proxy configurations only. For AIM 6.8 support, you must purchase and import a CA signed SSL certificate on the ProxySG.
AIM 6.9	Limited	This version was not officially tested, but full proxy support should work.
Windows Messenger 4.x	Yes	(4.0-XP, 4.7-XP+SP2)
Windows Messenger 5.x	Yes	
MSN Messenger 7.0	Yes	This is the last version that supports Windows 98 and Windows ME.
MSN Messenger 7.5	Yes	
WLM 8.0	Yes	Name changed from MSN to Windows Live Messenger (WLM); Microsoft deprecated this version in favor of WLM 8.1.
WLM 8.1	Yes	In 2007, Microsoft rendered as obsolete all versions previous to 8.1 because of a security issue.
WLM 8.5	Yes	
WLM 2009	Yes	In 5.4.x, WLM 2009 is tunneled. This version is also known as version 14.0. See "Unsupported IM Client Policy" on page 123.
Yahoo 5.5, 5.6	N/A	In April 2008, Yahoo! retired these client releases.
Yahoo 6.0, 7.0, 7.5	N/A	In August 2009, Yahoo! retired these client releases.
Yahoo 8.0, 8.1	Yes	
Yahoo 9.0	Yes	In 5.4.x, WLM 2009 is tunneled. See "Unsupported IM Client Policy" on page 123

Japanese Language Versions Supported

- ❑ AIM 5.1
- ❑ Yahoo 7.0
- ❑ WLM 8.0

Partially Supported IM Protocol Versions

AIM

The ProxySG does not recognize transparent AIM 6.x as AIM (IM) traffic. In some ProxySG configurations, however, client login and chat do succeed.

- ❑ AIM 6.x
 - 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 6.1 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.
- ❑ AIM 6.5
 - 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 AIM 6.0, 6.1 clients, and for transparent proxy deployments of AIM 6.5 and 6.8 clients, the following policy can be used:

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

Open SSH

SGOS 5.4.x supports OpenSSH version 5.1.

Open SSL

SGOS 5.4.x supports OpenSSL version 0.9.7m.

Peer-to Peer (P2P)

The P2P protocols supported on the ProxySG include:

- ❑ BitTorrent, with the exception of encrypted BitTorrent
- ❑ Gnutella
- ❑ eDonkey

SOCKS

SGOS 5.x supports SOCKS v5, authentication protocol v1.

Streaming

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

- ❑ The ProxySG supports the following versions and formats:
 - Windows Media Player 7-11
 - 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
 - Helix Player 11
- ❑ 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

WCCP

SGOS 5.4.x was tested with several releases of Cisco's IOS: 12.0.7, 12.1.6E, 12.2.18. For a list of Cisco platforms that support L2 packet return, go to www.cisco.com.

Copyright© 1999-2013 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™, ProxyOne™, CacheOS™, SGOST™, SGT™, Spyware Interceptor™, Scope™, ProxyRA Connector™, ProxyRA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, PacketShaper®, PacketShaper Xpress®, PolicyCenter®, PacketWise®, 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. AND BLUE COAT SYSTEMS INTERNATIONAL SARL (COLLECTIVELY “BLUE COAT”) DISCLAIM 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, 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.

Americas:

Blue Coat Systems, Inc.

420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL

3a Route des Arsenaux
1700 Fribourg, Switzerland