Blue Coat SGOS 6.3.x Release Notes

Version: SGOS 6.3.3.1
BCAAA Version 130
Release Date: 06/06/2012
Document Revision: 06/06/2012

Release Note Directory

These release notes present information by each release in the SGOS 6.3.x software line. Each section provides feature descriptions, fixes and known issues.

SGOS 6.3.x Feature Matrix

The following table lists the features introduced in the SGOS 6.3.x release line, with cross-reference links to feature descriptions.

Component	Feature	Introduced
Authentication	"IWA Direct" on page 21	6.3.1.1
	"Authentication Realm Validation" on page 22	6.3.1.1
ADN	"Enhanced Performance of TCP Tunnel Proxy" on page 22	6.3.1.1
	"Preferred IP Selection for ADN" on page 23	6.3.1.1
	"Sky UI Enhancements" on page 23	6.3.1.1
	"Byte-Cache Retention Policy" on page 26	6.3.1.1
	"Thin Client Processing" on page 27	6.3.1.1
Content Filtering	"Web Application Control" on page 28	6.3.1.1
Proxies: CIFS	"SMBv2 Support in the CIFS Proxy" on page 29	6.3.1.1
Proxies: Flash	"Acceleration of Encrypted Flash Traffic" on page 30	6.3.1.1
Proxies: HTTP	"Force Cache Policy" on page 31	6.3.1.1
Proxies: SSL	"Client Certificate Authentication" on page 33	6.3.1.1
	"Downloadable CA List" on page 34	6.3.1.1
	"Preserve Untrusted Certificate Issuer" on page 35	6.3.1.1
	"SSL Intercept Based on Authentication Credentials" on page 35	6.3.1.1
	"Configurable HTTP Connection Timeout" on page 8	6.3.3.1
Reporting	"HTTP Application Traffic Category Reporting" on page 36	6.3.1.1

Section A: SGOS 6.3.x Reference Information

This section applies to all SGOS 6.3.x releases.

Important Notes About SGOS 6.3.x

Before beginning the upgrade process, you must read the following information:

- If you are using the Blue Coat Authentication and Authorization Agent (BCAAA), SGOS 6.3.x requires BCAAA version 130, (located on the 6.3.x BlueTouch Online download page). Even if you are already running version 130, be sure to upgrade to a current BCAAA version (one associated with SGOS 6.2.x or later) because the newer versions contain a security vulnerability fix. You must upgrade to BCAAA version 130 before upgrading to SGOS 6.3.x. Do not upgrade SGOS unless you have first installed the compatible BCAAA version. Refer to the following documents for more information:
  - The *BCAAA Read Me* for BCAAA sizing requirements. This Read Me is posted with the BCAAA version on the BTO download portal.
  - The Blue Coat SGOS 6.3.x Upgrade/Downgrade Guide for instructions to upgrade or downgrade BCAAA.
- Direct upgrade from SGOS 4.x to SGOS 6.3.x is not supported. If you are upgrading to SGOS 6.3.x from SGOS 4.x and the appliance has previously run SGOS 5.x, the 5.x configuration is applied during upgrade. You must restore the SGOS 4.x configuration settings. The *Blue Coat* SGOS 6.3.x *Upgrade/Downgrade Guide* contains this procedure, but continue reading these Release Notes for further upgrade information.
- SGOS 6.2 introduced an increased object store capacity option for its multi-disk appliances. This configuration is incompatible with previous SGOS versions and if this option is enabled when you downgrade, an error message occurs and all data and settings are lost.

  To avoid the error before downgrading, enter the following command in enable mode: `proxysg# disk decrease-object-limit`

  After entering the command, the system reinitializes the disks. If successful, a message displays stating that the disk object limit decrease has been completed. After completion you may proceed with downgrading. For more information, see the *Blue Coat SGOS 6.3.x Upgrade/Downgrade Guide.*
- For SGOS 6.3.x, the oldest supported JRE is 1.5.0_15. See "Java Runtime Environment (JRE) Information" on page 7.

To proceed with the upgrade, go to "About Upgrading to this Release" on page 4.

Product Documentation

Access the SGOS 6.3.x product documentation on BlueTouch Online:

https://bto.bluecoat.com/documentation/sgos-63

Automatic Notification of New Software Releases

To be automatically notified when new ProxySG software releases are available, you can subscribe to the ProxySG appliance and/or SGOS 6 product information channel in the Knowledge Base:

1. Log in to BTO.
2. Go to **Knowledge Base > Product Information > Products > ProxySG**

   or **Knowledge Base > Product Information > OS > SGOS 6**
3. Click **Subscribe**.

You will then receive email messages to let you know when new software releases are available for download. Click the link in the email to view the KB article. The article will provide you with the following types of information for the new release: the release number, the date the software was posted, highlights of the release, and links to related documentation and training materials.

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

About Upgrading to this Release

After verifying the prerequisites stated in the following sections, read and follow the SGOS 6.3.x *Upgrade/Downgrade Guide* (https://bto.bluecoat.com/doc/17153). This document details the required process for upgrading to this release, including BCAAA upgrade procedures. Blue Coat also recommends reading the *SGOS 6.3.x Upgrade/Downgrade Feature Change Reference* for an explanation of how new features are affected by the upgrade or downgrade process.

Important: Schedule your upgrade during off-peak hours. If you have ADN configured in a managed deployment, upgrade the ADN Managers—Primary manager and Backup Manager—before upgrading the ADN nodes.

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.

Important: Before upgrading to SGOS 6.3.x, you must resolve all deprecated policy notices. For details on how to do this, refer to the *SGOS 6.3.x Upgrade/Downgrade Guide* (https://bto.bluecoat.com/doc/17153).

Before installing or upgrading to SGOS 6.3.x, perform the following:

1. Determine if SGOS 6.3.x is supported on your hardware platform. See "Supported ProxySG Appliance Platforms" on page 5.
2. Determine your upgrade path. See "Supported Upgrade/Downgrade Paths" on page 5.
3. Understand the BCAAA process. See the *BCAAA Read Me*, which is posted with the BCAAA version on the BTO download portal.
4. Understand how licensing works. See "About SGOS 6.x Licenses" on page 6.
5. Ensure that your browser has the correct JRE installed. See "Java Runtime Environment (JRE) Information" on page 7.
6. Recommended—Learn about the changes and fixes in the SGOS version you are upgrading to. See "SGOS 6.3.3.1, build 86341" on page 8.
7. Recommended—Learn about third-party product support. See Section F: "SGOS 6.x — Support Files and Support for Other Products" on page 53.
8. When you are ready to upgrade a ProxySG appliance, follow the steps in the *Blue Coat SGOS 6.3.x Upgrade/Downgrade Guide* (https://bto.bluecoat.com/doc/17153).

Supported ProxySG Appliance Platforms

The following ProxySG appliance platforms can be upgraded to SGOS 6.3.x:

- 32-bit platforms: SG210 (except for 210-5) and SG510
- 64-bit platforms: SG300, SG600, SG810, SG900, SG8100, and SG9000
- Virtual appliances: VA-5, VA-10, VA-15, VA-20

Note: The SG210-10 and SG210-25 can run SGOS 6.2 and later, but the SG210-5 is not supported on these SGOS releases. SGOS 6.2 and later provide new features and capabilities that require more system resources than available on the SG210-5. The SG210-5 continues to be supported on SGOS 6.1.x releases. Please contact your sales teams for upgrade options.

Supported Upgrade/Downgrade Paths

Before upgrading to SGOS 6.3.x, the ProxySG appliance must be running:

SGOS 5.4.9.1 or higher

SGOS 5.5.6.2 or higher

SGOS 6.1.5.2 or higher

SGOS 6.2.5.1 or higher

ProxySG VA Upgrade Path

- Existing ProxySG VA customers can upgrade from SGOS 5.5 to SGOS 6.3.

- New ProxySG VA customers can download and install the SGOS 6.3 Virtual Appliance Package (VAP). For details, refer to the *ProxySG VA Initial Configuration Guide:* https://bto.bluecoat.com/doc/17311

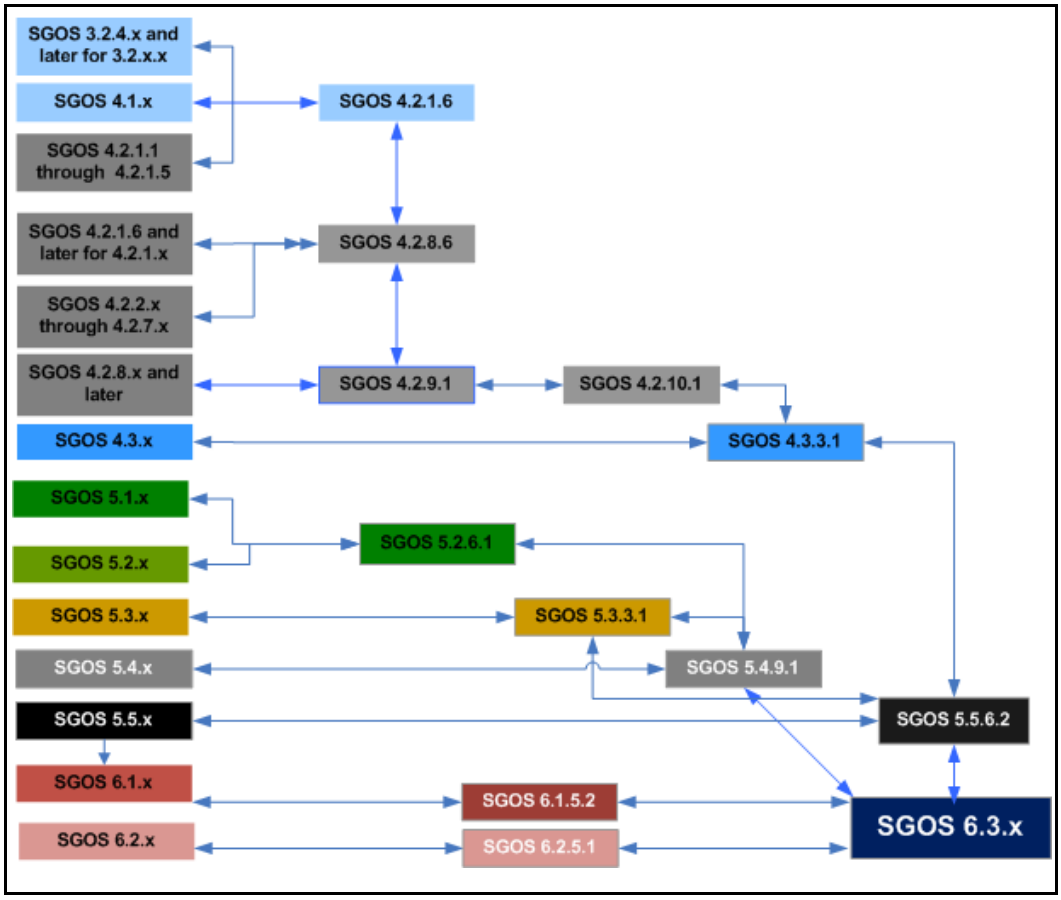


Figure 1–1 Upgrade Path

About SGOS 6.x Licenses

By default, automatic license check is enabled (the **Use Auto-Update** option is selected on the **Maintenance > Licensing > Install** tab). This means that the ProxySG appliance automatically checks for license updates upon reboot or once daily for a month before the currently installed license expires. To verify the current ProxySG appliance/SGOS license, navigate to the **Maintenance > Licensing > View** tab and review the **Licensed Components** area.

Important: Upgrading to a SGOS 6.x license from a previous SGOS version is an important step (that also has prerequisite steps) in the software upgrade process. Refer to the *Blue Coat SGOS 6.x Upgrade Guide* for the Blue Coat-verified procedure.

Java Runtime Environment (JRE) Information

To run the SGOS 6.3.x Management Console, you must install the Oracle Java JRE version 1.5.0_15 or later, including 1.6 (except for 1.6_05, which causes VPM online help problems). JRE 1.4.x is no longer supported. For SGOS 6.3.x, the earliest supported JRE is 1.5.0_15. For additional details about downloading JRE, see "Supported JRE Versions" on page 54.

Section B: SGOS 6.3.3.1, build 86341

Release Date: 06/06/2012, build 86341
BCAAA Version: 130
JRE Version: 1.5.0_15 and later, 1.6 (except 1.6_05)
Compatible with: SGME 6.1.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x

SGOS 6.3.3.1 Contents

See the following sections for information on this release.

