Blue Coat SGOS 6.6.x Release Notes

Current Version: SGOS 6.6.5.8

Release Date: May 10, 2017

Document Revision: May 31, 2017

Release Note Directory

These release notes present information about SGOS 6.6.x. Each section for a specific release provides feature descriptions, changes, and fixes. Sections about known issues and limitations for SGOS 6.6.x are listed separately.

Release Index

Information About All Releases

SGOS 6.6.5.8

Release Information

- **Release Date:** May 10, 2017
- **Build Number:** 201490

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x, 1.6.x, 1.7.x, 1.8.x, and 1.9.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.7.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Fixes in SGOS 6.6.5.8

- SGOS 6.6.5.8 includes fixes, including security fixes. See "Fixes in SGOS 6.6.5.8" on the next page.

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in ProxySG 6.6.x.

Fixes in SGOS 6.6.5.8

SGOS 6.6.5.8 includes the following fixes.

Security Advisory Fixes in this Release

B#	Issue
244317	Fixed OpenSSL vulnerabilities (CVE-2017-3731). For details, see SA141.

Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of SGOS you are running, including ones published after this release, go to:

https://bto.bluecoat.com/security-advisories

Access Logging

B#	Issue
243696	TCP keep-alives were not being sent at set intervals during continuous access logging, which caused some TOP sessions to be dropped.

Authentication

	Issue
235684	Authentication was slow if IWA Authentication didn't support Active Directory (AD) sites for a Krb5 component to locate a Key Distribution Center in a particular AD site.
235886	The Banner Attribute VPM object was missing a scrollbar.
238822	After about a month of operation, the appliance experienced memory pressure in HTTP/FTP when using Kerberos Constrained Delegation.
244555	The appliance experienced a hardware restart in process group "PG_POLICY_HTTP" in process "PDW t=110339 for=BC00292" in "libauthenticator.exe.so" when using SAML authentication.
245621	The proxy delayed responses to HTTP requests and then stopped responding when using LDAP authentication.
245932	Joining the appliance to the AD domain fails if RC4 was disabled in the AD environment.
246399	The proxy experienced memory pressure in the LSA component when an invalid username/domain name was sent to the proxy.
246761	The Admin Login Banner VPM layer CPL did not compile correctly.

CLI Consoles

B#	Issue
245666	The Proxy Auto-Configuration (PAC) file could not be cached.
246169	Fixed an issue with stuck SSH connections when the appliance initiated a session rekey. The affected SSH session would stop responding and use up to 30% of CPU on the appliance.

Flash Proxy

B#	Issue
244957	The flash proxy failed to accept the handshake, causing streaming connections to break.

HTTP Proxy

B#	Issue
241561	The ProxySG may experience a hardware restart in process "HTTP CW 4A874BB50" in "libshared_dll.exe.so" at .text+0x231420.
242378 243578	The `cs-bytes` access log field displayed negative values.
243558	A "500 internal server" error occurred when a URL contained credentials and a path that included ".".
243653	Client connections increased rapidly to the maximum number followed by high CPU usage.
245111	The appliance experienced a watchdog restart in process group "" process "" in "kernel.exe" at .text+0x123d287.
246296	A `max-cache-size 10000` setting appeared in the default configuration even though `10000` is the default value for `max-cache-size`.
243388	HTTP(S) proxy upstream requests don't have `Host` header canonicalized, in accordance with RFC 7320.

ICAP

B#	Issue
242715	ICAP internal health checks failed during ICAP scanning.
247011	The appliance server connection did not close when the client application closed the connection. This occurred in ICAP response mode with scanning enabled.

Management Console

B#	Issue
245954	The /policy_import_listing.html page did not load correctly if a user logged in to the Management Console with an account subject to the Admin Authentication Realm.
246545	If you did not click **Apply** to save changes after creating an SSL keyring, the Management Console stayed in a "Loading" state.

Manuals and User Documentation

B#	Issue
245267	The "Managing the WebEx Proxy" chapter in the *SGOS Administration Guide* now indicates that Intelligence Services subscription is required to use the **Share Application** and **Upload Files** controls.
246346	The "Intercepting and Optimizing HTTP Traffic" chapter in the *SGOS Administration Guide* now reflects the current default maximum object cache size. The default increased from 1024 MB to 10000 MB.
246757	Hardware guides for S-series platforms now allow exporting NIC installation/replacement instructions to PDF.
246950	Supported Content Analysis versions have been updated in in the *SGOS Release Notes*.

MAPI Proxy

B#	Issue
245313	The appliance might experience a restart in process: "Mapi.http.worker" in "libmsrpc.exe.so".

Policy

B#	Issue
242147	The event log displayed numerous "bin payload value overflow during increment or decrement" messages.
243826	A "Late condition guards early action" error occurred when trying to install policy including `http.request.body.max_size()` in combination with any authentication-related source condition (for example, `group=`, `user=`).
244108	During VPM installation, the appliance generated a warning that included: "Empty section removed: '[Rule "elcld.com for Earthlinks Tele"] url.domain=//elcld.com/". This issue occurred if the CachePulse service was enabled.
245935	The event log displayed the error message "CE Error accessing Policy Bin Object File".

Security

B#	Issue
242300	Ensure read-only admin users can access all read-only operations.
243187	In an SSL tunnel scenario, negotiated cipher policy was applied on the extra SSL connection instead of the original SSL connection. Symantec thanks Thomas Galliano for reporting this vulnerability.

SSL/TLS and PKI

B#	Issue
244547	The ChallengePassword attribute, generated when creating a Certificate Signing Request (CSR), was NULL, which resulted in the Symantec certificate authority (CA) declining the request.

SSL Proxy

B#	Issue
245938	The proxy did not present an exception or warning for a site with more than one level subdomain that used a single wildcard certificate.

TCP/IP and General Networking

B#	Issue
244220	The RIP filtering table (via the `no_rip` command) on an aggregated NIC interface did not work.
244691	The appliance experience high CPU utilization with form-based authentication.
246181	Client router affinity setting not honored in a WCCP environment when using aggregate interfaces on the ProxySG.

URL Filtering

B#	Issue
242757	The local content filter database did not clear a subscription error after connectivity to the database server was restored.
243455	Client workers increased until the appliance stopped processing traffic.
246243	Many known sites were categorized incorrectly as `unavailable`. This issue occurred if there was a disk issue.

SGOS 6.6.5.4 (patch)

Release Information

- **Release Date:** March 16, 2017
- **Build Number:** 198852

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x, 1.6.x, and 1.7.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.7.4
- **ProxyClient:** 3.4.x
- **United Agent:** 4.7.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:
  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Fixes in SGOS 6.6.5.4

- SGOS 6.6.5.4 includes fixes, including security fixes. See "Fixes in SGOS 6.6.5.4" on the facing page.

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in ProxySG 6.6.x.

Fixes in SGOS 6.6.5.4

SGOS 6.6.5.4 includes the following fixes. It also contains these patch releases.

Security Advisory Fixes in this Release

B#	Issue
242746	Fixed OpenSSH CPU utilization DoS (CVE-2016-6515). For details, refer to https://bto.bluecoat.com/security-advisory/sa136.
242743	Fixed OpenSSH KEXINIT memory usage DoS (CVE-2016-8858). For details, refer to https://bto.bluecoat.com/security-advisory/sa136.

Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of SGOS you are running, including ones published after this release, go to:

https://bto.bluecoat.com/security-advisories

Access Logging

B#	Issue
241445	The appliance might experience a page fault in process group "PG_ACCESS_LOG" in "libaccess_log.exe.so" when there are access log entries greater than 24 KB and/or they have low compression ratios (for example, 3:1 versus more typical 8:1 or 10:1 ratios).

Authentication

B#	Issue
235937	Authorization headers are not transmitted to the upstream server when SAML basic “no client redirect” is combined with Oracle OAM-11G.
237171	The `#(config captcha cap)` **`virtual-url`** *`<string>`* command should only accept strings in valid virtual-url format.
238756	There is memory pressure in SSL when the LDAP search user password is invalid.
238859	The appliance might experience a software reset at 0x810002 in process "tcpip_admin".
239524	Certificates in a personal certificate store are deleted when you log in to the Management Console.
239580	Unused Windows Domain health checks exist after the IWA realm is deleted, which might cause the overall health status to be in a warning state.
240047	RADIUS authentication to the appliance fails with a JRadius server when RADIUS attributes contain no value.

B#	Issue
240593	LDAP authentication health check returns UP when healthy, otherwise it returns DOWN. It is Unknown when no check has been made, which translates to UP/healthy in versions up to SGOS 6.5.9.9. In that version, for RADIUS and LDAP realms which rely on an external server, LDAP authentication health check returns DOWN when Unknown. The fix restores the behavior as in SGOS 6.5.9.8 and earlier. Note that it's not a problem for IWA-Direct, because those health checks are tied to the health of the underlying AD domain.
242206	LDAP authorization name cannot be used with KCD. To use the authorization username for KCD, use the following CLI command in the IWA realm configuration: `#(config iwa-direct iwa)` **`kcd-use-authz-name enable`**
242255	A policy rule with a user or group name that contains a "^" or '@' character does not match.

CLI Consoles

B#	Issue
239940	The appliance might experience a restart when executing the `Register-with-Director` command when registering with Director 6.1.22.1 or later when the SSH key is larger than 1024 bits.
241137	A deprecated link (**Management Console > Statistics >Advanced >Archive Configuration > View last installation status**) is visible in the MC.
241140	The Management Console displays duplicate links for **Statistics > Advanced > Failover > Show Fail-over Statistics** and **Show Failover config information**.
241210	The appliance might experience a hardware restart in process "username@ssh" in "libsshd.exe.so" after upgrade.

DNS Proxy

B#	Issue
236578	The appliance is not forwarding desktop SOA DNS records for dynamic DNS updates to Active Dir-ecory when SOA UPDATE opcode is not null.

HTTP Proxy

B#	Issue
234694	Depending on timing, some HTTP responses that use compression (such as `Content-Encoding: gzip`) may cause policy checks based on the normalized response body (http.response.apparent_data_type and http.response.data) to not match, even if the uncompressed response data should match.
236294	When a client sends multiple HTTP requests without waiting for a response to each (pipelining), the appliance may log an error due to "HTTP request header size threshold exceeded" and not process all of the requests.
240971	The appliance may experience a page fault in restart in process group PG_HTTP in process "HTTP CW 3E8E8FFB90" in "libhttp.exe.so" at .text+0x2948db when byte-range support is enabled.
241844	The appliance may show a "HTTP 400 error, Page cannot be displayed" when malware scanning and active content stripping policy are enabled.

B#	Issue
238561	HTTP validation enhancements have been made to support legitimate web sites that do not strictly adhere to the HTTP RFC. These improvements include two new access log fields and policy substitutions: - `x-bluecoat-normalized-response-headers` - Identify any normalization of the HTTP(S) response headers that was completed. - `x-bluecoat-invalid-response-headers` - If applicable, describes why the HTTP (S) response is still considered invalid after normalization. For details, refer to the *Content Policy Language Reference*.
242298	The appliance experienced a software restart at 0x80005 in PG_HTTP in process "HTTP SW 420018BB90 for 59D5FC0B90".

Licensing

B#	Issue
236578	An unexpected "stolen time" event on the Secure Web Gateway Virtual Appliance caused the license server communication grace period limit to be eliminated when the virtual appliance was suspended or the license server was unreachable.

MAPI Proxy

B#	Issue
242810	The appliance experienced a page fault restart in process "Mapi.http.worker" in "libforwarding.exe.so" while proxy forwarding was enabled.

Network Drivers

B#	Issue
240143	You could not manually set interface speed to on SG-S500 with 10gb NICs because the `show configuration` command displays 100mb for the related interface.

Policy

B#	Issue
230213	Issues occur with redirect-mode authentication if authentication rules are put in a non-default tenant policy.
239657	When a custom exception page is configured and users access a blocked website using HTTP, they receive the correct custom exception page. When using HTTPS, users receive the default exception page instead of the custom exception page.
242328	Client workers exceed the maximum, which causes the appliance to be unresponsive.