Changes in SGOS 6.3.3.1

SGOS 6.3.3.1 introduces the following changes.

Support for New ProxySG Platform

SGOS 6.3.3.1 supports the SG 900-55 model. For higher performance on the Proxy Edition, object caching is disabled by default on this model, but can be re-enabled if desired. Note that caching is enabled by default on the SG 900-55 MACH5 Edition.

Configurable HTTP Connection Timeout

You can specify the IP connection timeout used when attempting to establish a server connection.

```
http.server.connect_timeout(default|N)
```

In this property, `default` indicates the default connection timeout, and `N` is a number from 10 to 120 that specifes the number of seconds to wait before the connection times out. See the *SGOS 6.3 Content Policy Language Reference* for more information. (B#175529)

New CA Certificates

Seven new intermediate certification authority (CA) certificates have been added:

- VRSN_Class3_International_Server_CA_G3
- DigiCert_High_Assurance_CA_3
- DigiCert_High_Assurance_EV_Root_CA
- Network_Solutions_CA
- UTN_UserFirst_Hardware
- Go_Daddy_Sec_CA

- VRSN_Class_3_Ext_Val_SSL_CA

In addition, a duplicate CA certificate was deleted: VRSN_Class_3_Pub_Pri_Cert_Auth_G5

(B#175180, SR 2-453302452, SR 2-469227162)

Resolved Issues in SGOS 6.3.3.1

SGOS 6.3.3.1 contains the following fixes.

ADN

- TCP tunnel byte-caching acceleration no longer becomes degraded over time. This issue occurred in SGOS versions 6.2, 6.3.1.1, and 6.3.2.2. (B#175521, SR 2-450862445)
- In transparent deployments, the ADN load balancer no longer erroneously bypasses transparent connections from a branch office when it can find a concentrator in its database that supports the address type of the destination address. (B#172687)

Access Logging

- Enabling encrypted access logging no longer restarts the ProxySG appliance. (B#173107, SR 2-437914572)

Authentication

- Delegation and administrator credentials are no longer required in order to join a Windows domain. (B#173055, SR 2-434595451)
- IWA Direct is now supported in one sequence realm. (B#172478, SR 2-438042012)
- After upgrading, the ProxySG appliance no longer experiences high CPU usage every 15 minutes when refreshing LDAP information. (B#172753, SR 2-429893505)
- IWA Direct now prompts users whose accounts are locked out (in Active Directory) to re-authenticate instead of displaying an exception page. (B#175250, SR 2-458798164)
- The ProxySG no longer times out while responding to authentication requests. This issue occurred when NTLM requests built up. (B#175286, SR 2-458820092, SR 2-459610917)
- Error messages “Resetting schannel due to nt status 0xC0000199 while authenticating user" and "General error communicating with Active Directory" no longer appear in the event log when a machine account tries to authenticate. (B#175704, SR 2-464879466)
- The ProxySG handles DNS resolution problems on the network better. (B#174767, SR 2-454100032)

CIFS Proxy

- Files accessed via CIFS across an explicit ADN deployment are now refreshed. The issue occurred because the ProxySG didn't perform cache data comparisons. (B#175948, SR 2-462429154)

CLI Console

- Upgrading from SGOS 5.5.x no longer creates an irremovable `threat_protection` configuration in sysinfo (https://<*IP_address*>:8082/sysinfo). This issue applied to MACH5 Edition licenses. (B#173277)

Client Manager

- Restarting the ProxySG appliance after upgrading ProxyClient software no longer causes the software to revert to the previous version. This issue occurred on appliances running SGOS 6.x as well as appliances running SGOS 6.x with an SGOS 5.x image that was never booted. (B#172702, SR 2-422559259)
- ProxyClient download links now work. (B#173027, SR 2-433704900)

Flash Proxy

- When rejecting a connection due to a missing Flash license, the RTMP proxy now closes the socket and policy session, allowing new connections to be accepted. (B#173843, SR 2-426438922)
- Videos at www.indexuniverse.com now play correctly when the following policy is applied:

```
<Forward>
client.protocol=rtmpt server_url.address=72.3.155.202
streaming.transport(tcp)
<Proxy>
client.protocol=rtmpt url.address=72.3.155.202 action.rw(yes)
define action rw
set( url.port, 1935, server )
end
```

  (B#175056, SR 2-452048372)

HTTP Proxy

- Exception pages now display in explicit deployments where the SSL proxy is set to intercept all traffic. Previously, generic browser error pages displayed. (B#174542, SR 2-451971041)
- Page transformation policy is now applied to pages when rewriting via reverse proxy. (B#174672)

Section B: SGOS 6.3.3.1, build 86341

Management Console

- After marking **Enable NTP** (**Configuration > General > Clock**), applying the change, and closing the browser, the **Enable NTP** check box now remains marked when a new browser session is started. (B#169934)
- When web filtering is enabled in ProxyClient settings, web filter categories can now be expanded (**Configuration > ProxyClient > Web Filtering**). (B# 176104, SR 2-458674132, SR 2-465546412)

Policy

- The Perl Compatible Regular Expressions (PCRE) library no longer stops responding when policy that contains an invalid `\k` Perl escape sequence is compiled. (B#176467, SR 2-464081262)
- The ProxySG now correctly translates paths specified in the format *http://user:password@host/policy.txt* as the Remote URL for central policy (**Configuration > Policy > Policy Files**). (B#174488, SR 2-449509892)

SSL Proxy

- When an Enable HTTPS Interception on Exception rule exists in policy, requests to bad DNS names or unavailable servers are now intercepted. (B#175258)
- In previous versions, the ProxySG event log was flooded with SSL handshake and certificate related errors when a client or the server dropped the connection in the middle of the SSL handshake. These error messages are now logged in the SSL debug log. (B#173319)
- When a server returned an expired intermediate Certificate Signing Authority (CA), the ProxySG returned an expired certificate error even when the updated intermediate CA was in the browser-trusted CCL. The ProxySG now checks the local certificate store to see if it has a newer certificate and sets the error accordingly. (B#175662)

SSL/TLS and PKI

- Deleting a keyring via the `delete keyring force clientcert` CLI command no longer causes the ProxySG to stop responding. (B#174384)
- The "CFSSL Cert Proprietor" process no longer causes the ProxySG to stop responding after a reboot. (B#170814)
- The ProxySG is no longer vulnerable to denial-of-service (DoS) attacks via Server Gated Cryptography (SGC) renegotiation. (B#174183)

Section B: SGOS 6.3.3.1, build 86341

SkyUI

- Resizing columns in the Installed Operating Systems panel (**System Settings > Software > Operating System**) no longer causes the button in the Action column to change from **Restart** to **Downgrade**. (B#173282)
- SkyUI now allows entry of characters such as underscore (_) and dollar sign ($) for SMB signing usernames. This matches the behavior of the CLI. (B#173927, SR 2-442501865)

Storage

- The ProxySG no longer restarts with an error in a PG_IDLER process in kernel.exe after SGOS is upgraded from 5.4.x to 6.3.x. (B#173960, SR 2-443752842)

TCP/IP and General Networking

- The ProxySG no longer restarts with an error in a DNS UDP Worker process while parsing a DNS query. (B#173996, SR 2-444150151)
- Virtual Router Redundancy Protocol (VRRP) traffic is no longer dropped. This issue occured when VRRPE multicast packets with MAC prefixes of 02:e0:52 were bridged across a bridge interface. (B#174808, SR 2-452763162)
- The ProxySG no longer restarts with an error in a PG_TCPIP process in libstack.exe.so. This issue occurred in an ADN deployment. (B#174660, SR 2-453622261)
- In transparent deployments where traffic is intercepted over bridge interfaces, websites are now accessible after SGOS is upgraded to 6.3.x. (B#173071, SR 2-431698442)
- The "tcpip_protocol_worker_1" process no longer restarts when the ProxySG parses a malformed DNS query. (B#174067, SR 2-444469501)
- The ProxySG can now join Windows domains where the DNS group is configured with a domain name. (B#175435, SR 2-464515942)
- TCP errors no longer occur as a result of the order of TCP options in the SYN packet that the ProxySG sends. The RFC-1323 TCP options in the SYN packet have been reordered so that all servers can recognize them. (B#175691, SR 2-456424920)

URL Filtering

- Policy that is set to deny uploads now works when users access multiple Google accounts simultaneously. (B#176425, SR 2-465642756)

User Documentation

- The *SGOS Administration Guide* contained incorrect information for creating a Certificate Signing Request (CSR) to be sent to a CA for reverse proxy configuration. The guide has been updated. (B#176720)

Visual Policy Manager

- Statuses of rules (e.g., Disabled) now persist when moving multiple adjacent rules. (B#176107, SR 2-465764582)
- The Add/Edit Methods Objects dialog now shows all the available options for FTP. (B#175589, SR 2-460452581)

Known Issues in SGOS 6.3.3.1

At time of production, Blue Coat knows of the following issues.

ADN

- In the Management Console, the Proxied Sessions tab (**Statistics > Sessions > Active Sessions**) shows no active sessions; however, the Proxied Connections page (https://<*IP_address*>:8082/AS/sessions) correctly shows active sessions. (B#176466, SR 2-453302452, SR 2-469227162)

Authentication

- In an IWA Direct deployment, event logs show “Clearing ldap DC connection list for domain due to a network error" messages, but no packet loss is reported. (B#176431, SR 2-465619312)
- In an IWA Direct deployment with multiple domain controllers (DCs), the ProxySG can’t authenticate if the DC to which the ProxySG belongs goes offline. (B#175751, SR 2-454697142, SR 2-461128082, SR 2-463113622)

Proxy Forwarding

- Proxied users who log in to *https://online.dib.ae* are immediately logged out of the site. (B#175536, SR 2-436652212)

SSL Proxy

- When a web server asks for a certificate, the following policy rule on the SSL Proxy does not work:

  ```
  client.certificate.requested=yes.
  ```

  This occurs because the SSL Proxy does not run any policy rules during SSL renegotiation. (B#175202)

  Workaround: Create a policy for these websites where SSL tunneling is set up instead of an intercept option. For example:

Section B: SGOS 6.3.3.1, build 86341

```
<ssl-intercept>
url=http://www.example.com ssl.forward_proxy(no)
```

Section C: SGOS 6.3.2.2, build 79481

Release Date: 02/07/2012, build 79481
BCAAA Version: 130
JRE Version: 1.5.0_15 and later, 1.6 (except 1.6_05)
Compatible with: SGME 6.1.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x

SGOS 6.3.2.2 Contents

See the following sections for information on this release.

Changes in SGOS 6.3.2.2

SGOS 6.3.2.2 introduces the following changes:

- The regex modifier has been added to `user` in policy (`user.regex=`). This allows you to do a case-sensitive regular expression match against a full user name. This can be used to solve the issue where background services, for example NCSI, get authenticated as `domain\pc-name$`. (B#172406)
- ProxySG now supports up to 200 IWA realms. The realm count on IWA realms has been increased from 40 to 200. The ProxySG appliance continues to support a maximum of 40 realms for all other authentication types. (B#171664)
- The list of User Agents available as a Web Access Layer source in the Visual Policy Manager now includes the agents listed below. (B#169987)
  - Firefox 4.x, 5.x, 6.x, 7.x
  - MS Internet Explorer 8.x, 9.x
  - Opera 10.x, 11.x
  - Chrome 12 and lower, 13.x, 14.x, 15.x
  - Safari 4.x, 5.x
  - iPhone, iPad, iPod, Blackerry, Android, Windows Mobile
  - Wget 1.x

Resolved Issues in SGOS 6.3.2.2

The following issues have been fixed.

Access Logs

- Fixed the issue where all usernames in the `cs-username` field in the access log have '`%00`' added to the end. (B#172052, SR 2-427177992)

ADN

- If you configured an ADN node as Primary ADN Manager and then later configured the node for secure ADN by selecting a device profile, the appliance would no longer be able to locate the ADN manager, and displayed the "Primary Manager ID not set" error (even though the **Primary ADN Manager** setting was still set to **Self**). This has been resolved. (B#169320)

Authentication

- Fixed the issue where IWA Authentication might fail if a username or group contained international characters.
(B#172476, SR 2-432052802, 2-433816302, 2-434486340)
- In an IWA-BCAAA realm, after restarting the ProxySG appliance the web access of an user was denied until the refresh time of the surrogate credentials expired (IWA) because of some background services. (B#172406)
- In an IWA-Direct realm, when a request header contained a SPNEGO InitialContextToken header, NTLM requests would fail. This has been resolved. (B#171513)
- In an IWA-Direct realm, basic authentication failed when a user was a member of a group from a non-existent domain. This has been resolved. (B#171623)
- Fixed the issue that caused a page fault at `0x17F51DE98` in Process group `PG_POLICY_MANAGEMENT` in `kernel.exe` that occur when SSH invokes IWA-Direct before any other service does. (B#172756, SR 2-434388871 2-435873661)
- Fixed the issue that caused a software restart in process `lwmsg server worker` at `.text+0x0` that occurs when clients are sending two NTLM v1 messages to the ProxySG appliance on the same context handle.
(B#171714, SR 2-432154082, SR 2-435931532)
- Fixed an issue where LDAP authentication using a policy that had more than 200 different "user=" conditions for the same LDAP realm, or another realm was using LDAP for authorization, caused the ProxySG appliance to restart. (B#172737)

Content Filtering

- Fixed the issue where connection errors caused the ProxySG appliance to request and download the complete url-filtering database. (B#171009)

Cache Engine

- Fixed the issue where the hanging refresh bandwidth allocation from the CLI disabled automatic bandwidth management until it was re-enabled or the machine was restarted. (B#169451)

Section C: SGOS 6.3.2.2, build 79481

HTTP Proxy

- Fixed a software restart in process `HTTP Admin` in `http.dll` at .t`ext+0x5406d` due to a timing issue occurring under memory pressure. (B#170996)
- The '@import' rule allows users to import style rules from other style sheets. In a reverse proxy configuration, @import fields weren't re-written as expected (W3C in CSSv2). This has been resolved. (B#171837)

Flash Proxy

- When streaming video from a site that uses dynamic chunk size changes, caching was invalidated. This caused playback of these streams to fail when caching was enabled. This has been resolved. (B#169784, 170210)
- For Flash video clients that use pauses while seeking, such as Yahoo video, a ProxySG appliance was not able to cache content or play content from cache after a seek. This has been resolved. (B#156268)
- For some Flash client/server application combinations, playback could freeze after doing a seek. This has been resolved. (B#157785)
- In previous versions, Flash streams of changing chunk size failed to load through the RTMP proxy. These flash videos were reachable via outside Internet access, but got `netstream.play.streamnotfound` at the proxy, and users could not view the video. This issue has been fixed. (B#170210)

Management Console

- When selecting a new appliance failover group and the existing IP option, the Physical IP address of ProxySG appliance did not show up in the **Failover Groups Existing IP** drop down box. This issue has been resolved. (B#171380)
- When using the option to upload service information to an existing Service Request, the 'policy trace' check box is available if a custom or default trace object has been created and written to. However, when selecting this option, the upload process ignores that it had been selected, and did not report the failure in the 'view progress' box when the data was not uploaded. This has been resolved. (B#169838)

Policy

- Fixed the issue where the ProxySG appliance failed to match the policy `request.header.cookie="sslallow" action.red(yes)` at CI checkpoint when apparent data type policy was present. (B#160176, 169358, 169378)

SSL Proxy

- If an SSL Intercept policy was enabled on the ProxySG appliance and there were malfunctioning servers where the OCS does not send the certificate during SSL handshake, the event logs were flooded with `Failed to get the peer certificate` messages. This has been resolved. (B#163272, SR# 2-408255562)
- Fixed the issue that caused a software restart in process `CAG_Maintenance` at `.text+0x0`. (B#171716, SR 2-431639872)
- Support client Certificate authentication during SSL renegotiation has been added. (B#172459)

SSL/TLS and PKI

- Resolved the issue where the event log contains repeating "OCSP: AuthorityInfoAccess extension URL not found in certificate" messages when the OCSP responder is created to use the AIA information in a certificate. (B#172540)
- When attempting to use the `#(config statistics-export) config-path` *URL* command, the error message `Statistics export config download failed: Server certificate signed by unknown CA` was displayed. This has been resolved. (B#171339)

Streaming

- Fixed the issue where customers could not stream using FFmpeg player on Linux due to a lack of a user-agent header. (B#170318)

TCP/IP and General Networking

- Fixed the issue with UDP response traffic sent through incorrect routing path when a static route was expanded. (B#170327, B#170927, SR 2-410201602)
- Fixed the issue where the ProxySG appliance could not join the domain if the SRV response did not contain records for the target hosts. (B#171450, SR 2-425618252, 2-426566482, 2-436499411)

User Documentation

- The Proxy SSL guide demonstrated a method to allow a user to decide whether to proceed to the origin server when the server has a bad certificate. The example policy did not take into account that other policy, which evaluates response data, can override the redirect action. The guide has been updated. (B#169358)

WCCP

- In SkyUI, previous releases only allowed values from 0 to 99 in the WCCP Service groups field. This field has been changed to allow values from 0 to 254. (B#170908)

Known Issues in SGOS 6.3.2.2

At the time of production, Blue Coat knows of the following issues

Access Logging

- Enabling encrypted access logging restarts the ProxySG appliance. Fixed in 6.3.3.1. (B#173107, SR 2-437914572)

ADN

- In a transparent deployment, the ADN load balancer bypasses transparent connections from a branch office because it cannot find a concentrator in its database that supported the address type of the destination address. Fixed in 6.3.3.1. (B#172687)

Authentication

- To join a Windows domain, the current implementation requires delegation, which requires the ProxySG appliance to have administrator credentials. The solution will be changed in subsequent maintenance release so that delegation and administrator credentials are not required. Fixed in 6.3.3.1. (B#173055, SR 2-434595451)
- IWA Direct is not currently supported in a sequence realm as only one IWA direct realm per appliance is supported. This will be resolved in an upcoming release to allow IWA direct in one and only one sequence realm. Fixed in 6.3.3.1. (B#172478, SR 2-438042012)
- After upgrading, the ProxySG appliance experiences high CPU usage every 15 minutes when refreshing LDAP information. Fixed in 6.3.3.1. (B#172753, SR 2-429893505)

Management Console

- After selecting and applying **Enable NTP** on the **Configuration > General > Clock** page and closing the browser, when a new browser session is started the **Enable NTP** checkbox is not selected.

  Although the checkbox is not selected, the **Enable NTP** option is still enabled. Refresh the browser, and the checkbox displays as selected. In the CLI, you can run the command `#show ntp` and verify the status is `NTP is enabled`. Fixed in 6.3.3.1. (B#169934)

ProxyClient

- On a new 6.3.1.1 ProxySG appliance, if the ProxyClient software is upgraded to a later revision, for example 3.4.1.1 or 3.3.2.1, it will download and upgrade the software correctly. But when the Proxy SG appliance is restarted, ProxyClient reverts to the 3.3.1.1 version that was shipped with it. (B#172702, SR 2-422559259)
- Links to download ProxyClient do not work. Fixed in 6.3.3.1.

  Workaround: In your browser, disable TLS v1.0 to download ProxyClient.

  For Internet Explorer:

  a. Open Internet Explorer, click **Tools** > **Internet Options**.

  b. On the **Advanced** tab, and scroll down to the **Security** section.

  c. Find and clear the **Use TLS v1.0** check box.

  d. Click **OK**.

  e. Click the ProxyClient download link through Internet Explorer.

  (B#173027, SR 2-433704900)

SkyUI

- In the **Installed Operating Systems** panel (**System Settings > Software > Operating System**), if a column is resized, the button in the Action column changes from **Restart** to **Downgrade**. If the **Downgrade** button is selected, the ProxySG appliance restarts, but does not perform a downgrade. Fixed in 6.3.3.1. (B#173282)

TCP/IP and General Networking

- Health checks configured with ICMPv6 is not supported. (B#173061, SR 2-435995172)

Section D: SGOS 6.3.1.1, build 78243

Release Date: 11/30/2011, build 78243
BCAAA Version: 130
JRE Version: 1.5.0_15 and later, 1.6 (except 1.6_05)
Compatible with: SGME 6.1.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x

SGOS 6.3.1.1 Contents

See the following sections for information on this release.

New Features in SGOS 6.3.1.1

SGOS 6.3.1.1 introduces the following new features.

IWA Direct

The IWA Direct feature allows you to configure an IWA realm on the ProxySG appliance that connects directly to your Windows Active Directory. Previously, in order to use IWA you had to install and configure BCAAA on a server in your Windows domain. With this new feature, you can join the ProxySG appliance to the Windows domain and then configure the IWA realm to communicate directly with the Domain Controller to process authentication requests.

For More Information

For a detailed description of the feature and its use, refer to the *Blue Coat SGOS 6.3 Administration Guide* (https://bto.bluecoat.com/doc/17321), Integrating ProxySG Authentication with Active Directory Using IWA chapter.

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference* (https://bto.bluecoat.com/doc/17332).

Authentication Realm Validation

A realm validation feature has been added that allows you to test your realm configuration settings from within the ProxySG Management Console to ensure that you can successfully authenticate a user using the settings you provided. This allows you to catch and fix configuration errors immediately. This feature is available for IWA Direct, IWA BCAAA, Windows SSO, Novell SSO, LDAP, and RADIUS realms.

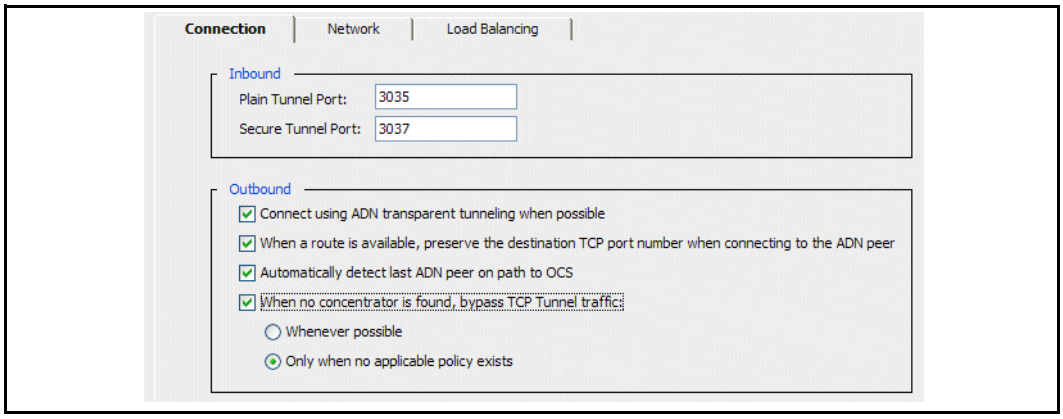
For More Information

For instructions on how perform configuration tests for a realm, refer to the corresponding authentication realm chapter in the *Blue Coat SGOS 6.3 Administration Guide* (https://bto.bluecoat.com/doc/17321).

For CLI syntax, refer to the *SGOS 6.3 Command Line Interface Reference*. (https://bto.bluecoat.com/doc/17330)

Enhanced Performance of TCP Tunnel Proxy

The TCP Tunnel proxy has been enhanced to improve performance and reduce resources on the Branch peer for services that use this proxy. To achieve additional memory savings and CPU resource efficiency on the ProxySG appliance, you can configure the Branch peer to bypass the TCP Tunnel connection if an upstream ADN concentrator is not discovered. This feature—referred to as *bypass-if-no-concentrator*—is automatically enabled on fresh installations of the Acceleration Solution, but is disabled by default on systems upgraded from a pre-6.3 software version. You can toggle this setting from the Advanced Management Console **Configuration > ADN > Tunneling > Connection** tab.



For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide* , Configuring an Application Delivery Network chapter. (https://bto.bluecoat.com/doc/17321)

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference*. (https://bto.bluecoat.com/doc/17332)

Preferred IP Selection for ADN

This new WAN optimization feature promotes optimal data reduction over ADN tunnels, allowing byte caching to occur in situations where previously it could not. Since byte caching requires an ADN control connection between each pair of ADN peers, byte caching cannot occur if the control connection fails to establish. The Preferred IP Selection feature allows you to control the list of available IP addresses to use for the ADN control channel and provides a way to see when the control connection is *not* established. This enables the peers to successfully establish a control connection and participate in byte caching benefits.

In the case of a managed ADN, administrators can now designate preferred IP addresses, effectively excluding management IP addresses that shouldn't be advertised to other peers. In the case of an unmanaged ADN, the preferred IP list can prevent problems caused by the concentrator trying to establish a control connection with the first configured IP address on the arriving interface; the arriving interface may not have any IP addresses configured or the first IP address may be a management IP address.