Serviceability

B#	Issue
238473	Snapshots are not generated if the number of copies is set to 1000.

SSL/TLS and PKI

B#	Issue
238011	Policy using a Required Client Certificate action causes an internal error on HTTPS connection when the appliance is connecting with TLSv1.2 and evaluating `client.certificate.common_name.substring` policy.
242662	The set of CA certificates has been added and removed from the browser-trusted CCL. **Note:** The corresponding trust package will be posted on April 2, 2017. See important information in TFA 000032748:http://bluecoat.force.com/knowledgebase/articles/Technical_Alert/000032748

SSL Proxy

B#	Issue
241168	Access Log incorrectly populates `x-cs-connection-negotiated-cipher` for DHE-DSS and ECDHE-ECDSA ciphers when using STunnel.
243378	SSL interception of HTTPS traffic is broken when SOCKS proxy handoff is enabled.
244389	When accessing some Google sites like www.google.com or other Google services like Gmail or Google Drive, the Chrome browser displayed error message "This site can't be reached" and error code "ERR_CONNECTION_CLOSED". This occurred because Chrome version 56 adds support for TLS 1.3, and some Google servers requested TLS 1.3 encryption if compatible with the browser. For details, refer to the following KB article: https://bluecoat.secure.force.com/knowledgebase/articles/Technical_Alert/With-protocol-detection-enabled-we-will-break-all-explicit-traffic-that-is-going-to-TLS1-3-sites/

Storage

B#	Issue
241538	/Storage/Statistic shows software errors instead of hardware errors after disk write errors occur.

System Statistics

B#	Issue
241538	The Summary Statistics values and the statistics from the CLI command `#show diagnostics heart-beat daily` show older values than the values in the sysinfo file.

TCP/IP and General Networking

B#	Issue
240126	The appliance might experience a watchdog restart in process "idler 0" in "kernel.exe" at .text+0x12af15d.
240696	Communication with an external server using IPV6 was slow when using VLANs.
241139	The appliance is not sending FIN packets on random connections when using a 10GB NIC.
242133	Web Cache Communication Protocol (WCCP) does not redirect HTTPS traffic.

URL Filtering

B#	Issue
236363	Application Classification is not showing Application details in the Active Sessions table. This issue occurs when: • the appliance has an outdated WebPulse database • the appliance does not have the service point URLs defined • WebPulse is enabled.
240372	Categorization of YouTube URLs can be bypassed by modifying the URL.
241936	The appliance experienced a page fault restart in process "OPP_Wo 0x399893d710" in "libfdt.so".
242434	The appliance experienced a watchdog restart in process in "kernel.exe".

6.6.5.4 - Patch Release Fixes

SGOS 6.6.5.4 includes all of the fixes included in the following patch releases:

- SGOS 6.6.5.310
- SGOS 6.6.5.3

SGOS 6.6.5.310 Patch

SGOS 6.6.5.310 includes the following fixes:

Policy

B#	Issue
242125	ProxySG appliances with common (hybrid) policy may experience memory pressure.

SSL Proxy

B#	Issue Workaround (if available)
244389	When accessing some Google sites like www.google.com or other Google services like Gmail or Google Drive, the Chrome browser displayed error message "This site can't be reached" and error code "ERR_CONNECTION_CLOSED". This occurred because Chrome version 56 adds support for TLS 1.3, and some Google servers requested TLS 1.3 encryption if compatible with the browser. For details, refer to the following KB article: https://bluecoat.secure.force.com/knowledgebase/articles/Technical_Alert/With-protocol-detection-enabled-we-will-break-all-explicit-traffic-that-is-going-to-TLS1-3-sites/

SGOS 6.6.5.3 Patch

SGOS 6.6.5.3 includes the following fixes:

Authentication

B#	Issue
239863	The ProxySG appliance may stop accepting configurations and then stay in a failed state when IWA-Direct group caching is enabled.
239168	You cannot load inline objects on a web page that are from third-party domain when using CAPTCHA.

TCP/IP and General Networking

B#	Issue
242125	Static bypass does not work with Web Content Communication Protocol (WCCP) Layer 2 (L2) when using aggregate interfaces.

SGOS 6.6.5.2

Release Information

- **Release Date:** October 21, 2016
- **Build Number:** 193348

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x, 1.6.x, and 1.7.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.7.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:
  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

Important Changes in 6.6.5.2

A new access log field has been added: `x-data-leak-detected` (B#229033).

Fixes in SGOS 6.6.5.2

- SGOS 6.6.5.2 includes fixes, including security fixes. See "Fixes in SGOS 6.6.5.2" on page 17.

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in ProxySG 6.6.x.

Fixes in SGOS 6.6.5.2

SGOS 6.6.5.2 includes the following fixes.

Security Advisory Fixes in this Release

B#	Issue
SA129	Multiple libxml2 Vulnerabilities
SA132	OpenSSL Vulnerabilities 22-Sep-2016 and 26-Sep-2016

Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of SGOS you are running, including ones published after this release, go to:

https://bto.bluecoat.com/security-advisories

Authentication

B#	Issue
235926	The Help button under "Set Banner Object" is greyed out and not available.
235927	The Admin Login Banner text box in the VPM bypasses the 2000 character limit.
238059	The appliance may experience a software restart in process PG_LSA when using SMB2.
238100	A create-validator for the CAPTCHA CLI command does not get stored in archived-config.
238167	The appliance uses 302 instead of 307 for authentication_redirect_from_virtual_host leg of authentication sequence.
238169	The appliance may experience a page fault in process group "PG_LSA" process "likewise windows domain DC connector" in "liblikewise.exe.so".
239094	Kerberos does not handle incorrect Active Directory DNS SRV entries correctly when an Infoblox appliance is acting as the DNS server.

Boot

B#	Issue
239002	On an S-SG400 or S-SG500, if a system image on one of the boot devices is corrupted but the redundant copy on the other boot device is valid, the system image will be marked as failed. If the system image is the default system image, then another system image will be selected as the default.

Client Manager

B#	Issue
232060	In the Active ProxyClients tab in the GUI the statistics are not displaying correctly.

CLI Consoles

B#	Issue
238666	The appliance may experience a hardware restart in process group "PG_SSH" at process "accepted@ssh" in "libsshd.exe.so" at .text+0x23a960 when there are multiple SSH connections during a high system load.
239602	The appliance may experience a page fault in process group "PG_SSH" at process "sshd.worker.*" in "libsshd.exe.so".

Collaboration

B#	Issue
235153	WebEx CLI commands are not enabled.

HTTP Proxy

B#	Issue
236610	The appliance may experience a software restart in libactive_sessions.exe.so" at .text+0x22e399.
238346	The appliance may experience a software restart in process "HTTP CW 1D981B3B50" in "libstack.exe.so".

ICAP

B#	Issue
237961	When ICAP RESPMOD is enabled, the ProxySG fails to decode some HTTP chunked responses that are valid, resulting in a fatal ICAP error.
238641	The appliance may experience a hardware reset in process "OPP_Wo 0x9e7a8580" in "libpolicy_enforcement.so".
239018	Added access log field "x-data-leak-detected".

Kernel

B#	Issue
238164	The ProxySG experienced a page fault in process "ipmi.exe".

MAPI Proxy

B#	Issue
238772	MAPI-HTTP html mail with malicious content is rendered incorrectly because of proxy inserted text.
239651	The appliance may experience a page fault process "Mapi.http.worker" in "libmsrpc.exe.so".

MC Legacy

B#	Issue
237888	Link Aggregation interfaces do not show up in the WCCP configuration window.
238066	Multiple instances of Link Aggregation interfaces are repeated in the WCCP configuration.

Policy

B#	Issue
235181	Policy rule for trust-destination-ip is not working for SSL sites even though it matches.

Security

B#	Issue
238861	Marked DES ciphers as low strength in response to Sweet32 vulnerability (CVE-2016-2183).

SSL Proxy

B#	Issue
239164	The appliance may experience memory pressure after upgrade to 6.6.5.1 when SSL is intercepted.
239737	The appliance may experience memory pressure in SSL and Crypto functions.

TCP/IP and General

B#	Issue
239049	Overlapping routes are not working after going from an SG510 running SGOS 6.2 to an ASG S200 running SGOS 6.6.4.2.
239467	The appliance restarts in process "" in "kernel.exe" at .text+0x123d287 during the update of the routing table.
239468	The appliance may fragment packets on S-Series appliances.

Timezones and NTP

B#	Issue
239525	The appliance time zone database has been updated to include a change in daylight savings time in Turkey. Details on this change can be found in the Technical Alert at: http://bluecoat.force.com/knowledgebase/articles/Technical_Alert/000028315

URL Filtering

B#	Issue
229493	Despite the Application Attributes controls being present the backend, data is not available at this time. Once the data is made available this feature will work.
238886	The appliance experienced memory pressure "Content Filtering".

SGOS 6.6.5.1

Release Information

- **Release Date:** September 15, 2016
- **Build Number:** 191844

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x and 1.6.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.7.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- If you downgrade from this release to a 6.6.x version that does not support Java Web Start, you cannot use the previously downloaded Java Network Launch Protocol (JNLP) files to access the Management Console. Instead, access the Management Console directly in a browser.

Changes in SGOS 6.6.5.1

- SGOS 6.6.5.1 introduces new features and enhancements. See "New Features in SGOS 6.6.5.1" on page 22.

Fixes in SGOS 6.6.5.1

- SGOS 6.6.5.1 includes fixes, including security fixes. See "Fixes in SGOS 6.6.5.1" on page 26.

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in ProxySG 6.6.x.

New Features in SGOS 6.6.5.1

SGOS 6.6.5.1 introduces the following new features.

Management Console Access Using Java Web Start

In previous versions of SGOS , some browsers could not display the Management Console. This release of SGOS includes Java Web Start support, which provides an alternative to running the Management Console directly in a browser. Use Java Web Start if any of the following applies to your deployment:

- Your browser does not support NPAPI.
- Your browser is not configured to run Java or JavaScript.
- You want to be able to launch multiple appliances from a single interface.

Depending on what you want to achieve, your environment must meet specific requirements to use Java Web Start. Refer to the SGOS *Administration Guide* for details.

ⓘ If you downgrade from this release to a 6.6.x version that does not support Java Web Start, you cannot use the previously downloaded JNLP files to access the Management Console. Instead, access the Management Console directly in a browser.

- Full information:
  SGOS Administration Guide – Accessing the SGOS Appliance

Boot Loader Changes

The boot loader was updated to address issues with corrupt system images and reboot loops. The updates consist of the following:

- You can restore factory defaults to your ProxySG appliance with the new command `r`.
- The boot loader informs you when a system image is corrupt, removes the corrupt image, and logs the corruption.
- The boot loader can regenerate lost system image metadata.

- Full information:
  Blue Coat KB article 000031250:
  https://bluecoat.secure.force.com/knowledgebase/articles/Solution/000031250

RDNS Lookups are Disabled by Default

To prevent potential misuse of RDNS by malicious third parties, the policy engine disables RDNS lookups by default. The following new CLI command supports this change:

```
#(config) policy restrict-rdns {all|none}
```

where `all` is the default setting.

This change affects the following policy gestures if they attempt to trigger an RDNS lookup when the host is specified as an IP address:

- `client.host=`
- `client.host.has_name=`
- `request.header.Referer.url.category=`
  (affects policy categories and local database lookups)
- `server_url.domain=`
  (affects policy categories and local database lookups)

- `url=`
- `url.category=`
  (affects policy categories and local database lookups)
- `url.domain=`
- `url.host=`

To enable RDNS lookups on trusted subnets, add `restrict rdns` definition blocks to policy. Symantec recommends that you write policy such as the following:

```
; restrict all RDNS except for the specified subnets

restrict rdns

  except

    <list of trusted subnets>

end
```

If you are upgrading to this release, the following command reverts the appliance to its previous behavior. To enable RDNS lookups globally via the CLI:

```
#(config) policy restrict-rdns none
```

Notes:

- The presence of a `restrict rdns` definition in policy overrides the global setting in the CLI. This CLI setting is only used when there are no RDNS restrictions defined in policy.
- Symantec strongly recommends that you do not allow RDNS lookups of untrusted IP addresses. RDNS should be restricted to only subnets under your control, or the control of another trusted party. For details on the potential impact of RDNS lookups, refer to Security Advisory SA130.

- Full information:
  ***SGOS Upgrade/Downgrade Guide* – Behavior Changes Applicable to SGOS 6.6.x Upgrade**
  ***Content Policy Language Reference* – Condition Reference**
  ***Command Line Interface Reference* – Privileged Mode Configure Commands**

Improved WAF Command Injection Detection Engine

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

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

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

```
define application_protection_set mySet

   engine=injection.command version=2

end

<proxy>

 http.requestion.detection.mySet(block)
```

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

```
define application_protection_set mySet
```

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

- Full information:
  Content Policy Language Reference – Definition Reference

  SGOS Upgrade/Downgrade WebGuide– Behavior Changes Applicable to SGOS 6.6.x Upgrade

  Web Application Firewall Solutions Guide – WAF Policy Reference

Simplified CAC Deployment

The Common Access Card (CAC) client workstation no longer requires a PKCS11 provider to be configured. The ProxySG appliance works with the software provided by the third-party card reader software (such as ActiveID® ActivClient®).

- Full information:
  Common Access Card Solutions Guide, SGOS 6.5.9.10 and later

Support for DHE-DSS Ciphers for Forward Proxy

This release supports DHE-DSS ciphers for Forward Proxy. The following ciphers are available in upstream connections in forward proxy mode:

- DHE-DSS-AES128-SHA
- DHE-DSS-AES128-SHA256
- DHE-DSS-AES256-SHA
- DHE-DSS-AES256-SHA256
- DHE-DSS-DES-CBC-SHA
- DHE-DSS-DES-CBC3-SHA

Enhancements and Changes in this Release

This release also includes the following changes:

- Access logs now report when errors occur due to Kafka broker configuration changes.
- You can now specify the authentication virtual URL for the CAPTCHA validator. Use the following CLI command:

  ```
  #(config captcha <realm_name>)virtual-url<URL>
  ```

- Currently-supported ciphers are now available when creating policy using the Visual Policy Manager.
- You can now designate sections of policy as being appliance-specific using the `#if` and `#endif` variables.

  For example, protect policy specific to Advanced Secure Gateway with:

  ```
  #if product=asg
  ; guarded rules
  ...
  #endif
  ```

  Protect policy specific to SGOS with:

```
#if product=sg

; guarded rules

...

#endif
```

For details, refer to the "Overview of Content Policy Language" chapter in the *Content Policy Language Reference*.

Fixes in SGOS 6.6.5.1

SGOS 6.6.5.1 includes the following fixes.

Security Advisory Fixes in this Release

B#	Issue
237378	This bug fix addresses multiple PCRE vulnerabilities. Refer to Security Advisory SA128 for details.
236776	This bug fix addresses a security control bypass vulnerability. Refer to Security Advisory SA130 for details.

Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of SGOS you are running, including ones published after this release, go to:

https://bto.bluecoat.com/security-advisories

Authentication

B#	Issue
235296	A restart occurred when an IPv6 prefix address was sent from the RADIUS server to the appliance.
235708	CAPTCHA validation returned an incorrect redirect type when using Microsoft Internet Explorer.
220104	The appliance restarted with a page fault in PG_UNKNOWN process "Session Manager" in "lib-session_manager.exe.so".
237317	Custom CAPTCHA validation forms could not be created when an exception was added incorrectly.

Client Manager

B#	Issue
234815	The appliance returns an error when an administrative user attempts to upload the updated version of Unified Agent client software to the appliance using the **Local File** option.

Collaboration

B#	Issue
236360	The CLI help text for the `#(config webex)` **`http-handoff`** subcommands was incorrect.

HTTP Proxy

B#	Issue
235642	Tolerate request parsing caused invalid request headers to be passed to the Web Application Firewall. As a result, the appliance stopped responding.
237985	Some web pages were blocked when HTTP responses included a list of multiple identical `content-length` values (such as `content-length: 10, 10`); these responses were treated as invalid and rejected.

B#	Issue
237986	Some web pages did not load and an exception occurred when HTTP responses included invalid `content-length` headers and a transfer-encoding: chunked header; these responses were treated as invalid and rejected.
231208	An unexpected restart occurred in process group: " ", Process: " " in kernel.exe. This issue occurred when all of the following were enabled on the appliance: • SSL interception • ICAP REQMOD policy • Blue Coat WebFilter content filtering • Application Classification service • access logging

ICAP

B#	Issue
234104	The Content Analysis log displayed numerous "ProtocolICAP::Process: error parsing ICAP request" errors.

Management Console

B#	Issue
236283	When multiple virtual appliances were deployed with the same serial number, the Management Console reported that the license was suspended instead of displaying a warning to resolve the issue within 30 days.
237248	You could import a maximum of 500 CA certificates through the Management Console. The limit has been removed.

MAPI Proxy

B#	Issue
236625	The appliance restarted with a page fault in access logging while logging a MAPI-HTTP request that requires escaping.

Policy

B#	Issue
237575	The `client.address=` condition did not work as expected when the client address was unavailable at the start of the transaction.
235849	The appliance restarted with a page fault in Process group: "PG_POLICY_HTTP" in process: "PDW".

Security

B#	Issue
237142	Secure connections using SSLv3 was enabled by default when using Client Manager and hardcoded for port 8084. For best security, Client Manager no longer accepts SSLv3 connections.

SNMP

B#	Issue
237543	The appliance stopped responding when it experienced heavy traffic including SNMP requests.

SSL Proxy

B#	Issue
236753	When DHE-DSS ciphers were used, `server.connection.negotiated.cipher` policy failed.
237493	Fixed an issue where the appliance did not handle policy based on URL or domain correctly. This occurred when the HTTPS service was configured with the TCP Tunnel proxy type and protocol detection was enabled.

SSL/TLS and PKI

B#	Issue
235448	The appliance experienced a hardware restart in process "HTTP CW 5F6F56B50" in "libtransactions.exe.so". This issue occurred when the following were enabled on the appliance: • policy trace • Geolocation service • SSL interception • automatic protocol detection

Storage

B#	Issue
236541	On the SG-S500 platform, the CLI reported a message, "SCSI: Mode selector page 8" while SGOS was loading.

TCP/IP and General Networking

B#	Issue
228663	WCCP configuration did not accept a link aggregated interface.
235276	S-Series appliances ignored requests from ProxyAV 510 appliances.
237272	IPv6 connections in transparent proxy did not work when `#(config general)`**`reflect-client-ip`** was enabled.

URL Filtering

B#	Issue
236564	An increased number web applications available to the Application Classification service might have resulted in prolonged database processing times. As a result, the watchdog sometimes triggered a system reboot.
236743	Top-level domains in the local database category were not rated correctly.
236102	Content filtering intermittently reported "none" for URLs that had valid categories. This issue occurred when a multi-processor appliance processed high volumes of data.
236855	Attempts to update the Intelligence Services databases (such as Geolocation and Application Protection) using the `download get-now force` command failed.

6.6.5.4 - Patch Release Fixes

SGOS 6.6.5.4 includes all of the fixes included in the following patch releases:

- SGOS 6.6.5.310
- SGOS 6.6.5.3

SGOS 6.6.5.310 Patch

SGOS 6.6.5.310 includes the following fixes:

Policy

B#	Issue
242125	ProxySG appliances with common (hybrid) policy may experience memory pressure.

SSL Proxy

B#	Issue Workaround (if available)
244389	When accessing some Google sites like www.google.com or other Google services like Gmail or Google Drive, the Chrome browser displayed error message "This site can't be reached" and error code "ERR_CONNECTION_CLOSED". This occurred because Chrome version 56 adds support for TLS 1.3, and some Google servers requested TLS 1.3 encryption if compatible with the browser. For details, refer to the following KB article: https://bluecoat.secure.force.com/knowledgebase/articles/Technical_Alert/With-protocol-detection-enabled-we-will-break-all-explicit-traffic-that-is-going-to-TLS1-3-sites/

SGOS 6.6.5.3 Patch

SGOS 6.6.5.3 includes the following fixes:

Authentication

B#	Issue
239863	The ProxySG appliance may stop accepting configurations and then stay in a failed state when IWA-Direct group caching is enabled.
239168	You cannot load inline objects on a web page that are from third-party domain when using CAPTCHA.

TCP/IP and General Networking

B#	Issue
242125	Static bypass does not work with Web Content Communication Protocol (WCCP) Layer 2 (L2) when using aggregate interfaces.

SGOS 6.6.4.3

Release Information

- **Release Date:** July 22, 2016
- **Build Number:** 188886

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.6.x
- **ProxySG Appliances:**
    - S500, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:
    - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
    - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

Changes in SGOS 6.6.4.3

- SGOS 6.6.4.3 introduces new features and enhancements. See "New Features in SGOS 6.6.4.3" on page 32.

Fixes in SGOS 6.6.4.3

- SGOS 6.6.4.3 includes fixes, including security fixes. See "Fixes in SGOS 6.6.4.3" on page 34.

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in ProxySG 6.6.x.

New Features in SGOS 6.6.4.3

SGOS 6.6.4.3 introduces the following new features.

CAPTCHA Validation

You can implement a CAPTCHA challenge-response test for specific proxied client requests. Configuring the feature consists of creating a CAPTCHA validator and form in the CLI, and then including them in policy. You can implement CAPTCHA validation with or without authentication. The following is an overview of what happens during validation:

- A client makes a request that, according to policy, is subject to CAPTCHA validation.
- The browser presents an HTML form including a CAPTCHA image that the user must solve. A correct response verifies that the request was human-initiated.
  - If the response is incorrect, the form loads a new CAPTCHA image.
  - If the response is correct, the browser loads the requested page and the appliance sets a session cookie. The CAPTCHA test is not invoked for future requests from the same client and to the same domain until the cookie expires.

The following have been added to support this feature:

- CLI commands, to create and manage CAPTCHA validation forms:

  ```
  #(config) security captcha
  ```

  ```
  #(config captcha <realm_name>)
  ```

- CPL actions, to include CAPTCHA validators in policy:

  ```
  validate()
  ```

  ```
  validate.form()
  ```

  ```
  validate.mode()
  ```

- Full information:
  SGOS Administration Guide – **Forms-Based Authentication and Validation**

  Command Line Interface Reference – **Privileged Mode Configure Commands**

  Content Policy Language Reference – **Action Reference**

Notice and Consent Banner for Administrators

You can now configure the notice and consent banner for admin users through the Visual Policy Manager (VPM). In previous versions, configuration of this feature was limited to the CPL.

- Full information:
  Notice and Consent Banner Configuration Webguide – **Create a Banner for the Management Console > VPM**

  Visual Policy Manager Reference – **The Visual Policy Manager**

Web Application Firewall Enhancements

This release includes the following WAF enhancements:

WAF Policy Enhancement

You can now base policy decisions on the results of WAF application protection and validation with two new policy conditions:

- `http.request.detection.result.validation=`
- `http.request.detection.result.application_protection_set=`

Verbose Header and Body Logging

You can use a new policy gesture to report on the contents of the header, body, or both from a user request in an access log.

Add header or body content to the WAF access log with the following policy actions:

- `http.request.log_details[body,header] (yes|no)`
- `http.request.log_details[body] (yes|no)`
- `http.request.log_details[header] (yes|no)`

When any of these policy actions is set to `yes`, the bcreporterwarp_v1 access log is populated with the respective request data:

- `x-bluecoat-request-details-header`
- `x-bluecoat-request-details-body`

In a WAF deployment, this data is critical in determining the validity of detections. When used in conjunction with the new `http.request.detection.result.validation=` and `http.request.detection.result.application_protection_set=` conditions, you can review the header or body contents to qualify detections and rule out false positives. By default, the maximum size of body content is 8 KB. This can be increased with either the `http.request.data.N=` or `http.request.body.inspection_size()` policy gesture.