By default, the list is empty; this means that all IP addresses configured on the ProxySG appliance are eligible to be used for inbound ADN control connections and explicit tunnel connections. Note that this list indicates a *preference* only; if the concentrator gets an inbound ADN control connection on an IP address that is not in the preferred list, that connection is still accepted.

Preferred IP lists are configured in the command line interface:

```
SGOS#(config adn tunnel) preferred-ip-addresses
```

For More Information

For CLI syntax, see the *SGOS 6.3 Command Line Interface Reference*.

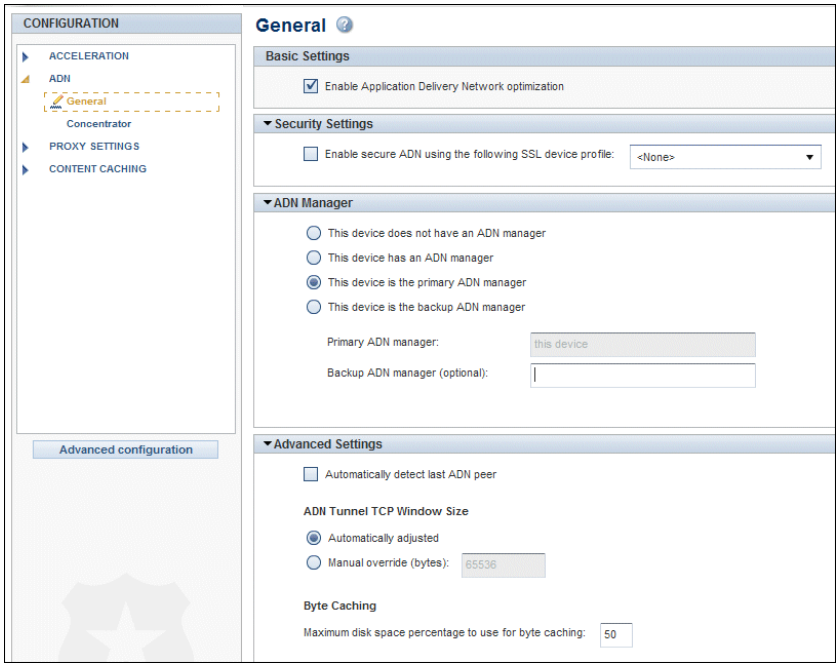
Sky UI Enhancements

The following enhancements were added to Blue Coat Sky UI.

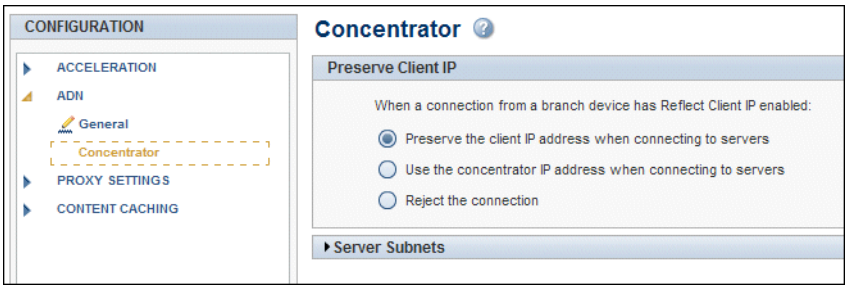
- "ADN Configuration" on page 24
- "SSL Proxy Configuration" on page 24
- "Auto Refresh of Reports" on page 25
- "Email Sysinfo" on page 25

ADN Configuration

The Sky UI includes two new panels for configuring the application delivery network (ADN). In the General panel, you can enable ADN, set up a secure ADN, configure a managed network, and modify advanced settings.

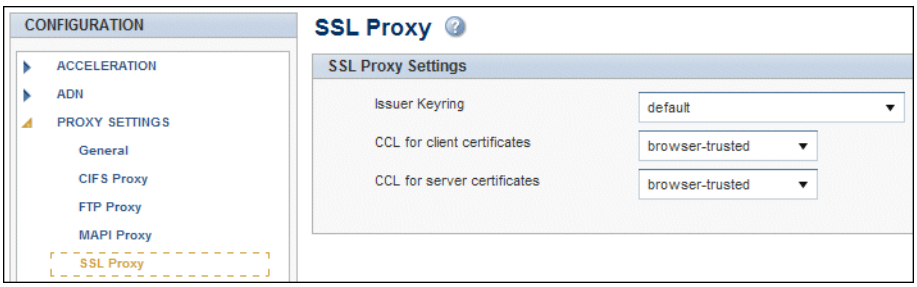


If you are configuring the Concentrator peer, you can specify whether you want the client IP preserved when connecting to servers. Additionally, if the Concentrator peer is deployed out-of-path, you can configure server subnets to advertise.



SSL Proxy Configuration

A new panel for configuring the SSL proxy is included in the Sky UI.

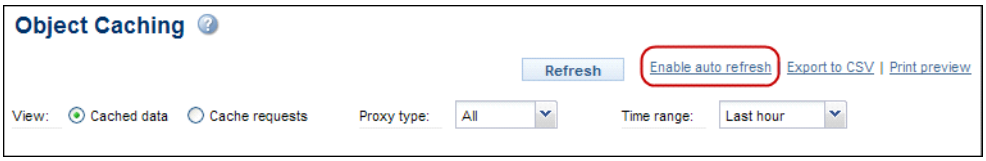


Note that to create certificates or keyrings, you must use the CLI or Advanced Management Console.

Auto Refresh of Reports

You can turn on auto refresh for the following reports:

- Traffic Summary
- Bandwidth Savings
- Object Caching
- Connection History



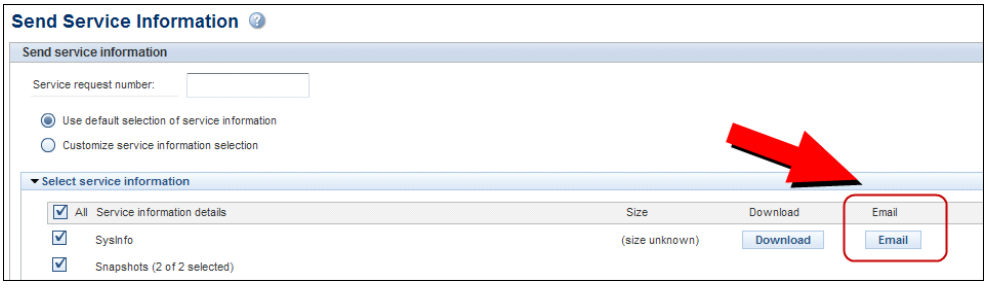
Auto refresh is disabled by default. When you click **Enable auto refresh**, the report is automatically refreshed at regular intervals while it is displayed on the screen. The refresh interval depends on the report time range.

Time Range on Report	Refresh Interval
Last 5 minutes	10 seconds
Last hour	60 seconds
Last 24 hours	15 minutes
Last 7 days	6 hours
Last 30 days	1 day

Auto refresh is enabled only while the report is displayed onscreen. When you go to another report or another screen in the UI, auto-refresh is no longer activated.

Email Sysinfo

The Send Service Information panel (**System Settings > Troubleshooting > Send Service Information**) includes a new button that allows you to email the sysinfo file (sysinfo.txt) as an attachment to any email address (not just Blue Coat Support). You can specify multiple recipients.



Note that this feature requires that you have configured a mail server on your ProxySG appliance. To verify that your ProxySG appliance has an SMTP gateway configured, use the following CLI commands:

```
#(config) smtp
#(config smtp) view
```

If no gateway is configured, use the following CLI command:

```
#(config smtp) server domainname | ip-address [port]
```

Alternatively, you can go to the Advanced Management Console and choose **Maintenance > Event Logging > Mail**.

For More Information

See the *Blue Coat Sky v6.3.x Release Notes*.

You can also click the help icon  in Blue Coat Sky for context-sensitive help on any of the reports or panels.

Search for the feature in the Acceleration WebGuide:

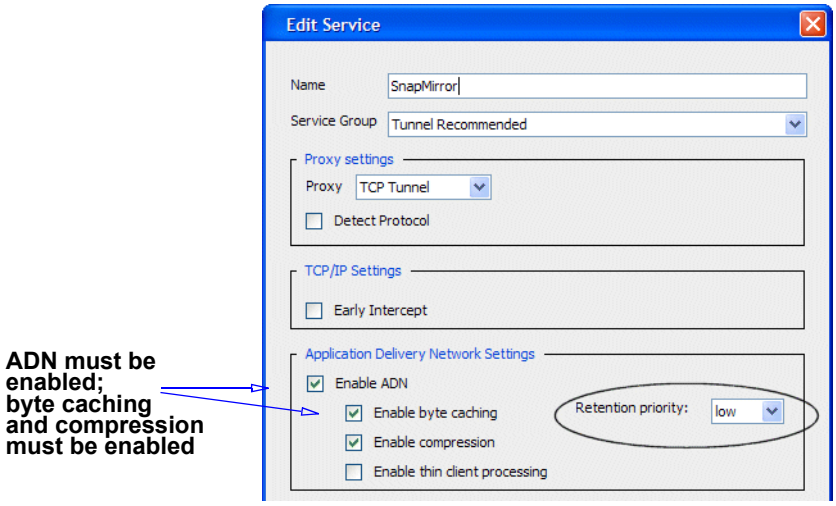
https://bto.bluecoat.com/sgos/ProxySG/63/Acceleration_WebGuide/Acceleration_WebGuide.htm

Byte-Cache Retention Policy

You can control how long data is stored in the byte cache dictionary by assigning a *retention priority* to a particular service. If you want to keep certain types of data in the dictionary for as long as possible, set a **high** retention priority for the service. For data that changes frequently and where the byte caching efficacy decreases over time, you can set a **low** retention priority for the related service. Most services are set to **normal** priority by default.

A fresh installation of SGOS 6.3 will have the following services marked as low retention priority: External HTTP, SnapMirror, Double Take, iSCSI, CommVault, FCIP and SRDF. All other non-thin-client services are normal priority. Systems that are upgraded to SGOS 6.3 will have normal retention priority set for all services.

When creating or editing a service in the Advanced Management Console, you can set the retention priority to **low**, **normal**, or **high**.



For More Information

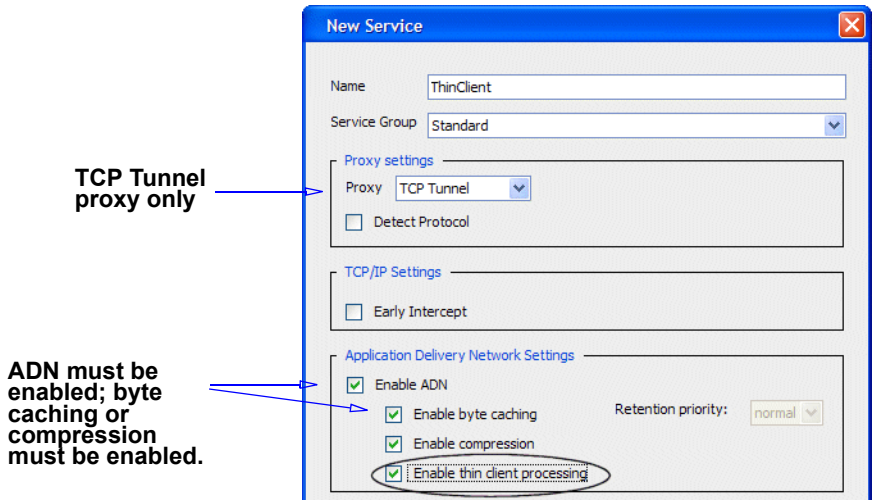
For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing Proxy Services chapter. (https://bto.bluecoat.com/doc/17321)

Thin Client Processing

Applies special treatment to application traffic from thin client applications and virtual desktop infrastructure environments such as RDP, VNC, Citrix, and VDI. This processing improves responsiveness of thin client actions. For example, end-users will notice that the desktop displays significantly faster. In addition, thin client data is not retained in the byte cache as long as other types of data because this data is temporal in nature; the byte cache, therefore, can be used more efficiently for other types of traffic where byte cache matches can span longer time intervals.

A fresh installation of SGOS 6.3 will have the following services marked for thin client processing: MS Terminal Services, VNC, Citrix, and X-Windows; however, none will be marked for interception. Systems that are upgraded to SGOS 6.3 will not have thin client processing enabled for any services; this configuration must be done manually.