`http.request.log_details()` works for other deployments as well, but you must create a custom access log format that includes the new fields, or make use of the default WAF log.

- Full information:
  Content Policy Language Reference– Condition Reference and Action Reference

Hardware Support

This release supports Seagate 1TB HDD ST1000NX0353 hard disks for the S200 platform.

Maximum HTTP Object Cache Size

The maximum object size that the ProxySG appliance can cache has increased from 4 GB to 10 GB. This change does not apply to upgrades, only new installations.

Fixes in SGOS 6.6.4.3

SGOS 6.6.4.3 includes the following fixes.

Security Advisory Fixes in this Release

B#	Issue
233211 233225	This bug fix addresses OpenSSL vulnerabilities. Refer to Security Advisory SA117 for details.

Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of SGOS you are running, including ones published after this release, go to:

https://bto.bluecoat.com/security-advisories

Authentication

B#	Issue
233608	The appliance no longer experiences high CPU in LSA and OpenLDAP when there is no user load.
232841	In a hybrid LDAP/WinSSO configuration, issues occur following LDAP client referrals.

CLI Console

B#	Issue
236048	The `show failover` command no longer shows an internal message in output.

Client Manager

B#	Issue
235987	Management of Unified Agent has been added to the Management Console, including configuration and statistics.

HTTP Proxy

B#	Issue
231925	When clients use FTP over HTTP, the appliance no longer incorrectly adds an extra `%` character to the URI in the HTML `<BASE>` tag.
235674	The CLI console and Management Console accept a `max-cache-size` larger than 32256 MB.

ICAP

B#	Issue
235674	The appliance no longer experiences a hardware restart at `0xe` in process group `PG_HTTP` when doing REQMOD scanning.

MAPI Proxy

B#	Issue
235747	When the appliance removes attachments from received e-mail, and the message body is HTML, the attachment removal description is appended in UTF-8. Previously, it was appended incorrectly in UTF-16.
235584	ICAP response headers that the appliance sends to the ICAP server are now correct.
225510	The Active Sessions window now indicates that ICAP scanning is in progress.
235531	Access logs now display the `message-id` for received messages.

Policy

B#	Issue
235815	Incorrect URL encoding no longer causes content filtering to report the wrong category.

SOCKS Proxy

B#	Issue
235707	More than one remote session can be established using SOCKS client.

SSL Proxy

B#	Issue
232907	Cache handling of multiple emulated certificates with the same common name has been enhanced to avoid certificate cache collisions, potentially reducing CPU utilization. **Note:** Remove the SSL splash text policy workaround after upgrading to a release with this fix. This fix also address a condition where an expired cached certificate could be used when presenting an exception page. See the following documentation on BTO for details: • Technical Alert TFA140 • Knowledge Base article 000022650 • Knowledge Base article 000024136
229635	HSM hostnames now permit the hyphen character.
224906	In a reverse proxy deployment, SSL connections are no longer dropped when the origin content server (OCS) downgrades TLS versions or multiple servers with different TLS versions are load-balanced.

SSL/TLS and PKI

B#	Issue
232551	The **Client Negotiated Cipher** and **Server Negotiated Cipher** VPM objects now list all of the appliance's supported cipher values.
235232	In Windows, the Management Console now loads with Java 7. You do not have to enable TLS 1.0, TLS 1.1, and TLS 1.2 in the Java Control Panel.

URL Filtering

B#	Issue
229395	When you cancel a BCWF database download, you now receive the expected message "Download canceled".
231923	When downgrading to SGOS 6.5 and earlier, you no longer receive a "% cannot use forwarding when Secure is enabled" message if a forwarding host is configured for the WebPulse connections.

Web Application Firewall

B#	Issue
229395	Tolerate request parsing no longer causes invalid request headers to be passed to Web Application Firewall. This issue resulted in a software restart.

SGOS 6.6.4.2

Release Information

- **Release Date:** June 24, 2016
- **Build Number:** 188535

Compatible With

- **BCAAA Version:** 5.5 and 6.1
- **SGME:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.6.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:
  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

Changes in SGOS 6.6.4.2

- SGOS 6.6.4.2 has no new features.

Fixes in SGOS 6.6.4.2

- SGOS 6.6.4.2 includes fixes. See "Fixes in SGOS 6.6.4.2" on page 39.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://bto.bluecoat.com/security-advisories

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

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in SGOS 6.6.x.

Fixes in SGOS 6.6.4.2

SGOS 6.6.4.2 includes the following fixes.

URL Filtering

B#	Issue
235815	Resolved issues where URL rewrites with encoded characters might have triggered a restart. In addition, URL filtering lookups might not have matched correctly when the request URI had encoded characters and a policy-defined category existed.

SGOS 6.6.4.1

Release Information

- **Release Date:** June 20, 2016
- **Build Number:** 187589

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **United Agent:** 4.6.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:

  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

- On an initial upgrade to version 6.6.4.x, if the default protocols (TLS 1,0, 1.1, and 1.2) for the HTTPS Console service were selected previously, only TLS 1.1 and 1.2 are selected by default now. If the HTTPS Console service's protocols were changed from the defaults previously, the selections do not change.

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

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

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

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

- Keyrings with certificates and/or CSRs over 8k created in this release are not backward-compatible with previous 6.6.x releases. A keyring in its downgraded form is unusable, and attempting to use it will result in errors. Symantec recommends importing a smaller certificate and/or CSR when downgrading to an earlier release. After a downgrade, keyrings are subject to the 8000-byte limit.
- The ProxySG Virtual Appliance MACH 5 Edition now supports increased VM memory sizes; however, you *must* do the following before upgrading to this release:

  1. Update the license key using the CLI command:
     `#licensing update-key`
  2. Set the VM memory to 2048 MB (2 GB).

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

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

- The ProxySG Secure Web Gateway Virtual Appliance (SWG VA) now supports increased VM memory sizes; however, you must do the following before upgrading to this release on the V-100 platform:

  1. Update the license key using the CLI command:
     `#licensing update-key`
  2. Set the VM memory to 8192 MB (8 GB). For instructions on how to configure the VM memory, see the following knowledge base article:
     http://bluecoat.force.com/knowledgebase/articles/Solution/000031436

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

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

Changes in SGOS 6.6.4.1

- SGOS 6.6.4.1 introduces new features and enhancements. See "New Features in SGOS 6.6.4.1" on the facing page.

Fixes in SGOS 6.6.4.1

- SGOS 6.6.4.1 includes a number of fixes. See "Fixes in SGOS 6.6.4.1" on page 48.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://bto.bluecoat.com/security-advisories

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

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in SGOS 6.6.x.

New Features in SGOS 6.6.4.1

SGOS 6.6.4.1 introduces the following new features.

Optimize WAF Scanning to Improve Performance

To improve performance, you can now optimize Web Application Firewall (WAF) engine scanning for requests whose response is served from the object cache on the appliance. Use the following property:

```
http.request.detection.bypass_cache_hit(yes|no)
```

where:

- `yes` - WAF engines do not scan requests that result in a response cache hit.
- `no` - WAF engines scan all requests; this is the default behavior.

In reverse proxy deployments with a high cache-hit ratio, enabling this property can have a significant positive impact on performance.

- Full information:
  Content Policy Language Reference **– Property Reference**

  Web Application Firewall Solutions Guide

XML Request Parsing

You can now write policy to parse XML requests:

- `http.request.detection.xml.cdata()`
- `http.request.detection.xml.invalid()`
- `http.request.detection.xml.node_depth()`
- `http.request.detection.xml.schema.schema_name()`
- `http.request.detection.xml.xinclude()`
- `http.request.detection.xml.xxe()`
- `http.request.detection.xml.xpath_validation()`

Use these gestures with the new `define xml_schema-type_schema` definition block.

In addition, the appliance can now treat requests with the `content-type` header as if the body content-type is XML. Use the existing property with `xml` as a parameter:

```
http.request.body.data_type(xml)
```

- Full information:

  Content Policy Language Reference **– Property Reference and Definition Reference**

Multi-Tenant Policy Supports More Conditions for Tenant Determination

In the Landlord policy file, you can now use `proxy.address` and `proxy.port` to determine your tenants.

- Full information:

  Content Policy Language Reference **– Condition Reference**

  Multi-Tenant Policy Deployment Guide

Office 365 Exchange Online Support

E-mail security is improved in this release with Office 365 Exchange Online support. This adds support for Windows Outlook 2010, 2013 and 2016 clients using MAPI over HTTPS. You can now:

- Write policy to intercept Office 365 MAPI/HTTPS traffic; refer to the *SGOS Administration Guide* for details and policy examples
- Scan attachments in messages between Microsoft Office 365 mail services and Outlook 2013 or Outlook 2010 (with hotfix)
- Monitor Office 365 traffic in active sessions and troubleshoot problems using access logs

The existing CLI command manages MAPI handoff:

```
#(config mapi)handoff {enable | disable}
```

In this release, it also manages MAPI-HTTP handoff.

A new access log, mapi-http, has been added.

- Full information:
  ***SGOS Administration Guide* – Managing Microsoft Outlook E-mail Traffic**

  ***Command Line Interface Reference* – Privileged Mode Configure Commands**

Detection and Improved Handling for Invalid Characters

In this release, support has been added for:

- Detecting invalid in characters HTTP response header lines
- Converting alternate whitespace characters in headers to standard spaces
- Improved handling of invalid characters at the beginning of header and HTTP 0.9 responses
- Detecting invalid HTTP version strings in HTTP response headers l Improved handling of invalid/missing response codes
- Unfolding of normal and empty continuation lines in HTTP response headers
- Improved handling for different variations of chunked encoded responses

Symantec thanks Steffen Ullrich and his HTTP Evader tool for helping to identify these issues.

Set ICAP Header Values for REQMOD and RESPMOD

The request and response ICAP headers can now be set via policy. This can be done via the following gestures in the `set()` action within a define action block:

- `icap_reqmod.request.x_header.`*`header_name`* - Identifies an ICAP request header for REQMOD.
- `icap_respmod.request.x_header.`*`header_name`* - Identifies an ICAP request header for RESPMOD.

where *header_name* is a string specifying the new header value.

ICAP headers are now also available via the access log as ELFF values:

```
x-icap-reqmod-header(<header_name>)

x-icap-respmod-header(<header_name>)
```

- Full information:
  ***Content Policy Language Reference* – Action Reference**

Simultaneously Scan and Upload Content

You can now have ICAP scan a request while the appliance uploads your content. Use the following property:

```
request.icap_mirror(yes|no)
```

- Full information:

  Content Policy Language Reference – Property Reference

Force ICAP Rescanning

Use the following new property to force ICAP to rescan any cached responses:

```
response.icap_service.force_rescan(yes|no)
```

where:

- `yes` - The ICAP service rescans the response.
- `no` - ICAP does not rescan response. This is the default value.

Previously, the existence of ICAP header policy on the appliance determined whether ICAP rescanned responses.

- Full information:
  Content Policy Language Reference – Property Reference

Routing Domain Support for DNS Forwarding Groups

After creating a new DNS forwarding group, you can associate that group with a specific routing-domain.

```
#(config dns fowarding group_name) routing-domain <routing domain name>
```

Hyper-V Virtual Appliance

The Secure Web Gateway Virtual Appliance (SWG VA) and ProxySG Virtual Appliance MACH5 Edition (MACH5 VA) are software solutions that can now be installed and deployed on a server running the Microsoft Hyper-V™ hypervisor running Windows 2012 R2. For complete information, see the *Secure Web Gateway Virtual Appliance Initial Configuration Guide, Hyper-V Hypervisor Platform.*

Certificates and CSRs over 8k Supported in Keyrings

SGOS no longer restricts the size of certificates and certificate signing requests (CSRs) used in keyrings created in the CLI or Management Console. You can now create certificates and CSRs larger than 8000 bytes in size for use in keyrings. However, if you downgrade to a previous version of SGOS which does not support certificates or CSRs exceeding 8k, using the large keyrings would generate errors. For details, see "Upgrading To/Downgrading From This Release" on page 40.

Enhancements and Changes in SGOS 6.6.4.1

SGOS 6.6.4.1 also introduces the following enhancements and changes:

Subscription Database Download Progress and Cancellation Enhancements

You can now cancel a database download while it is in progress. This is available in the CLI for the following services:

- Content Filtering
- Application Classification
- Application Protection
- CachePulse
- Geolocation
- Threat Risk Levels

To cancel the download, issue the **`download cancel`** command at the appropriate prompt. For example, issue the following command to cancel an Application Protection database download:

```
#(config application-protection) download cancel
```

You can also press and hold CTRL+C to cancel a download initiated through the **`download get-now force`** command. With both methods of canceling the download, the CLI indicates that the cancellation is in progress and when it is complete.

The following apply to content filtering, Application Classification, Geolocation, and Threat Risk Levels:

- When you initiate a download in the Management Console, the **Download Options** section displays a "Download is in progress" message.
- In the Management Console, you can cancel a download by clicking the new **Cancel Download** button on the **Download** tab.

Authentication Enhancements

- The following CLI subcommand has been added:

  ```
  #(config iwa-direct realm_name)suppress-ntlm-challenges {enable | disable}
  ```

  When enabled, the appliance suppresses NTLM challenges and sends only Negotiate challenges for NTLM and Kerberos; NTLM responses are still accepted. When disabled, the appliance does not suppress NTLM challenges.

- The SOCKS proxy now supports Kerberos authentication, including cases when a user logs in without specifying their password (such as logins with smart cards). You can use Kerberos authentication over SOCKS5 when a SOCKS client itself does not support Kerberos authentication or proxy servers. To acquire a Kerberos ticket, the SOCKS client must be able to access the appliance using the hostname.

  Use the existing `socks.authenticate()` property to authenticate SOCKS5 connections using Kerberos credentials.

URL Categorization Change

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

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

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

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

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

<table>
<tr><td colspan="2">If a URL matches a custom category in policy but not a Blue Coat WebFilter category, testing it yields the following responses:</td></tr>
<tr><td>Current behavior:
<code>Policy: Policy-Shopping</code>
<code>Blue Coat: none</code>
Previous behavior:
<code>Policy: Policy-Shopping</code></td><td>Current and previous behavior:
<code>Policy: Policy-Shopping</code></td></tr>
<tr><td colspan="2">If a URL does not match any custom category in policy or a Blue Coat WebFilter category, testing it yields the following responses:</td></tr>
<tr><td>Current and previous behavior:
<code>Policy: none</code>
<code>Blue Coat: none</code></td><td>Current and previous behavior:
<code>Policy: none</code>
<code>Blue Coat: none</code></td></tr>
</table>

Fixes in SGOS 6.6.4.1

SGOS 6.6.4.1 includes the following fixes:

Access Logging

B#	Issue
219640	The output for the `#show configuration` command now indicates that `collaboration` access log (WebEx) was deleted.

HTTP Proxy

B#	Issue
226419	When a cached object is more than 4 GB in size, and the client request `Range: bytes=` header is greater than 4 GB, the HTTP proxy now delivers the data to the client within an expected time frame.

ICAP

B#	Issue
221834	The SSL access log now displays the `User-Agent` header field correctly when a virus-infected file is uploaded with `POST` or `PUT`, and ICAP is configured for `REQMOD`.
230031	Available ICAP services are no longer empty after accessing the **Response Analysis Service** VPM object.

Kernel

B#	Issue
228124	The appliance no longer stops responding due to hardware (I/O controller or disk) issues.

Policy

B#	Issue
233655	Installing VPM policy no longer times out.

Reverse Proxy

B#	Issue
227560	When policy includes the `http.request.detection.other.parameter_pollution_separator("")` property and the GET method retrieves data such as `GET /index.html?parm1=abc&parm1=def HTTP/1.1`, the appliance concatenates the `abc` and `def` parameters with no intervening characters. As a result, `abcdef` is analyzed as a unit. Previously, when parameter pollution policy included an empty string (" ") as the separator, the policy compiled to a comma (",") instead.

SSL/TLS and PKI

B#	Issue
234766	Google Chrome version 50 cannot access Google sites such as https://www.google.com and https://www.gmail.com when SSL proxy is enabled. For more information, refer to the Technical Alert at http://bluecoat.force.com/knowledgebase/articles/Technical_Alert/000031241.
234091	On an initial upgrade to version 6.6.4.x, if the default protocols (TLS 1,0, 1.1, and 1.2) for the HTTPS Console service were selected previously, only TLS 1.1 and 1.2 are selected by default now. If the HTTPS Console service's protocols were changed from the defaults previously, the selections do not change. **Note:** Any subsequent upgrades to 6.6.4.x, for example after a downgrade, do not change the protocol selections; the protocols selected prior to the subsequent upgrade are retained. On a downgrade to version 6.6.4.x, your selections do not change (whether you kept the default selections or changed them). On a new installation of version 6.6.4.x, ECDHE-RSA-RC4-SHA is disabled by default for SSL Client, SSL Device Profile, HTTPS Management Console, and HTTPS Reverse Proxy services; however, upgrading to this release does not disable the cipher by default.
232983	Weak ciphers and HMAC algorithms are no longer offered as defaults. If you have upgraded to this release from a previous 6.6.x version, issue the `# (config ssh-console)`**`ciphers reset`** and `#(config ssh-console)`**`hmacs reset`** commands to reset the default list. New installations do not require this step. **Note:** Although these weak ciphers and HMACs are still available for selection (they appear in the `choices` lists in CLI output), Symantec recommends that you issue the `reset` commands after an upgrade and use only strong ciphers and HMACs.

Storage

B#	Issue
227880	The ProxySG S200 platform no longer stops responding with an AHCI page fault.

TCP/IP and General Networking

B#	Issue
223570	The `#(config interface` *`number`*`)`**`half-duplex`** command now works as expected when interface settings are adjusted for a full-duplex 1 Gbps network.

URL Filtering

B#	Issue
224729	After an upgrade or downgrade, the Management Console now displays the lists of licensed components (**Maintenance > Health Monitoring > Licensing**) and subscription services (**Maintenance > Health Monitoring > Subscription**) correctly.

Web Application Firewall

B#	Issue
219649	When using Web Application Firewall (WAF) policy with multi-tenancy, the default tenant no longer has to reference a WAF property or gesture.

SGOS 6.6.3.2

Release Information

- **Release Date:** December 2, 2015
- **Build Number:** 177934

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x
- **Management Center:** 1.4.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:

  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.

- In this release, the Management Console, policy, and the command line include references to Application Attributes; however, you cannot enable the service or install related policy. This feature is unavailable until further notice.
- SSH security is improved in this release. As a result, your SSH client must be a current version that supports OpenSSH 6.7p1. Using an older client to connect to the SSH console reports an error. To continue using SSH connections, update your SSH client.

- External certificates imported in this release are not backward-compatible with previous 6.6.x releases. If you import external certificates in SGOS 6.6.3.2 or later, and then downgrade to an SGOS version earlier than 6.6.3.2, you must import the certificates again.

  After a downgrade, imported external certificates are subject to the 8000-byte limit.

See "New Features in SGOS 6.6.3.2" on the facing page for details on external certificate size in SGOS 6.6.3.2 and the SSH security improvement.

Changes in SGOS 6.6.3.2

- SGOS 6.6.3.2 introduces new features. See "New Features in SGOS 6.6.3.2" on the facing page.

Fixes in SGOS 6.6.3.2

- SGOS 6.6.3.2 includes the following fixes.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://bto.bluecoat.com/security-advisories

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

Limitations

- See "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in SGOS 6.6.x.

New Features in SGOS 6.6.3.2

SGOS 6.6.3.2 introduces the following new features.

WAF Block Exceptions

A property has been added to allow you to specify a built-in or user-defined exception message to return to the user when a Web Application Firewall (WAF) engine or property blocks a request:

`http.request.detection.exception(exception_id, details, format_string)`

where:

- *`exception_id`* is a built-in or user-defined exception
- *`details`* is a text string, enclosed within quotation marks, for the exception message
- *`format_string`* is text defined with define string and substituted for `$(exception.format)`

- Full information:
  Web Application Firewall Solutions Guide

Effective Date WAF Condition

The `effective_date=` condition has been added to allow you to control rule selection and usage based on the date that WAF rules were added. This ensures that rule behavior does not change from one update to the next of the Web Application Protection database. Use the condition to specify the set of WAF rules selected by the enclosing `define application_protection_set` definition. Symantec delivers WAF rule updates for the Blacklist and Analytics Filter engines through the Web Application Protection (WAP) subscription.

- Full information:
  ***Content Policy Language Reference* – Condition Reference**

  Web Application Firewall Solutions Guide

Managing Top-Level Domains

The appliance now allows you to add top-level domains to its internal suffix list to ensure that authentication cookies for top-level domains are handled correctly. To manage the list of top-level domains, in the Management Console, select **Configuration > Authentication > Top Level Domains**.

- Full information:
  ***SGOS Administration Guide* – Controlling Access to the Internet and Intranet**

Support for ECDHE Ciphers for Reverse Proxy

This release supports Elliptic Curve Diffie-Hellman Exchange (ECDHE) for Reverse Proxy, in both the SSL Client and Reverse Proxy service. ECDHE is also supported in the SSL Device Profile and the HTTPS Management Console. The following ECDHE ciphers were added:

- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-RC4-SHA

- Full information:
  ***SGOS Administration Guide* – Managing X.509 Certificates** and **Managing SSL Traffic**

SHA2 Default

SHA2 is now the default hash algorithm on the appliance. The Birth Certificate is also SHA2. The ProxySG appliance uses SHA2 when hashing for certificate creation, CSR creation, access-log signing, archive signing, and OCSP.

Support for Unified Agent

The appliance now acts as the client manager for both ProxyClient and Unified Agent deployments. To support this feature, the Management Console includes configuration options (**Configuration > Clients**) and statistics (**Statistics > Clients**) for Unified Agent.

Enhancements and Changes in SGOS 6.6.3.2

SGOS 6.6.3.2 also introduces the following enhancements and changes:

CVE Information in Block and Monitor Details Access Log Fields

- If you have a valid Web Application Protection subscription, the `x-bluecoat-waf-block-details` or `x-bluecoat-waf-monitor-details` fields in the `bcreporterwarp_v1` format (or other access log to which you added the fields) display the relevant CVE numbers in the format `""cve"":[""`*`<cve-number>`*`"",...]` when a request triggers a Blacklist engine rule that has CVE details.

Improved Block and Monitor Details Access Log Field Format

- The `x-bluecoat-waf-block-details` and `x-bluecoat-waf-monitor-details` field formats have been updated for improved readability. Log output for block details and monitor details comprises key-value pairs in the following format:

  ```
  [{"eng":"<engine>","part":"<part>","<optional_specifier>":
  "<optional_value>","data":"<data>"},{...}]
  ```

  The following is an example of the output:

  ```
  [{""eng"":""blacklist"",""part"":""query_arg"",""rule"":
  [""BL-4230-2""],""data"":""' or 1=1--""}]
  ```

New bcreporterwarp_v1 Access Log Field

- A new field, `x-bluecoat-transaction-uuid`, has been added to the bcreporterwarp_v1 access log format. With this field, Symantec Reporter performance improves when it indexes transaction identifiers for requests. In addition, the field is available as a substitution variable in policy and exception pages.

  Note: This field replaces `x-bluecoat-transaction-id` in the log format.

Unlimited Users with Web Application Protection License

- Starting in SGOS 6.6.3.2, the Web Application Protection license allows unlimited user connections; this applies to both new installations and upgrades. '

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

  In a reverse proxy deployment, if you have an existing valid Web Application Protection subscription and the service is enabled, the system does not enforce the user limit prescribed by the ProxySG appliance's base license. The system enforces the user limit if the subscription expires, you disable the service, or you downgrade SGOS.