When using the Advanced Management Console to create or edit a service that uses the TCP Tunnel proxy, you can enable thin client processing.



For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing Proxy Services chapter. (https://bto.bluecoat.com/doc/17321)

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference*. (https://bto.bluecoat.com/doc/17332)

Web Application Control

The application control feature in SGOS 6.3 provides two new destination objects in the Web Access Layer—**Request URL Application** and **Request URL Operation**—that allow for more granular control over access to WEB 2.0 applications within your network. The ProxySG appliance can currently identify over 90 Web applications—including Facebook, Twitter, Netflix, Gmail, Amazon, and Google Search—and this list is growing every day. For a current list, go to http://www.bluecoat.com/security/web-application-controls.

The application control feature has the following requirements:

- A Proxy Edition license (not a MACH5 license) must be installed.
- The Blue Coat WebFilter (BCWF) feature must be enabled. (**Configuration > Content Filtering > General**)
- The full BCWF database must be downloaded. The applications and operations lists will be blank if BCWF is not enabled and available for use. (**Configuration > Content Filtering > Blue Coat WebFilter**)
- The ProxySG appliance must have one or more Web services, such as External HTTP and HTTPS, set to intercept. Bypassed Web traffic is not classified into applications.

The following new Web 2.0 policy control objects were added in this release:

- **Request URL Application**: The **Request URL Application** object gives you the ability to block popular Web applications such as Facebook, Linkedin, or Pandora. As new applications emerge or existing applications evolve, BCWF tracks the domains that these Web applications use to serve content, and provides periodic updates to include the new domains that are added. You can use the **Request URL Application** object to block an application and all the associated domains automatically.

  For the applications you have blocked, you do not have to update your policy to continue blocking the new content sources; To block newly recognized applications, you will need to select the new applications and refresh your network policy.

- **Request URL Operation**: The **Request URL Operation** object restricts the actions a user can perform on a Web application. For instance, when you select the **Upload Picture** action for the **Request URL Operation**, you create a single rule that blocks the action of uploading pictures to any of the applications or services where the action can be performed such as Flickr, Picasa, or Smugmug.

  When you block by operation, unlike blocking by application, you prevent users in your network from performing the specified operation for all applications that support that operation. They can however, access the application itself.

  Note, however, that the Request URL operation object only pertains to operations for sites that BCWF recognizes as Web applications. So, blocking picture uploads would not prevent users in your network from using FTP to upload a JPEG file to an FTP server, or from using an HTTP POST to upload a picture on a Web site running bulletin board software.

For More Information

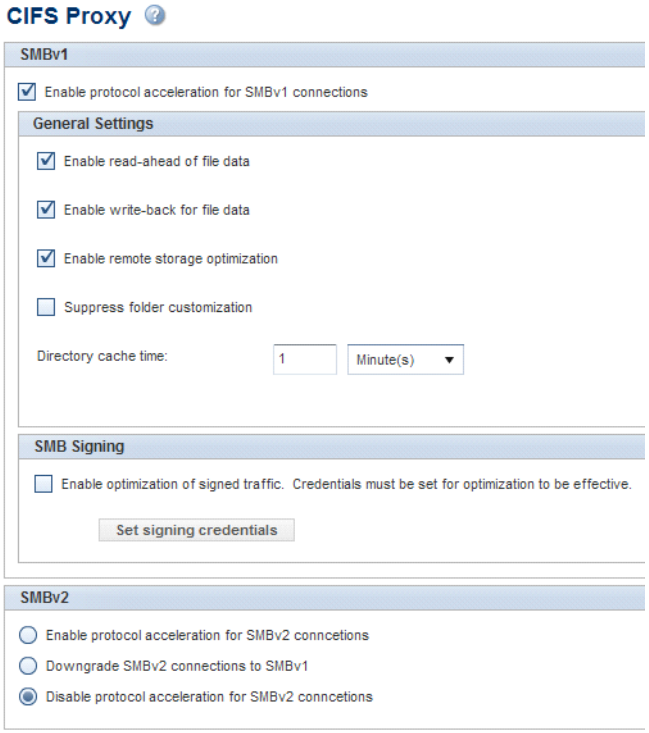
For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Filtering Web Content chapter. (https://bto.bluecoat.com/doc/17321)

SMBv2 Support in the CIFS Proxy

With the SMBv2 support added in SGOS 6.3, the CIFS proxy permits connections to negotiate SMBv2 rather than forcing them to downgrade to SMBv1. SMBv2 connections can be accelerated with byte caching, compression, and object caching; SMBv1 and SMBv2 share a common object cache. The CIFS proxy supports many SMBv2 protocol enhancements including data pipelining, request compounding, larger reads and writes, improved scalability for file sharing, durable opens during temporary loss of network connectivity, and the leasing mechanism for caching.

When upgrading from a previous SGOS release, SMBv1 and SMBv2 acceleration will be enabled by default. SMBv2 support in an ADN deployment requires both the branch and concentrator peers to be running SGOS 6.3 or higher. If they aren't, SMBv2 connections are downgraded to SMBv1. Keep in mind that protocol optimization cannot be applied to SMBv2 connections that require messages to be signed.

The CIFS Proxy page in Blue Coat Sky has a new section for SMBv2 configuration.



For More Information

See the *Blue Coat Sky v6.3.x Release Notes*.

You can also click the help icon in Blue Coat Sky for context-sensitive help on any of the reports or panels.

See "Configure the CIFS Proxy" in the Acceleration WebGuide:

https://bto.bluecoat.com/sgos/ProxySG/63/Acceleration_WebGuide/Content/02Tasks/Traffic_Management/configure_cifs_proxy_settings_ta.htm

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference*. (https://bto.bluecoat.com/doc/17332)

Acceleration of Encrypted Flash Traffic

The Flash proxy is now able to process encrypted protocols (RTMPE and RTMPTE), allowing this traffic to take full advantage of the ProxySG appliance's object caching and protocol-specific optimizations. The proxy decrypts incoming encrypted Flash data, accelerates the connection, and then re-encrypts the outgoing data. In previous SGOS versions, the encrypted Flash traffic was tunneled. Note that encrypted and plain content are stored separately in the object cache.

If your ProxySG appliance is already set up to accelerate Flash traffic, no additional configuration is necessary. Just verify the following service configuration:

- **Transparent deployment** You need to have an RTMP proxy service configured to listen on port 1935 (the typical RTMP port), and this service must be set to intercept. This service controls RTMP and RTMPE traffic.
- **Explicit deployment** You should have an Explicit HTTP proxy service configured to listen on ports 8080 and 80, and this service must be set to intercept. This service controls plain and encrypted Flash connections tunneled over HTTP.

In addition, a new CPL property was added to let you control whether encrypted Flash traffic is tunneled or accelerated. By default, RTMPE and RTMPTE traffic is not tunneled; incoming data is decrypted, the connections are accelerated, and the outgoing data is encrypted. Because encryption is CPU intensive, you might want to write policy to turn it off. Or, if there are issues with accessing a specific site, you can write policy to tunnel the encrypted RTMP traffic to that site. If a connection is tunneled due to this type of policy, the Active Sessions Detail column will show **Encrypted, tunneled by policy.**

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Content Policy Language Reference*. (https://bto.bluecoat.com/doc/17317)

Force Cache Policy

Previous versions of SGOS offered a force_cache policy that forced the caching of HTTP responses that would otherwise be considered uncacheable because the response header contained a reason (such as "`set-cookie`" or "`private`") that caused it not to be cached. However, this policy was all or nothing: you couldn't specify a particular reason for forcing the caching. The force cache policy has been enhanced in 6.3.1 to allow caching to be forced for a specific reason or reasons. Nine different reasons are supported, as listed in Table 1 below. The HTTP proxy supports all nine reasons, while streaming proxies have limited support, as indicated in the table.

You can define the force cache policy in content policy language (CPL) or in the Visual Policy Manager (VPM).

Table 1: Force Cache Reasons

Reason (VPM)	Reason (CPL)	Details
Missing HTTP version in the response	`missing-http-version`	The first line of the HTTP response does not contain "HTTP/" at the beginning, so the ProxySG appliance does not know the protocol/version. Not supported on streaming proxies.

Table 1: Force Cache Reasons (Continued)

Reason (VPM)	Reason (CPL)	Details
'No-cache' & 'Pragma: no-cache' response header	`response-no-cache`	Includes both `Cache-Control: no-cache` and `Pragma: no-cache` response header/meta tag. Supported on Windows Media over RTSP or HTTP and RealMedia over RTSP or HTTP.
'No store' response header	`response-no-store`	Refers to the `Cache-Control: no-store` response header/meta tag. Supported on Windows Media over RTSP or HTTP, but not on RealMedia over RTSP or HTTP.
'Private' response header	`private`	Refers to the `Cache-Control: private` response header/meta tag. Supported on Windows Media over RTSP or HTTP, but not on RealMedia over RTSP or HTTP.
'Set-Cookie' response header	`set-cookie`	Includes both `Set-Cookie` and `Set-Cookie2` response headers. Not supported on streaming proxies.
'Vary' response header	`vary`	Refers to the `vary` response header. Not supported on streaming proxies.
'Expires' response header with a date in the past	`expired`	The HTTP response has `Expires` header and its value is in the past. Not supported on streaming proxies.

Table 1: Force Cache Reasons (Continued)

Reason (VPM)	Reason (CPL)	Details
'Unknown Transfer-Encoding' response header	`unknown-transfer-encoding`	The `Transfer-Encoding` response header value is unknown. Not supported on streaming proxies.
Personal pages	`personal-pages`	For advanced users or support only. The ProxySG appliance looks for a non-304, non-image type N response first, and then checks to see if it has either a query string or a `Cookie` header in the request. If either a query string or `Cookie` request header is present, the ProxySG appliance makes it non-cacheable, but the `force_cache(personal-pages)` property can override it. Not supported on streaming proxies.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Content Policy Language Reference*. (https://bto.bluecoat.com/doc/17317)

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference*. (https://bto.bluecoat.com/doc/17332)

Client Certificate Authentication

Sometimes, when a user navigates to a secured web address in a browser, the server hosting the site requests a certificate to authenticate the user. The client certificate authentication feature allows the ProxySG appliance to store client certificates and present the appropriate certificate to the Web server upon request.

The ProxySG appliance stores individual client certificates and keys in individual keyrings. You can then write policy that instructs the appliance which client certificate to use, and when to use it.

For convenience, you can also group client certificates and keyrings into a keylist that contains all of the client certificates for a specific purpose, such as certificates for a specific website or certificates for users in a particular group. If your policy

references a keylist rather than an individual keyring, you must specify how to determine which certificate to use. This is done by matching the value of a substitution variable defined in the policy against a specified certificate field attribute value within the certificate. The ProxySG appliance determines what certificate field attribute to use based on an extractor string you supply when you create the keylist.

When a certificate is requested, if the policy selects a client certificate, the appliance presents the certificate to the requesting server. If no certificate is specified in policy, an empty certificate is presented.

Note: This feature is only applicable to intercepted SSL traffic.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing X.509 Certificates chapter. (https://bto.bluecoat.com/doc/17321)

Downloadable CA List

When a client sends an HTTPS request to an OCS, the OCS presents its certificate to the browser. The browser then validates the certificate using the corresponding CA certificate in its list of trusted CAs (if it has one, otherwise it will present a trust dialog to the user). When the ProxySG appliance intercepts an HTTPS connection, it terminates the client request and then initiates a new request to the OCS, posing as the client. Therefore, the ProxySG appliance must also have an up-to-date list of trusted CA certificates to enable the certificate validation process. The ProxySG appliance uses its built-in `browser-trusted` CA Certificate List (CCL) for this purpose.

In previous SGOS versions, the ProxySG appliance's list of browser-trusted CAs was only automatically updated upon SGOS upgrade. If you wanted to add additional trusted CA certificates between upgrades, you had to manually update the list on each appliance in your network. However, with the Downloadable CA List feature, the appliance will now automatically download an updated `browser-trusted` list of CAs every seven days by default. This smart download compares the existing `browser-trusted` list on the appliance to the new list only modifies CA certificates that are have been added or deleted since the last update. Any manual changes that you have made to the file are preserved. The updates, which include both an updated `browser-trusted` CCL as well as the corresponding CA certificates, are packaged in a file called a *trust package* (`trust_package.bctp`), which is signed by the Blue Coat CA and will be validated before the ProxySG appliance will install it. You can also configure the download behavior, changing the download location or schedule. You can also choose to use manual download only.

Note: The `trust_package.bctp` trust package may also contain updates to the `image-validation` CCL and its associated CA certificates. This CCL is used to validate signed SGOS images.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing X.509 Certificates chapter. (https://bto.bluecoat.com/doc/17321)

Preserve Untrusted Certificate Issuer

Before SGOS 6.3, if a website presented a certificate to the ProxySG appliance that was not signed by a trusted certificate authority (CA), the ProxySG appliance could either send an error message to the user, or ignore the error and continue to process the request. The ProxySG appliance did not allow the user's browser to display the certificate information and let the user accept the security risks and continue with the SSL handshake.

In SGOS 6.3, the Preserve Untrusted Certificate Issuer feature has been added to allow the ProxySG appliance to present the browser with a certificate that is signed by its untrusted issuer keyring. The browser displays certificate information to the user, and lets the user accept the security risk of an untrusted certificate and proceed to the website.

The `default-untrusted` keyring has been added to the ProxySG appliance to use with the Preserve Untrusted Certificate Issuer feature. The `default-untrusted` keyring should not be added to any trusted CA lists.

Note: This feature only applies to SSL forward proxy transactions with HTTPS interception enabled.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing the SSL Proxy chapter. (https://bto.bluecoat.com/doc/17321)

SSL Intercept Based on Authentication Credentials

The SSL intercept based on authentication credentials feature extends policy to allow you to select which SSL transactions to intercept based on username and/or group membership. Previously, you could only make user-based intercept decisions on HTTP traffic. With this new feature, conditions are available in the SSL Intercept layer for creating policy that allows you to make SSL intercept decisions based on authentication credentials.

For example you can:

- Intercept all SSL traffic except traffic from a specific user, such as the CEO or CFO.
- Intercept all SSL traffic except traffic from users who belong to a specific user group, such as finance.

SSL intercept is a resource-intensive operation. This feature provides the administrator more granular control for bypassing SSL traffic that does not need to be monitored by extending the SSL intercept policy conditions to include user and group-based rules.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, Managing the SSL Proxy chapter (https://bto.bluecoat.com/doc/17321), the *Blue Coat SGOS 6.3 Visual Policy Manager Reference* (https://bto.bluecoat.com/doc/17329), or the *Blue Coat SGOS 6.3 Content Policy Language Reference* (https://bto.bluecoat.com/doc/17317).

HTTP Application Traffic Category Reporting

The application reporting feature gives you visibility into which Web applications users are accessing on the network, the amount of bandwidth these applications are consuming, and how much bandwidth is gained by optimization of applications over different time periods. The ProxySG appliance can currently identify over 90 Web applications—including Facebook, Twitter, Netflix, Gmail, Amazon, and Google Search—and this list is growing every day. For a current list, go to http://www.bluecoat.com/security/web-application-controls.

Two different application-based reports are available:

- **Application Mix**—provides graphs and statistics about the top Web applications on the network. See "Application Mix Report" on page 36.
- **Application History**—provides details for a selected Web application. See "Application History Report" on page 38.

Application reporting has the following requirements:

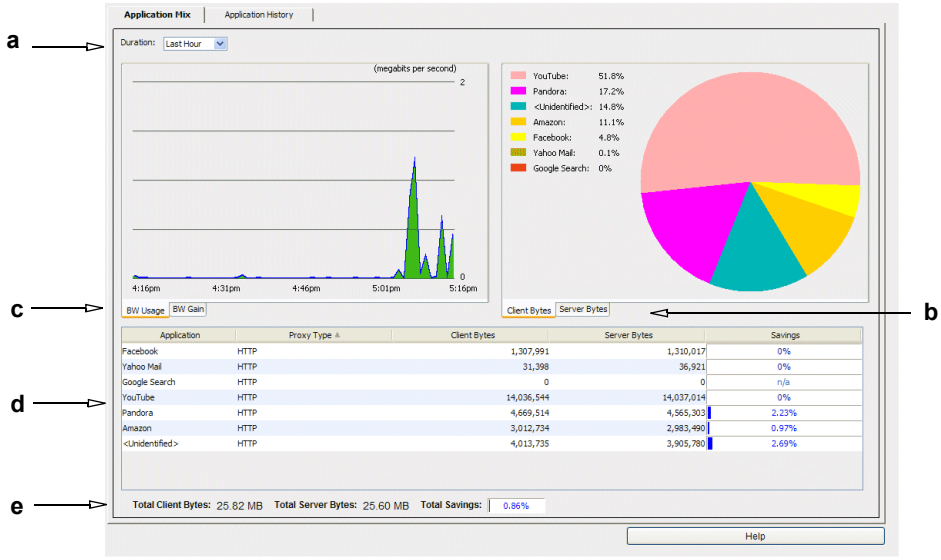
- Proxy Edition license (not a MACH5 license)
- The Blue Coat WebFilter feature must be enabled. (**Configuration > Content Filtering > General**)
- A current BCWF database must be downloaded to the ProxySG appliance. (**Configuration > Content Filtering > Blue Coat WebFilter**)
- The ProxySG appliance must have one or more Web services, such as External HTTP and HTTPS, set to intercept. Bypassed Web traffic is not classified into applications.

Application Mix Report

The Application Mix report shows a breakdown of the Web applications running on the network. This report can give you visibility into which Web applications users are accessing, the amount of bandwidth these applications are consuming, and how much bandwidth is gained by optimization of Web applications over different time periods.

The report has three parts to it:

- Line graph showing aggregated bandwidth usage or gain
- Pie graph showing client/server byte distribution of Web applications
- Statistical table listing client/server bytes and savings for each Web application.



Key

a: Modify the reporting time period.

b: View client- or server byte-distribution charts and statistics.

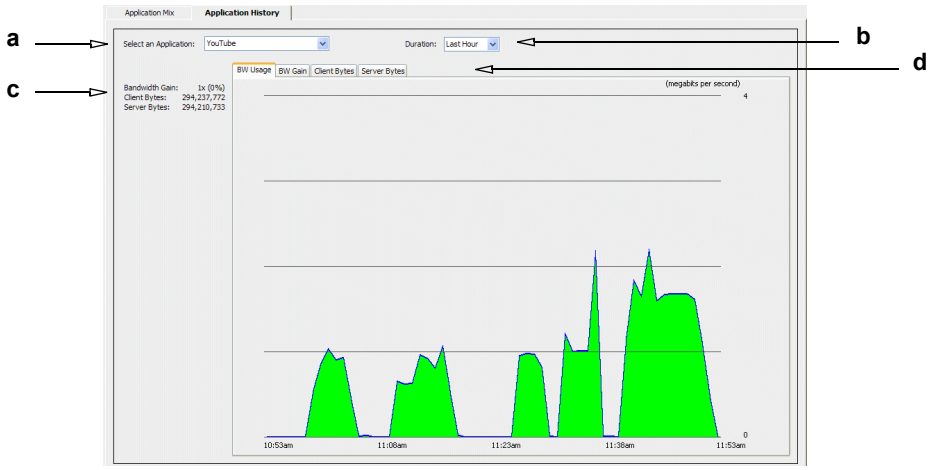
c: View aggregated bandwidth usage or gain graphs.

d: Review client bytes, server bytes, and bandwidth savings.

e: Review totals for client bytes, server bytes, and total savings.

Application History Report

The Application History report shows historical data about Web applications; you can select a particular Web application and then view its bandwidth usage, gain, client bytes, and server bytes over different time periods.



Key:

a: View statistics for a particular Web application.

b: Modify the historical reporting period.

c: View totals for client and server bytes and the average bandwidth gain for the selected application.

d: Display charts for bandwidth usage, bandwidth gain, client bytes, and server bytes.

For More Information

For details, refer to the *Blue Coat SGOS 6.3 Administration Guide*, the Statistics chapter. (https://bto.bluecoat.com/doc/17321)

For upgrading and downgrading impacts related to this feature, refer to the *SGOS 6.3 Upgrade/Downgrade Feature Change Reference*. (https://bto.bluecoat.com/doc/17332)

Security Advisories

To see if there are any Security Advisories that apply to the version of SGOS you are running, go to:

https://kb.bluecoat.com/index?page=content&channel=SECURITY_ALERTS

New advisories are published as security vulnerabilities are discovered and fixed.

Resolved Issues in SGOS 6.3.1.1

This release incorporates the bug fixes from SGOS 6.2.5.1, 6.1.5.2, 5.5.7.1, and 5.4.9.1.

The following issues, reported in previous SGOS versions, have also been fixed in SGOS 6.3.1.1.

ADN

- ADN is now able to retrieve device IDs when IPv6 addresses are used for ADN managers. (B#167610, SR# 2-403799863)
- IPv6 configurations for ADN Primary Manager IP, Backup Manager IP and External VIP configuration now display in `show configuration` output. (B#167611, SR# 2-405592881)
- The amount of memory reserved for ADN management for 210, 300-5/10, 810-5 and 9000-10 platforms has been reduced to minimize the risk of memory regulation. (B#165749).

Authentication

- ProxySG appliances configured with BCAAA Siteminder Agent no longer insert incorrect characters (? instead of &) when constructing the URL for the authentication page. (B#159025)
- The ProxySG appliance no longer restarts at `0x810002 in Process: "LDAP Authorization Refresh Worker"` if an LDAP realm is being removed while its authorization is actively computed. (B#167445, SR# 2-405127884)

CIFS Proxy

- When remote storage optimization is disabled, the ProxySG appliance is now able to mark files as being “offline”. (B#162740, SR 2-382911032)

CLI Consoles

- SSH Host and client keys are now retained when upgrading from SGOS 5.5.3.1/5.5.4.1 to SGOS 6.x, which prevents proxies from becoming disconnected from Director. (B#159104, SR 2-369527507)

Client Manager

- Archived configurations from a Mach5 licensed system no longer contain commands that prevent the configuration from being reloaded onto the ProxySG appliance. (B#168198 SR#2-397650476)

FTP Proxy

- In transparent deployments, the ProxySG appliance now processes extended passive FTP commands (EPSV, EPRT, PORT, and so on) successfully with default settings. (B#165258, SR# 2-393744502)
- While going through the FTP Proxy, users are no longer denied access when trying to access an FTP server that requires a 100 character password. (B#168074, SR#2-406735244)

Kernel

- The rare internal kernel error that caused the ProxySG appliance to restart because of a page fault at `0x483fff020 in processgroup "PG_OBJECT_STORE" in Process: "CEA Cache Administrator"` has been fixed. (B#160239, SR# 2-39047362)

SNMP

- MIB files have been fixed sot that they are now RFC-compliant regarding capitalization. (B#167441)

SSL

- The ProxySG appliance no longer restarts due to a race condition occurring when two users access the same website and one is tunneled and the other is intercepted. (B#167414, SR#2-392837381, SR#2-408427372)

TCP/IP and General Networking

- You can no longer install an invalid netmask into the static route table with the `inline static-route-add` command. (B#166768)
- The ProxySG appliance no longer sends IPv6 DNS queries after setting an IPv4-only policy. (B#166802)

VPM

- The URL Application Name (or operation) VPM object dialog Select All functionality has been redesigned to be more intuitive. (B#165731)

Windows Media Proxy

- Media Streams played through Microsoft Silverlight plug-in no longer fail to play.(B#168212, SR 2-390134973)

Known Issues in SGOS 6.3.1.1

At the time of production, Blue Coat knows of the following issues.

ADN

- A Branch peer running a release prior to SGOS 5.5.4 will not be able to form transparent tunnels with a Concentrator peer running SGOS 6.2 (or above). The Branch peer must be running SGOS 5.5.4 or higher.
- If you configure an ADN node as Primary ADN Manager and then later configure the node for secure ADN by selecting a device profile, the appliance will no longer be able to locate the ADN manager, displaying the **Primary Manager ID not set** error (even though the **Primary ADN Manager** setting is still set to **Self**). To work around this issue, reset the **Primary ADN Manager** setting to **None** and **Apply** the change. You can then set the **Primary ADN Manager** setting back to **Self** and apply the device profile successfully. Fixed in 6.3.2.2. (B#169320)
- If your PacketShaper plug-in is not up-to-date, ADN traffic will be classified as `ProxySG-ADN/Default`. To solve this issue, install the new PacketShaper plug-in (**Blue Coat ProxySG v1.3.0**), which can be downloaded from the appropriate **PLUG INS** link on the PacketShaper Download page on BlueTouch Online: https://bto.bluecoat.com/download/product/32.