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

SSH Security Improvements

- SSH cipher and HMACs support is updated when the appliance is in FIPS mode:
  - AES-CBC ciphers (aes128-cbc and aes256-cbc) are unsupported.
  - AES-GCM ciphers (aes128-gcm@openssh.com and aes256-gcm@openssh.com) are supported.
  - hmac-sha1-96 is unsupported.
  - hmac-sha2-256 and hmac-sha2-512 are supported.
- You can use new CLI commands to manage the SSH console ciphers and HMAC algorithms:
  - `#(config ssh-console)ciphers`
  - `#(config ssh-console)hmacs`

  Refer to the *ProxySG FIPS Mode WebGuide* and *Command Line Interface Reference* for details.

Unrestricted External Certificate Size

- SGOS no longer restricts the size of external certificates imported via the CLI or Management Console. You can now import external certificates larger than 8000 bytes in size; however, if you downgrade to a previous version of SGOS, the certificates must be re-imported and are subject to the size limit. For details, see "Upgrading To/Downgrading From This Release" on page 51.

> Imported external certificates not exceeding 8000 bytes are usable in 6.6.3.x. Imported external certificates exceeding 8000 bytes are not usable in 6.6.3.x. SGOS 6.5.8.1 and later also support imported external certificates over 8000 bytes.

Time and Volume Quotas Performance Improvement

- The impact on CPU utilization when user quotas are enabled is improved (though a performance impact still exists).

Updated Web Application Names and Operations

- Web application and operation names are updated periodically in the content filtering database. If you try to install policy that includes older web application/operation names, the appliance issues a deprecation message. When this occurs, replace the application/operation names in policy with the new ones specified in the deprecation message. If the deprecation message includes an expiration date, update your policy before that date.

Ability to Load Multiple Policy Files

- You can now load multiple policy files at once, excluding built-in policy source files, using the following command:

```
# load policy <space-separated-list>
```

Fixes in SGOS 6.6.3.2

SGOS 6.6.3.2 includes the following fixes:

Authentication

B#	Issue
221868	Health checks no longer report that an IWA Direct realm configured on the appliance is healthy even if it is offline.
221867	Kerberos authentication through IWA Direct no longer fails when an appliance is joined to a Windows Domain and has the same hostname as an existing appliance already joined to the domain.

Cache Engine

B#	Issue
221099	A watchdog restart in process group "PG_OBJECT_STORE" in process "CEA Disk 0xn-nnnnnnnn" no longer occurs when a ProxySG appliance with limited disk space stores large HTTP objects and access log files.

Hardware Drivers

B#	Issue
221219	The SSL accelerator slot number reported on **Maintenance > Systems and Disks > SSL Cards** is now correct.

ICAP

B#	Issue
220471	The appliance no longer stops processing traffic when a chunked object exists in cache and the OCS has been modified to return a `Content-Length` header for that object on subsequent requests.

Management Console

B#	Issue
221220	The size of the Licensed Components section (**Maintenance > Licensing > View**) has been fixed, making it easier to read licensing information.
221503	Selecting a keyring whose name includes spaces from the **Issuer Keyring** menu in the **Enable SSL Interception** VPM object no longer causes policy installation to fail.

Policy

B#	Issue
221464	Issuing the `#`**`restore-defaults keep-console`** command now removes tenant policies.

B#	Issue
219508	Issuing the `#(config)`**`policy reset tenant`** command now removes tenant and CachePulse policies.

Real Media Proxy

B#	Issue
221475	The RTSP Proxy now releases client sessions when requests are made to access a resource at a bad URL.

Reverse Proxy/Web Application Firewall

B#	Issue
220148	When multiple WAF detection engines match against a request, redundant entries no longer populate the `x-bluecoat-waf-attack-family` access log field.
221233	The event log no longer reports "Application Protection database purged" if you try to purge the database while the Application Protection service is enabled. To purge the database, you must first disable the service.

SNMP

B#	Issue
221475	An appliance with numerous open TCP connections no longer crashes if you perform an snmpwalk against it.

SSL Proxy

B#	Issue
220218	The Management Console lists FIPS ECLs correctly.
227885	When a client and OCS/server negotiate extended master secret TLS extension, the appliance no longer terminates the connection.

SSL/TLS and PKI

B#	Issue
218073	The SSL proxy can now intercept HTTP 2.0 connections.
220147	When you try to remove an HSM keyring that is not present in the HSM keygroup, and when the HSM keygroup has only one HSM keyring, the CLI now displays the expected message: `% HSM keyring <keyring_name> is not in this HSM keygroup`

Streaming

B#	Issue
222223	RTSP Proxy now releases client sessions when requests are made for malformed URL resources.

TCP/IP and General Networking

B#	Issue
221452	Issuing a `ping6` command no longer causes the appliance to stop responding.
220754	The appliance no longer experiences high CPU usage in TCP/IP when the number of connections is large (for example, more than 10,000) with any type of intercepted TCP traffic.
216553	In **Statistics > Network > Interface History** , the statistics of an aggregate interface now match the sum of statistics of all VLANs configured on the interface. See KB article 000028635 for details.
220966	Numerous "host" entries in a PCAP filter (**Proxy > Maintenance > Service Information > Packet Captures**) no longer increase the size of the filter's internal representation. When this issue occurred, it sometimes caused the appliance to stop responding.

Visual Policy Manager

B#	Issue
221851	You no longer have to select **Advanced Match** before you can complete the **Name** field in the **Request URL** object in the Visual Policy Manager.
221756	The **Name** field in the **WebEx Site** VPM object now accepts non-alphanumeric characters.

SGOS 6.6.2.3

Release Information

- **Release Date:** September 15, 2015
- **Build Number:** 169141

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x
- **Management Center:** 1.4.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x
- **ProxyClient:** 3.4.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Symantec Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

The following are the supported upgrade/downgrade paths for this release:

- Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
- Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

Any other upgrade or downgrade path is unsupported and could result in unexpected behavior.To avoid upgrade and downgrade issues, Symantec strongly recommends that you follow the tested upgrade procedure outlined in the *SGOS Upgrade/Downgrade Webguide:*

https://bto.bluecoat.com/webguides/upgrade_downgrade_sgos/Upgrade_Downgrade_SGOS.htm

For more information, please see the Blue Coat knowledge base article at http://bluecoat.force.com/knowledgebase/articles/Solution/000024130.

Changes in SGOS 6.6.2.3

- SGOS 6.6.2.3 has no new features.

Fixes in SGOS 6.6.2.3

- SGOS 6.6.2.3 includes the following fixes.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

https://bto.bluecoat.com/security-advisories

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

Limitations

- "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in SGOS 6.6.2.x.

Fixes in SGOS 6.6.2.3

SGOS 6.6.2.3 includes the following fixes.

Policy

B#	Issue
224036	User Quotas (time or volume) no longer cause the policy installation to fail when a User Quota action is applied to a rule with a User/Group source condition.
224858	The ProxySG appliance no longer experiences a page fault restart in HTTP or MMS (Microsoft Media Server) when the restrict DNS list is empty.

Serviceability

B#	Issue
224859	The appliance no longer experiences a software restart when debug statements are enabled in a release build.

URL Filtering

B#	Issue
221855	The appliance no longer fails to downgrade to SGOS releases prior to version 6.5.7.6.
223876	The appliance no longer experiences a watchdog restart in the Health Check component during an SGOS upgrade if the BCWF database is being upgraded.

Web Application Firewall

B#	Issue
224861	The appliance no longer experiences memory pressure while using Web Application Firewall (WAF).

SGOS 6.6.2.1

Release Information

- **Release Date:** August 4, 2015
- **Build Number:** 162765

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x
- **Management Center:** 1.4.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x
- **ProxyClient:** 3.4.x
- **ProxySG Appliances:**
  - S500, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 86 for links to platform documentation.

Third-Party Compatibility

For supported Java, operating system, and browser versions, refer to Symantec Knowledge Base article 000031300.

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:

  - Upgrade to SGOS 6.6.x from SGOS 6.5.7.6 or later.
  - Downgrade from SGOS 6.6.x to SGOS SGOS 6.5.7.6 or later.

  Any other upgrade or downgrade path is unsupported and could result in unexpected behavior. Symantec is aware of an issue (B#221855) related to downgrading; see "SGOS 6.6.x Known Issues" on page 74 for details.

  You can also refer to the Symantec Technical Alert for this issue:

  http://bluecoat.force.com/knowledgebase/articles/Technical_Alert/SGOS-6-6-2-1-downgrade-issue

  To avoid upgrade and downgrade issues, Symantec strongly recommends that you follow the tested upgrade procedure outlined in the *SGOS Upgrade/Downgrade Webguide:*

  https://bto.bluecoat.com/webguides/upgrade_downgrade_sgos/Upgrade_Downgrade_SGOS.htm

- In this release, the Web Application Protection layer in the VPM has been deprecated. After upgrading to this release, the deprecated layer might still appear in the generated CPL. To remove the layer completely, launch the VPM and click **Install Policy**. For further information, refer to the following Symantec Knowledge Base article:

  http://bluecoat.force.com/knowledgebase/articles/Solution/000029371

Important Note for Hybrid Cloud Customers

- Blue Coat recommends that Hybrid cloud customers upgrade to SGOS 6.6.2.1 only after Blue Coat Web Security Service (ThreatPulse) is updated to version 6.8.1.3. Running SGOS 6.6.2.1 with a previous ThreatPulse release causes policy compilation errors on the hybrid proxy, and the proxy cannot retrieve and install subsequent updates to common policy.

  Blue Coat currently plans to release Web Security Service 6.8.1.3 in August 2015; the release schedule could change, but you can verify that the service update has occurred when you receive an email notification from Blue Coat. After the service update, you must reactivate the common policy (in the ThreatPulse portal, select **Solutions > Content Filtering > Policy** and click **Activate**). Then, proceed with the upgrade to SGOS 6.6.2.1. Refer to the *Blue Coat Web Security Service Release Notes* and *SGOS Upgrade/Downgrade WebGuide* for additional release or upgrade details.

System Image and Bootchain Validation

SGOS 6.5.7.5 and later include a way for you to validate your SGOS system image and bootchain on the ProxySG appliance. After you upgrade to SGOS 6.5.7.5 or later, you can use the show installed-systems verbose CLI command to display the image signature. You can then compare the signature displayed for each release against a list of valid signatures posted on BlueTouch Online (BTO).

This method is available for the ProxySG 300, 600, 810, 900, 9000, S-Series, MACH5 VA, and SWG VA platforms. In addition, system image signatures for releases prior to SGOS 6.5 are not always displayed in the `show installed-system verbose` output. The signatures on BTO that you can use for comparison are available only for SGOS 6.5.x and later releases.

For more information, please see the Blue Coat knowledge base article at http://bluecoat.force.com/knowledgebase/articles/Solution/000024130.

Changes in SGOS 6.6.2.1

- SGOS 6.6.2.1 introduces new features. See "New Features in SGOS 6.6.2.1 " on the next page.

Fixes in SGOS 6.6.2.x

- Symantec is not listing fixes for this inaugural release in the 6.6.2.x software series.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://bto.bluecoat.com/security-advisories

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

Limitations

- "SGOS 6.6.x Limitations" on page 73 for a description of limitations in this release.

Known Issues

- See "SGOS 6.6.x Known Issues" on page 74 for a list of all issues that Symantec is aware of in SGOS 6.6.2.x.

New Features in SGOS 6.6.2.1

SGOS 6.6.2.1 introduces the following new features.

Intelligence Services Subscription Service

Intelligence Services is a framework for delivering existing and new data services to Symantec products. In addition to Blue Coat WebFilter (BCWF) web and security categorization, Intelligence Services subscriptions incorporate new subscription-based services like Threat Risk Levels and Geolocation for forward proxy.

Existing BCWF web and security categories are available in the Standard Intelligence Service offering. Threat Risk Levels and Geolocation for forward proxy are available in the Advanced Intelligence Service offering.