  After installing the new plug-in, ADN traffic will be classified as `ProxySG` (Blue Coat ProxySG Appliance Control traffic), `ProxySG-ADN` (Blue Coat ProxySG Appliance Tunnel traffic), or `ProxySG-Management` (ProxySG Management Console Traffic).

Authentication

- Session Monitor entries will always show an expiry time of "Never Expire" when viewed from the /Bin/System-Bins/Entries/_Session_Bin URL. However, the configured expiration time will still be enforced. (B#142321)
- On rare occasions, the Domain Controller will reset a TCP connection due to network issues. If this occurs during a domain join, it may cause the domain join to fail with "%ERROR_GEN_FAILURE" or "NETNAME_DELETED". If you see one of these errors, check the network and the Domain Controller for issues and then try joining the appliance to the domain. (B#167410)
- If you join the ProxySG appliance to a Windows Active Directory domain and then later leave the domain, the appliance's machine account in Active Directory does not get disabled automatically. You must manually disable the machine account in your Active Directory. Make sure that if you assigned a Kerberos SPN to this account that you also remove the SPN using the `setspn -D <SPN>` command. (B#167886)
- When joining a Windows Active Directory domain, the ProxySG appliance does not check to see if another ProxySG appliance with the same machine name is already joined to the domain. Because a password is automatically created for the machine account upon joining the domain, if two appliances are joined to the domain using the same machine name, the first appliance joined will no longer be able to access the Active Directory because it will no

longer have the correct password. To prevent this problem, make sure you use a unique machine account name for each ProxySG appliance that you join to your Windows domain. Note that because the ProxySG appliance also periodically changes its machine account password, if you were to reload a configuration using an old sysinfo file, you could run into the same issue with the appliance having an incorrect password. To workaround this issue, leave and re-join the domain (using a unique machine account name) to reinitialize the machine account password. (B#170283)

- To ensure that IWA uses the Kerberos protocol rather than downgrading to NTLM, the DNS name that you use for Kerberos authentication must be unique. With IWA Direct, create a DNS "A" record that resolves to the DNS name of the appliance's Active Directory machine account name. For IWA BCAAA, create a DNS "A" record that resolves to the appliance's FQDN. Keep in mind that the DNS name you choose must not match the Active Directory machine account name for the appliance. For example, rather than using the machine name, you might create a DNS entry for the appliance using a name such as bcaaaUser1. (B#167368)
- On Windows 2008, when debug logging has been enabled in BCAAA, BCAAA may write the following error to its debug logs:

  ```
  A call to setsockopt for BCAAA server socket returned error: 0x273a.
  This may not indicate a problem, and BCAAA will continue initialization
  as normal.
  ```

  The error is benign and can be ignored. It does not indicate a problem. (B#135400)

Boot

- Upgrade from a previous FIPS release fails under specific upgrade paths. If your appliance was manufactured with SGOS 6.1.3.1 and you upgraded to a signed 6.1.3.1 build and enabled FIPS, you cannot directly upgrade to 6.3.x. In this case you must upgrade to 6.1.5.1 before upgrading to 6.3.x. (B#168519)

Cache Engine

- Running the **`disk decrease-object-limit`** or **`decrease-object-limit`** CLI commands while traffic is passing through the system causes the appliance to reboot; this command should be executed on an idle system only. (B#165555)

CIFS Proxy

- Using a Windows 2008 server that does not have SMB signing enabled and uses ABE based permissions may cause issues with CIFS directory caching. (B#166062, SR#2-388049254)
- The `show cifs` CLI command does not work if the URL contains spaces, even when the URL is enclosed in quotation marks. The workaround is to replace any spaces with `%20`. (B#155626)

Client Manager

- If you change the name of an existing category using the **ProxyClient > Web Filtering > Policy > Edit Categories** dialog, the change will not be properly reflected in the **Categories/User-Group** list on the **Configuration > ProxyClient > Policy** tab. (B#94653)
- When downgrading SGOS 6.3.x to an earlier version, the installed ProxyClient version is not preserved. (B#156326)

DNS Proxy

- When you configure a DNS server using IPv6 link-local address, the ProxySG appliance does not accept DNS responses. (B#158905)

Encrypted MAPI

Encrypted MAPI acceleration on the ProxySG appliance has the following limitations:

- Encrypted and plain MAPI traffic may be bypassed if 64-bit Exchange enterprise and Outlook clients are used. (B#156424)
- Outlook users must belong to the same domain as the Exchange server and the ProxySG appliance. Multi-domain support is not available in this release. (B#158870)
- Outlook establishes NTLM connections with Exchange Server over Load Balanced Client Access Array solutions. NTLM connections are tunneled by the ProxySG appliance. Workaround: enable Kerberos support for Load Balanced solutions. (B#155098)

Flash Proxy

- When streaming video from a site that uses dynamic chunk size changes, caching is invalidated. This causes playback of these streams to fail when caching is enabled. Fixed in 6.3.2.2.

  Workaround: Install the `bypass_cache(yes)` policy for the site on the ProxySG appliance.

  (B#169784, 170210)
- Videos that contain zero audio frames may not cache properly and playback may end prematurely. (B#156485)
- In a proxy chaining deployment, cached Hulu streams may intermittently stop for a short time towards the end of the stream and then resume after a few seconds. (B#168454)
- When streaming live radio from certain sites (such as streema.com), streams will sometimes fail to play when the stream is connected through RTMP instead of through RTMPE. As a workaround, try reloading the page. (B#168495)

- Dynamic streaming (play2) may cause video playback to stop in heavily bandwidth-constrained environments when a hierarchy of ProxySG appliances are caching the video. (B#156892, #156896)
- For Flash video clients that use pauses while seeking, such as Yahoo video, a ProxySG appliance may not be able to cache content or play content from cache after a seek. Fixed in 6.3.2.2. (B#156268)
- For some Flash client/server application combinations, playback may freeze after doing a seek. To work around this problem, simply perform another seek and playback should resume. Fixed in 6.3.2.2. (B#157785)
- Advanced functionality, such as stream publishing, may not work optimally through the ProxySG appliance.
- When playing a multi-bitrate dynamic live stream from certain sites the playback may freeze.As a workaround, create a `bypass_cache(yes)` policy for the site. (B#158036)
- There may be problems caching certain video files delivered via Flash Media Server 3.0. The workaround is to use `bypass_cache(yes)` policy to prevent caching these videos. (B#158954)
- If the Flash Media Server returns two different onMetaData messages for the same VOD stream, the ProxySG appliance will bypass the stream and invalidate any content cached up to that point. (B#165916, SR#2-396906692)

HTTP Proxy

- When authenticating transparent HTTPS traffic using an IWA Direct realm, BASIC requests are not restricted to secure virtual URLs. To prevent security breaches, make sure you configure secure virtual URLs for your HTTPS traffic. (B#167309)
- If an object has a `last-modified-time` close to the current time and the ProxySG appliance is configured with `http strict-expiration serve`, the ProxySG appliance will serve the cached object even though it may be stale. (B#154956)
- Changes in the HTTP maximum connection limit due to a change in licensing do not take effect until after the new license is installed and the appliance is rebooted. (B#153815)
- In some cases, if a site uses two different hosts to serve data, downloads may fail if pipelining is enabled. To work around this issue, disable pipelining on the domain using the `pipeline(no)` policy.(B#149274)
- There is an issue downloading some YouTube objects via the ProxySG appliance onto an iPhone. The workaround for this issue is to disable client side persistence. For more information, refer to FAQ 279 in the Blue Coat Knowledge Base (https://kb.bluecoat.com/index?page=content&id=FAQ279) (B#155291)

- When writing a policy to block a host found in an HTTP request, some requests may not be blocked if Trust Destination IP is also enabled. A workaround is to use the resolved IP address for the host you want to block. (B#154935)
- When using WebFTP through the ProxySG appliance using a transparent setup with reflect client IP, FTP communications in active mode will not complete.
  Workaround: Use passive mode or disable reflect client IP. (B#145300, 153162)
- When accessing the advanced URL for the HTTP debug log and trying to delete an ICAP service, sometimes the service is not deleted. Please retry after the debug log has been downloaded fully from the browser. (B#147373, 153163)
- When the Clientless Limits feature is enabled, and many clientless requests are in a deferred status, disabling the limit configuration might cause the ProxySG appliance to restart. To prevent this issue, do not disable the limits when more than one thousand request are deferred. (B#143016)
- Exception pages do not work on HTTP CONNECT when using Firefox 3.0.10 or later or IE 8 or later unless SSL intercept (on exception) is enabled. (B#166795)

ICAP

- With ICAP and Patience pages both configured, the Save As dialog will not display upon file download with IE-8.0.6001.18702 and IE 7.0.5730.13. Blue Coat recommends using trickling. (B#151088, 153164)

Management Console

- The **Savings** column on the **Statistics > Application Details > Application Mix** and the **Statistics > Traffic Details > Traffic Mix** tabs does not sort properly, and any N/A entries remain at the bottom of the list. Sorting works correctly for all other columns. (B#170944)
- When using the **Statistics > Authentication > User Logins** tab to search for logged in users, you cannot use the / or \ characters in your search because the Management Console does not properly URL encode the URLs it generates from this tab. For example, a search for MY-AUTH-REALM* would not yield any results, whereas MY-AUTH-REALM* would. (B#167279)
- When accessing the Management Console from a system running the Windows 7 Ultimate SP1 32-bit OS, the **Services > Proxy Services** tab shows the **Predefined Service Groups** and **Default Action** services only; other services are not displayed. (B#170443)

MAPI Proxy

- Endpoint Mapper does not restrict source IP for secondary MAPI connection interception. Workaround: add the IP address to the static bypass list. (B#154100)

Platform-Specific

SG210-5

- The SG210-5 is not supported on SGOS 6.2 or higher because these newer releases introduce features and capabilities that require more system resources than available on the SG210-5. The SG210-5 continues to be supported on the SGOS 6.1.x releases. Please contact your sales teams for upgrade options.

SG9000

- If an onboard NVIDIA network interface on the SG9000 platform is configured to auto-negotiate and the device it is connected to is set to 100/full, there is a possibility that the interface will lock up. After the NIC gets into this state, a power cycle is required to get the NIC back to a functional state. This is a hardware issue NVIDIA has documented. To resolve this issue, reconfigure the ProxySG appliance's NIC and the external device's NIC to auto-negotiate or to matching speed/duplex settings. Note that this is the recommended configuration for Gigabit interfaces. (B#144158, SR 2-313781541)

ProxySG VA

- Under rare circumstances, the ProxySG VA can issue spurious Watchdogs exceptions. There is no unique signature to this failure – the appliance will fail with HWE 0x11 and SWE 0x02. This failure usually occurs after the product has experienced a period of load, followed by a sustained idle period. (B#157534)

Policy

- The ProxySG appliance fails to match the policy `request.header.cookie="sslallow" action.red(yes)` at CI checkpoint when apparent data type policy is present. Fixed in 6.3.2.2. (B#160176, 169358, 169378)

Serviceability

- Boot: There are no warnings on image load and information to sysinfo indicating the platform version of code loaded on the system. (B#165672, SR# 2-371493702)

SNMP

- Entries in the ipIfStatsTable in the the IP-MIB are not populated correctly and therefore queries to this table will return invalid results. (B#144836)

SSL Proxy

- If an SSL Intercept policy is enabled on the ProxySG appliance and there are malfunctioning servers where the OCS does not send the certificate during SSL handshake, the event logs are flooded with `Failed to get the peer certificate` messages. Fixed in 6.3.2.2. (B#163272, SR# 2-408255562)

SOCKS Proxy

- SOCKS services are unavailable on MACH5 licensed ProxySG appliance deployments. (B#152664)

TCP/IP and General Networking

- Occasionally, when you manually change the speed/duplex settings of one interface that is a member of a hardware bridge and then manually reset the speed/duplex settings to autonegotiate, the bridge interfaces may become out of sync if there has also been a change on the directly connected switch. (B#155727)
- Acceleration of active FTP through a load balanced ADN deployment is not supported. (B#168130)
- When failover is configured between two ProxySG appliances, the group is not formed when the secret key is more than 32 characters; both the appliances become the master. (B#165649)
- For very high bandwidth-delay links using the SCPS feature, it may be necessary to manually set the ADN window size to maximize throughput. Consider manually increasing the ADN window size with satellite links that have more than 14 Mbps of available bandwidth. Note that the ProxySG appliance needs to be restarted for the window size setting to take effect. (B#153174)
- In some WCCP GRE deployments, IP fragmentation may occur as a result of the additional bytes being added to the frame due to GRE encapsulation. The reassembly of these fragments received by the SG causes an increase in CPU. (B#151889)
  Workaround: See Knowledge Base solution 3790 (https://kb.bluecoat.com/index?page=content&id=KB3790).
- Link propagation on the optional Intel fiber card: One of the interfaces remains down while the other interface fluctuates between up and down states; this is triggered when link propagation is enabled on the fiber card and one interface that is part of the bridge losses its link and the other does not. (B#150676)
- When Bypass Keep-Alive is enabled, only the bypassed connections that are received after it is enabled apply; pre-existing connections continue to exist without sending keep-alive. (B#144923)

Visual Policy Manager (VPM)

- **Request URL Application** destination object: When the list of web applications is filtered (for example, by Upload Attachment), the **Select All** option actually selects all applications (not just the filtered applications). Workaround: change the filter to **All** before clicking **OK**; you will then see the entire list of applications, with only the filtered items selected.

Windows Media Proxy

- Accelerated streaming (MMS, HTTP, and RTSP) connections continue to show as ESTABLISHED on ADN Branch and Concentrator peers even after the client and server have both closed the session. (B#165642)
- When proxying RTSP traffic, if an RTSP server returns an invalid OPTIONS response to the ProxySG appliance, the stream will stop. This may occur when proxying RTSP streams from a Windows Media Server that does not have the latest service packs installed. Verify that server is running WMServer/ 9.1.1.5001 or later. (B#166405, SR# 2-397380182)

Yahoo Instant Messaging

- Explicit/SOCKS connections through the ProxySG appliance with Yahoo 8.1 clients: file transfers succeed, but do not display in the statistics. (B#141470)

Deprecations and Removals

The following have been deprecated or removed from SGOS 6.3.x.

Websense and SmartFilter

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

```
#(config external-services)create websense new_websense_service
Warning: Websense off-box support has been deprecated and will be
removed in a future release
  ok
```

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

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

In addition, you can no longer add/configure Websense external services or add Websense external services to Service Groups through the Management Console. You can, however, still view /edit existing Service Groups containing Websense external services from the Management Console.

CLI Commands

security iwa

The **`security iwa`** CLI commands and all associated subcommands are deprecated. They have been replaced by the **`security iwa-bcaaa`** command and subcommands.

MIB Changes

The following MIB changes were made in 6.3.1.1:

BLUECOAT-MIB

- Added device IDs for the SG300 (`device 32`), SG900 (`device 34`), SG9000 (`device 29`), AV1200 (`av 7`), and AV1400 (`av 5`).
- Changed SG600 device ID to `device 31`.

BLUECOAT-SG-PROXY

- Changed the syntax of the `sgProxyCPUCoreTable` object to be RFC compliant.
- Added the word `Core` to the table entries in `sgProxyCpuCoreTableEntry` to match the OID names.

Section E: Limitations in SGOS 6.3.x

These issues are known by Blue Coat but are not fixable because of the interaction with third-party products, works as designed but might cause an issue, or other reason.

Director

- Director might become unresponsive when executing a profile or restoring a backup on a ProxySG appliance. Director must be rebooted when this issue occurs.

IPv6

- DSCP over IPv6 is not yet supported. (B#143787)
- In an IPv6-only network (no IPv4 connections to the ProxySG appliance) with Reflect Client IP disabled, the ProxySG appliance requires the `server_url.dns_lookup prefer-ipv6` policy to successfully resolve IPv6 DNS requests. (B#143668)

Licensing

- The product description in the licensing component may show as SGOS 5.x even after upgrading to 6.x; SGOS 5.x reflects the version that the system was manufactured with. (B#145068)

Management Console

- The default Active Session list requests limit is 5,000.
- After you apply changes and see the message **Changes were committed to the SG successfully**, it actually takes the ProxySG appliance about 30 seconds to process the changes. Do not restart the ProxySG appliance during this processing time or you may lose the changes you made.
- Certain commands (server subnets, Internet gateways, VLANs) do not accept a slash in the **IP Address** field, so you cannot enter a subnet with CIDR notation (for example, 10.10.10.0/24). Because of this limitation, you will need to define a subnet by entering the IP address and subnet mask/prefix length in separate fields (IP Address: 10.10.10.0, Subnet Mask: 255.255.255.0). (B#164612)

SSL/TLS

- Due to security reasons, MD2 support for certificate verification has been removed from openssl by default (starting with version 0.9.8m). As a workaround, disable protocol detection from a specific website *<web_addr>*:

  `if url=<web_addr> detect_protocol(no) (`(B#159333)

- The ProxySG appliance cannot select a client certificate during SSL renegotiation. Therefore, if a website requests a client certificate during SSL renegotiation, the appliance will present an empty client certificate to the site. Keep in mind that Microsoft IIS (version 6 and later) is configured to request client certificates during SSL renegotiation handshakes by default and the client certificate authentication feature will therefore not work with an IIS server unless you disable this behavior by enabling `SSLAlwaysNegoClientCert` (IIS 6), using the netsh command (IIS 7) or running the `enable_ssl_renegotiate_workaround.js` (IIS 7) script. Refer to the Microsoft documentation or search the Blue Coat Knowledge Base for details on how to use these options.

TCP/IP and General Networking

- When multiple network IP addresses are configured on the same interface, the ProxySG appliance uses the wrong IP address when connecting to an external device. To avoid this issue, Blue Coat recommends that customers requiring multiple IP support should use a unique interface for each subnet. (B#158585)
- The `trust-destination-mac` and `return-to-sender outbound` options cannot be guaranteed to work in conjunction if there is a conflicting (asymmetric) route. The workaround is to disable `return-to-sender outbound` or to disable `trust-destination-mac` on the bridge. (B#158573)

Section F: SGOS 6.x — Support Files and Support for Other Products

This section lists third-party products that interact with the ProxySG appliance.

Support Files

This section provides links to files and documents referenced in the ProxySG appliance documentation set.

.htpasswd File (Perl Script)

This file is used during Local Realm (Authentication) configuration.

- https://bto.bluecoat.com/doc/13282

XML Schemas for SOAP

These schemas are used in authentication and authorization responses and requests.

- http://www.bluecoat.com/xmlns/xml-realm/1.0/xml-realm-1-0.xsd
- http://www.bluecoat.com/xmlns/xml-realm/1.0/xml-realm-1-1.xsd

Support for Other Products

This section provides the required versions of other products that interact with the ProxySG appliance.

Supported Clients and Browsers

The following are the combinations of OS, browser, and Oracle 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:

- Windows XP (SP2 or later)
- Windows Vista
- Windows 7

Supported Browser Versions

The supported browser versions for the MC and VPM are as follows:

- Windows: Internet Explorer (IE) 8.0 - 9.0 and later, Firefox 3.6 - 9.0 and later
- Apple Mac OSes: Safari 4, Safari 3, Firefox 3.6 - 9.0 and later
- Linux: Firefox 3.6 - 9.0 and later

Supported browsers means the browsers on which Blue Coat tested SGOS 6.3. Other browsers might work, but are not guaranteed by Blue Coat.

Supported JRE Versions

Supported Java JRE versions:

- 1.5.0_15 and later
- 1.6 (except 1.6_05, which causes VPM Help problems)

Notes

- On the Java download page, Java naming conventions refer to JRE 5.0 and JRE 1.5 interchangeably. JRE 5.0 is the 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 Java download page (if the automatic download hangs, first terminate the download):

  `http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-javase6-419409.html`
- 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.
- If you upgrade JRE from a lower version, clear the browser private data.

Interoperability with PacketShaper

If you are deploying the PacketShaper with a ProxySG appliance running SGOS 6.2.4 or higher, you should download and install the new ProxySG plug-in, version 1.3.0. Without the plug-in, PacketShaper classifies these flows into the `ProxySG-ADN/Default` class.

Go to the PacketShaper Download page on BlueTouch Online to download the new plug-in:

https://bto.bluecoat.com/download/product/32

Select the **PLUG INS** link for the PacketShaper version you are running and then select **Blue Coat ProxySG v1.3.0** to get to the download page.

Blue Coat Director, Reporter, and ProxyClient

Director

SGOS 6.3.x is compatible with SGME 5.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:

SGME version	Manages SGOS versions....
SGME 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
SGME 5.4.2.5	SGOS 5.3.x, SGOS 5.4.x, and SGOS 5.5.1.1 SGOS 4.3.x
SGME 5.4.2.x	SGOS 5.3.x and SGOS 5.4.x SGOS 4.3.x
SGME 5.4.1.x	SGOS 5.4.x and all SGOS versions supported by SGME 5.3.x

Reporter

This release is compatible with the following Blue Coat Reporter releases:

- Reporter 8.x
- Reporter 9.x

ProxyClient

ProxyClient versions 3.1.x, 3.2.x, 3.3.x, and 3.4.x are compatible with SGOS 6.3. To download the latest version, refer to the *Blue Coat ProxyClient Release Notes*.

Anti-Malware

The Blue Coat ProxySG appliance 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 Blue Coat AVOS 3.x.

SGOS 6.3.x works 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 6.x Support	Comments
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 appliance.
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	Beginning November 9th, 2009, clients are required to upgrade.
WLM 2009	Yes	In 6.x, WLM 2009 is tunneled. This version is also known as version 14.0. Beginning November 9th, 2009, Messenger 2009 (version 14) users must upgrade their clients. Users who have already installed the latest version, which was released Aug 18th 2009 (Build: 14.0.8089.726), are not required to upgrade.

Table 1-1. IM Client Compatibility Matrix

Client Version	SGOS 6.x Support	Comments
Yahoo 5.5, 5.6	N/A	In April 2008, Yahoo! retired these client releases.
Yahoo 8.0, 8.1	Yes	
Yahoo 9.0	Yes	In 6.x, Yahoo 9.0 is tunneled.

Partially Supported IM Protocol Versions

AIM

The ProxySG appliance does not recognize transparent AIM 6.x as AIM (IM) traffic. In some ProxySG appliance 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 appliance: The client can log in and chat normally.
    - SOCKS proxy with detect protocol enabled on the ProxySG appliance: 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 appliance: The client can log in and chat normally
    - HTTP proxy with detect protocol enabled on the ProxySG appliance: 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 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
```

Peer-to Peer (P2P)

SGOS 6.3.x supports the following P2P protocols:

- BitTorrent, with the exception of encrypted BitTorrent
- GNUtella
- eDonkey

RSA SecurID

SGOS 6.3.x supports RSA 6.0 with SecurID.

SOCKS

SGOS 6.3.x supports SOCKS v5, authentication protocol v1.

Streaming

Streaming support is limited to the following players and servers:

- The ProxySG appliance supports the following versions and formats:
  - Windows Media Player 7-12
  - Windows Media Server 9
  - Microsoft Silverlight

  Important: SGOS 6.x does not support older Windows Servers that do not support WM-HTTP when NTLM authentication is enabled.

  Newer Windows Clients, such as 11.x, do not support the MMS protocol.

  Silverlight is supported in SGOS 6.x; however, it must use WM-HTTP streaming protocol for streaming Windows content. WM-HTTP is also known as MS-WMSP.

- The ProxySG appliance supports the following Real Players and Servers:
  - RealOne Player, version 2
  - RealPlayer 8 and 10
  - RealServer 8 through 10
  - Helix Universal Server
  - Helix Player 11
- The ProxySG appliance 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

Flash Proxy (RTMP) Support

Flash streaming proxy is compatible with current versions of Flash Server, client plugins, and browsers. Blue Coat recommends using the application versions listed in the table below for full functionality.

Table 1–1 Supported Applications

Application	Version	Operating System
Adobe Flash plugin	10.x	Windows XP
Adobe Flash Server	3.x, 3.5.x, 4.x	Windows 2003 Server
Internet Explorer or Firefox	IE 7.x, 8.x FF 3.x and higher	N/A

WCCP

SGOS 6.3.x was tested with the following releases of Cisco IOS: 12.4 and 15.0. For a list of Cisco platforms that support L2 packet return, go to www.cisco.com.

America's:

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