If you have a valid subscription, you can specify Intelligence Services as a data source on the appliance. In the Management Console, select **Configuration > Content Filtering > Blue Coat**.

ⓘ See "Enhancements and Changes in this Release " on page 69 for details on how using Intelligence Services as the data source can affect BCWF credentials data in the configuration archive.

- Full information:
  SGOS Administration Guide – Content Filtering

  Command Line Interface Reference – Standard and Privileged Mode Commands

Threat Risk Levels

Threat Risk Levels is an Intelligence Service. Threat Risk Levels indicate a requested URL’s potential risk by providing a numerical rating from 1-10 (with 1 indicating low level of risk and 10 indicating high level of risk), which you can reference when writing policy to protect your network and your users.

If you have a valid subscription, you can:

- Look up threat risks for a URL. In the Management Console, select **Configuration > Threat Protection > Threat Risk Levels**.
- Make policy decisions based on a URL's threat risk. Use the **Threat Risk** Visual Policy Manager (VPM) object or the `url.threat_risk.level=` condition in content policy language (CPL), where the value of `url` depends on the policy layer. Refer to the *Content Policy Language Reference* for syntax details.
- Override a URL's threat risk level. Use the **Set Effective Threat Risk Level** VPM object.
- View threat risk statistics over time. Select **Statistics > Threat Risk Details**.

- Full information:
  SGOS Administration Guide – Analyzing the Threat Risk of a URL

  Visual Policy Manager Reference – The Visual Policy Manager

  Content Policy Language Reference – Condition Reference

Geolocation for Forward Proxy

This release of SGOS supports geolocation in both reverse proxy and forward proxy deployments. You can:

- Determine the IP addresses to which a specified domain resolves, as well as the geographical location of each IP address. In the Management Console, select **Configuration > Geolocation > DNS Lookup**.
- Make policy decisions based on the geographical locations of the IP addresses that a domain resolves to. Use the **Resolved Country** VPM object or `supplier.country=` condition in CPL.

- Specify whether to allow access to IP addresses in all countries, no countries, or specific countries. If you allow connections to all countries or no countries in policy, you can optionally override that rule. Use the **Set Geolocation Restriction** VPM object or `supplier.allowed_countries()` property in CPL.

Geolocation for forward proxy is available as an Advanced Intelligence Service. Geolocation for Web Application Firewall Reverse Proxy is available in the Web Application Protections (WAP) subscription service.

- Full information:
  SGOS Administration Guide **– Geolocation**

  Visual Policy Manager Reference **– The Visual Policy Manager**

  Content Policy Manager Reference **–Condition Reference *and* Property Reference**

YouTube API v3 Support In This Release

In April 2015, Google discontinued YouTube Data API v2.0. As a result, Blue Coat categories for YouTube API v2 are not supported in SGOS 6.6.x.

Instead, you must specify a valid server key for the YouTube API v3 in order to use Blue Coat categories for YouTube. Set the server key and enable YouTube as a provider.

To obtain a key, log in to the Google Developers Console. In the console, create a project and generate the key. Refer to the following Blue Coat KB article for details:

https://bluecoat.force.com/knowledgebase/articles/Solution/000023564

This feature is provided on an "as-is" basis. Blue Coat has no control of, and is not responsible for, information and content provided (or not) by YouTube. Customer is required to apply and use its own API key in order to activate this feature, and therefore obligated to comply with all terms of use regarding the foregoing (for example, see https://developers.google.com/youtube/terms), including quotas, restrictions and limits on use that may be imposed by YouTube. Blue Coat shall not be liable for any change, discontinuance, availability or functionality of the features described herein.

Web Application Firewall for Reverse Proxy

In this release of SGOS , the appliance has enhanced web application firewall (WAF) capabilities to protect web applications from attacks. A major feature in this release is the addition of advanced detection engines. Also included is an improved ability to handle false positives; in addition to using pattern matching, the appliance can now determine if an attack was attempted:

- Based on *attack families*, which are types of common attacks.
- Using *advanced engines*, which distinguishes the languages and protocols used in families of attacks from legitimate, innocuous strings in requests.

  You can write CPL to take specific actions per engine.

- Using *Analytics Filter*, which detects attack characteristics and triggers intelligently based on the sum of the anomalies. This technology is based on attack signature matching with weights and thresholds.
- Using *blacklists*, which are based on an extensive database of attack signatures. The blacklists discover well-known attack patterns quickly and efficiently.

- This release has additional WAF changes:
  - Some CPL introduced in SGOS 6.5.x for web application protection has been updated.
  - New fields have been added to the `bcreporterwarp_v1` log format introduced in SGOS 6.5.x.
  - Some WAF features in the VPM introduced in SGOS 6.5.x have been deprecated.

- Full information:
  Web Application Firewall Solutions Guide

Content Policy Language Reference – Condition Reference

SGOS Upgrade/Downgrade WebGuide - Behavior Changes Applicable to SGOS 6.6.x Upgrade

Multi-Tenant Policy

Multi-Tenant Policy allows multiple distinct groups of users to enforce unique and common sets of policy while sharing the same appliance. This feature is supported in both forward and reverse proxy deployments, and you manage it solely from the Command Line Interface (CLI). Multi-tenant policy offers the following key benefits:

- Unique and global policies - Enforce unique policy for subsets of users while maintaining global policy for all users with a single VPM, local, central, and forwarding policy.
- Scalable policy - If your organization deploys multiple appliances and your user traffic is processed globally,you can install the same policy *criterion* and tenant policy on each appliance in the organization. Regardless of which appliance processes a user's traffic, they are always subjected to the same policy.

Enabling Multi-tenant policy automatically disables support for Blue Coat's Cloud/ProxySG appliance hybrid policy feature, Universal Policy.

As your appliance processes user requests, those requests are parsed for specific information (criterion) to determine if the user should be subjected to a specific tenant policy.

You require a separate license from Symantec to use multi-tenant policy. For details, refer to your Symantec Sales Engineer (SE).

- Full information:
  Multi-Tenant Deployment Guide

  Command Line Interface Reference – Privileged Mode Configure Commands

Integration with SafeNet Java HSM 3.x

The appliance supports integration with SafeNet Java HSM 3.x Hardware Security Module (HSM). An HSM provides additional security for storing cryptographic keys and certificates, which is required in some highly regulated industries. The appliance is able to use a network-attached HSM appliance to store private CA keys, and to perform digital signature operations.

- Full information:

  SGOS Administration Guide – Managing the SSL Proxy

Routing Domains

The Routing Domain feature allows you to segregate network interfaces into distinct groups that only allow traffic to be forwarded to one of the other interfaces in that group. Routing Domain configurations include distinct routing and gateway details. Manage this feature solely from the CLI.

- Full information:
  Creating Multiple Logical Networks on a Single ProxySG Appliance with Routing Domains

Link Aggregation

Use the Link Aggregation feature to bundle multiple physical interfaces into one logical aggregate interface. This allows increased throughput and network resiliency. Link aggregation is accomplished using the industry-standard IEEE 802.1AX Link Aggregation standard. Switch support and switch configuration are required.

- Full information:
  SGOS Administration Guide – Configuring Adapters and Virtual LANs

Command Line Interface Reference – Privileged Mode Configure Commands

Interface Shutdown

In SGOS versions prior to 6.6.2.1, a ProxySG appliance interface comes up whenever an Ethernet cable is connected to it. For additional security, you can now disable any interface not actively in use.

- Full information:
  SGOS Administration Guide – Configuring Adapters and Virtual LANs

  Command Line Interface Reference – Privileged Mode Configure Commands

WebEx Proxy

The WebEx proxy provides fine control over WebEx desktop and file sharing operations. For example, it can be configured to allow a user to attend a meeting, but restrict the user from sharing a file, hosting a meeting, or sharing the desktop.

- Full information:
  SGOS Administration Guide – Managing the WebEx Proxy

Adobe RTMP VOD Pre-Population

Pre-population of RTMP Flash content is supported. The appliance supports pre-population of dynamically streaming files from the RTMP protocol family from OCSes (that is, streaming Flash servers).

- Full information:
  SGOS Administration Guide – Managing Streaming Traffic

  Command Line Interface Reference – Privileged Mode Configure Commands

User Quotas

You can limit user access to the Internet by creating policy for:

- Time quotas - Limit the amount of time that users can spend on the Internet or Internet resource during a specific period of time.
- Volume quotas - Limit users' Internet or Internet resource usage during a specific period of time.

Before you can install policy to set user limits, you must enable the quota library in the CLI. Issue the following command:

```
#(config)policy quota
```

To create time and volume quotas, use the **Time Quota** and **Volume Quota** objects in the VPM.

Enabling user quotas might have a performance impact on CPU utilization.

- Full information:
  SGOS Administration Guide – Filtering Web Content

  Visual Policy Manager Reference – The Visual Policy Manager

  Command Line Interface Reference – Privileged Mode Configure Commands

Integration with Security Analytics Platform

The appliance includes an access log format to support integration with the Security Analytics Platform. You can configure the new `bcsecurityanalytics_v1` log format to send appropriate log entries to the Security Analytics Platform. This log format is available in the Management Console in **Configuration > Access Logging > Formats**.

- Full information:
  ***SGOS Administration Guide* – Creating Custom Access Log Formats**

  Security Analytics Platform documentation:

  https://bto.bluecoat.com/documentation/All-Documents/Security%20Analytics%20Platform

Support for Apache Kafka

You can use Kafka as a new access log upload client to upload logs from the appliance to Symantec Reporter or Symantec Hosted Reporting Service (available soon in the Symantec Web Security Service). The logs are relayed to a cluster of one or more servers over a mutually authenticated channel.

To use Apache terminology, the appliance is the *producer*, Reporter/Hosted Reporting Service is the *consumer*, and the cluster of servers is the *broker*.

To use Kafka as the upload client:

- The appliance must be able to access the Kafka broker.
- The Reporter/Hosted Reporting Service server must be available.

- Full information:
  ***SGOS Administration Guide* – Configuring the Upload Client**

  For more information on Kafka concepts and terminology, refer to Apache documentation:

  http://kafka.apache.org/documentation.html

SAML Attribute Forwarding

You can forward SAML attributes (including the user name) in SAML 2.0 assertions through HTTP headers to front-end or back-end servers. The attribute value is rewritten using the following substitution:

`$(saml.attribute.<name>)`

You can create request header rewrite policy to forward SAML attribute values in headers if the attribute value matches the specified condition. Use the **SAML Attribute** VPM object or the `saml.attribute.saml_attribute_name=` condition in CPL.

- Full information:
  ***SGOS Administration Guide* – SAML Authentication**

  ***Visual Policy Manager Reference* - The Visual Policy Manager**

  ***Content Policy Language Reference* – Condition Reference**

Authentication Monitoring and Logging Enhancements

Integrated Windows Authentication (IWA) Latency Logging

Transaction-based access log fields are set during NTLM authentication (over the schannel connection):

- `x-server-auth-time` : The time in milliseconds that it took to perform the authentication
- `x-auth-server-name` : The DNS name of the domain controller to which the schannel is connected

- Full information:
  SGOS Administration Guide – Access Log Formats

Integrated Windows Authentication (IWA) Domain Refresh

A CLI subcommand initiates a refresh of the domain trust information from Active Directory:

```
#(config windows-domains)edit <domain name>
```

```
#(config windows-domains <domain name>) refresh-trusts
```

Event logs include output from the domain trust enumeration.

- Full information:
  Command Line Interface Reference – Privileged Mode Configure Commands

Integrated Windows Authentication (IWA) Groups Display All

New CLI subcommands allow you to perform test authentication and:

- Display up to 20 groups in a specified realm:

  ```
  #(config iwa-direct <realm name>) test-authentication
  ```

- Display all groups in a specified realm:

  ```
  #(config iwa-direct <realm name>) test-authentication-show-all
  ```

- Full information:
  Command Line Interface Reference – Privileged Mode Configure Commands

Enhancements and Changes in this Release

This release also includes the following:

IPv6 Support in Attack Detection

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

Set Application Name in Policy and Access Log Fields

You can set a custom name for the application associated with a URL. This value of this property populates the WebPulse access log field `x-bluecoat-application-name` when traffic matches and access logging is enabled.

```
<proxy>
url.domain=company.com application.name(<app_name>)
```

where <*app_name*> is the application name.

Simplified Policy Trace

The **Trace** object in the Visual Policy Manager allows you to either fully disable or fully enable tracing. The intermediate levels (request tracing and rule/request tracing) have been removed.

In addition, the corresponding `trace.rules()` property has been deprecated. If you specified request, rule/request, or verbose tracing in policy before upgrading to SGOS 6.6.2.x, after the upgrade tracing is enabled.

Deny Policy

A new Web Request Layer has been added to the Visual Policy Manager. It supports new `Deny` objects which allow you to block outgoing requests and outbound application operations.

New Policy Subcommands

The following subcommands are new in this release:

```
# show policy config
```

```
# show policy executable
```

```
# show policy source
```

```
# show policy tenant
```

Health Monitoring

Health metrics for new and existing subscription services (such as Geolocation, Intelligence Services, and Application Protection) are available on new tabs in the Management Console.

- To view the services' communication status, select **Statistics > Health Monitoring > Subscription**.
- To configure notification methods for each metric, select **Maintenance > Health Monitoring > Subscription**.

The CLI command `#(config) alert` has a new subcommand to support subscription health monitoring. Use the following command to set the notification type, or disable notification, for *all* subscription services:

```
#(config) alert notification subscription communication-status {email | log | trap
| none}
```

Subscription License Support

A CLI command allows you to configure and view download settings:

```
#(config subscription-license) {download|view}
```

Blue Coat WebFilter Username/Password in Configuration Archive

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

WebPulse Enhancement

WebPulse configuration has changed. **Use secure connections** is no longer an option; starting in SGOS 6.6.2.x, WebPulse always uses secure connections.

Management Console Appliance Key

The appliance keyring is updated to a SHA-256 certificate with 2048-bit RSA encryption on upgrade to SGOS 6.6.2.x. A new read-only Blue Coat appliance CA certificate list (CCL) called `bluecoat-appliance` will also be created which trusts only Blue Coat appliance keys. The appliance will automatically switch the configuration over from using the original `appliance-ccl` to using the new `bluecoat-appliance` CCL if the `appliance-ccl`l was not modified by the customer. Otherwise, the`bluecoat-appliance` CCL is created, but the appliance customers' use of the `appliance-ccl` will remain unaffected.

Appliance Identifier

You can identify the appliance for a given log entry. Display the compact identifier of the appliance through the new CLI command:

```
>show appliance-identifier
```

The appliance identifier is the same as the value returned in the access log and policy substitution `x-bluecoat-appliance-identifier`.

Management Console Enhancement

The look and feel of the ProxySG appliance Management Console has been updated.

Monitoring Support for Unified Agents and ProxyClients

On the **Statistics** and **Configuration** tabs in the Management Console, **ProxyClient** labels have been renamed to **Clients** to accommodate both types of remote client (Unified Agent and ProxyClient). A separate **Active Unified Agents** screen is available for client histories, and the **Client Details** now display a **Type** column that identifies the remote client. For details, refer to the *ProxyClient Administration and Deployment Guide*.

External Certificate List

You can define an external certificate list and select it in the SAML realm.

SGOS 6.6.x Reference Information

The following sections provide reference and compatibility information for the SGOS 6.6.x software series.

- "SGOS 6.6.x Limitations" on the next page
- "SGOS 6.6.x Known Issues" on page 74
- "ProxySG Appliance Resources" on page 86
- "Documentation and Other Self-Help Options" on page 87

SGOS 6.6.x Limitations

Symantec is aware of the following limitations. These are issues that are not fixable because of an interaction with third-party products or other reasons, or they are features that work as designed but might cause an issue.

Authentication

The CLI might display the following message when you issue the **`rejoin`** command to re-join the appliance to the Windows domain:

```
#(config security windows-domains)rejoin<domain_alias> <name> <password>
```

```
% The password is incorrect for the given account
```

The CLI responds with the message if you attempt a rejoin soon after using the **`join`** or **`rejoin`** command to join the appliance to the same domain before all domain controllers (DCs) have synchronized. If this occurs, allow time for all DCs to synchronize and attempt the rejoin again.

HTTP 500 "Internal Error" Responses to CRL or OSCP Requests

Users receive HTTP error 500 code "internal error" responses to CRL or OSCP requests. The behavior occurs because some cache objects have an incorrect ICAP status. The behavior does not occur if policy is installed to bypass caching.

To work around this limitation, delete the cache objects for specific sites. Issue one of the following CLI commands:

```
#(config)content delete regex <regular_expression>
```

```
#(config)content delete url <URL
```

SCP Access Log Upload

- Access log file uploads through SCP can be periodic only; continuous upload is not supported.
- As of version 6.6.5.400, SCP supports gzip file uploads only.

SGOS 6.6.x Known Issues

Symantec is aware of the following issues in SGOS 6.6.x.

Access Logging

B#	Issue Workaround (if available)	Fixed In (when applicable)
219640	The output for the `#show configuration` command does not indicate that `collaboration` access log (WebEx) was deleted. If you delete the log, the output should show output such as `delete log collaboration`.	"Fixes in SGOS 6.6.4.1" on page 48
237171	The CLI command `#(config captcha <realm_name>) virtual-url <string>` should accept strings only in valid virtual-URL format.	

ADN

B#	Issue Workaround (if available)	Fixed In (when applicable)
213090	The ProxySG appliance shows some degradation in ADN performance.	

Authentication

B#	Issue Workaround (if available)	Fixed In (when applicable)
221868	Health checks report that an IWA Direct realm configured on the appliance is healthy even if it is offline. In addition, event logs indicate correctly that the domain is offline.	"Fixes in SGOS 6.6.3.2" on page 56
221867	If an appliance is joined to a Windows Domain and has the same hostname as an existing appliance already joined to the domain (usually a result of using the same configuration without changing the hostname), Kerberos authentication through the IWA Direct realm fails. The authentication failures occur because the two appliances are modifying the same machine account object in Active Directory, resulting in the machine account password becoming unsynchronized. This invalid configuration exposes a small memory leak.	"Fixes in SGOS 6.6.3.2" on page 56
233608	The appliance might experience high CPU in LSA and OpenLDAP when there is no user load.	"Fixes in SGOS 6.6.4.3" on page 34
232841	In a hybrid LDAP/WinSSO configuration, issues occur following LDAP client referrals.	"Fixes in SGOS 6.6.4.3" on page 34

Boot

B#	Issue Workaround (if available)	Fixed In (when applicable)
228694	VMWare Fusion 8 Pro is not a supported platform for the ProxySG Secure Web Gateway Virtual Appliance.	"Fixes in SGOS 6.6.4.1" on page 48
237711	**Issue**: If a boot loader has multiple copies of the same system image and one of those images is corrupted, the boot loader might incorrectly mark all of the system images as "Failed". **Workaround**: Use the starter or CLI to manually select the image you want to boot.	

CLI Console

B#	Issue Workaround (if available)	Fixed In (when applicable)
236048	The `show failover` command shows an internal message in output.	"Fixes in SGOS 6.6.4.3" on page 34

Client Manager

B#	Issue Workaround (if available)	Fixed In (when applicable)
234815	The appliance returns an error when an administrative user attempts to upload the updated version of Unified Agent client software to the appliance via the "Local File" option.	"Fixes in SGOS 6.6.5.1" on page 26
235987	You cannot manage Unified Agent from the ProxySG Management Console.	"Fixes in SGOS 6.6.4.3" on page 34

Hardware Drivers

B#	Issue Workaround (if available)	Fixed In (when applicable)
221219	The SSL accelerator slot number reported on **Maintenance > Systems and Disks > SSL Cards** is incorrect.	"Fixes in SGOS 6.6.3.2" on page 56
230512	**Issue:** The ProxySG Virtual Appliance MACH 5 Edition now supports increased VM memory sizes; however, an upgrade to this release on the SGVA-5-M5 platform fails unless you perform the following workaround. **Workaround:** Perform the following steps: 1. Update the license key using the CLI command: `#licensing update-key` 2. Set the VM memory to 2048 MB (2 GB). 3. Upgrade to version 6.6.4.x. **Note:** Symantec recommends increasing the memory sizes for other platforms, but doing so is not a requirement in order to upgrade to this release. For details, see "Upgrading To/Downgrading From This Release" in "SGOS 6.6.4.1" on page 40	

B#	Issue Workaround (if available)	Fixed In (when applicable)
231271	Creating a Hyper-V virtual machine with more than 8 GB of memory results in a crash.	

Health Checks

B#	Issue Workaround (if available)	Fixed In (when applicable)
232047	Occasionally the WebPulse service is not able to recover automatically when it gets into a state where all of the services are reporting that they are sick. This results in the following event log message: `Dynamic categorization error: No service specified to use.`	

HTTP Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
226419	When a cached object is more than 4 GB in size, and the client request `Range: bytes=` header is greater than 4 GB, the HTTP proxy might take longer than expected to deliver the data to the client.	"Fixes in SGOS 6.6.4.1" on page 48
231925	When clients use FTP over HTTP, the appliance might incorrectly add an extra `%` character to the URI in the HTML `<BASE>` tag.	"Fixes in SGOS 6.6.4.3" on page 34
235674	The CLI console and Management Console do not accept a `max-cache-size` larger than 32256 MB.	"Fixes in SGOS 6.6.4.3" on page 34

246166	**Issue:** YouTube is throwing a transformation error.
	Workaround: Include one of the following in policy:
	`define action ForceUncompressedResponse`
	`delete(request.header.Accept-Encoding)`
	`end`
	`<Cache>`
	`url.domain=youtube.com`
	`     action.ForceUncompressedResponse(yes)`
	
	`define action remove_brotli`
	`iterate(request.header.Accept-Encoding)`
	`          iterator.exact = "br" iterator.delete()`
	`      end`
	`end`
	`<Proxy>`
	`action.remove_brotli(yes)`	

ICAP

B#	Issue Workaround (if available)	Fixed In (when applicable)
220471	The ProxySG appliance might stop processing traffic when a chunked object exists in cache and the OCS has been modified to return a `Content-Length` header for that object on subsequent requests. This issue can occur when ICAP mirroring is enabled.	"Fixes in SGOS 6.6.3.2" on page 56
221834	The SSL access log does not display the `User-Agent` header field correctly when a virus-infected file is uploaded with `POST` or `PUT`, and ICAP is configured for `REQMOD`.	"Fixes in SGOS 6.6.4.1" on page 48
230031	Available ICAP services are empty after an upgrade to SGOS 6.6.3.2. This occurs after accessing the **Add/Edit Response Analysis Service** VPM object.	"Fixes in SGOS 6.6.4.1" on page 48
235674	The appliance experiences a hardware restart at `0xe` in process group `PG_HTTP` when doing REQMOD scanning.	"Fixes in SGOS 6.6.4.3" on page 34

Kernel

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

243790	The ProxySG appliance may experience a watchdog restart in process `kernel.exe` when policies such as the following are in use:
	`<proxy>`
	`url.regex="-://-//" access_log(no)`
	Symantec recommends the following change:
	`<proxy>`
	`url.subtring="-://-//" access_log(no)`	

228124	The appliance stops responding due to hardware (I/O controller or disk) issues.	"Fixes in SGOS 6.6.4.1" on page 48

Management Console

B#	Issue Workaround (if available)	Fixed In (when applicable)
219234	**Issue:** The **Statistics > Application Details > Application History** tab displays traffic for <Unidentified> applications by default even though the **Select an application** menu has an application selected. **Workaround:** Select another application in the menu for the **Application History** tab to display accurate statistics.	
221220	The size of the Licensed Components section (**Maintenance > Licensing > View**) makes it difficult to read licensing information.	"Fixes in SGOS 6.6.3.2" on page 56
221503	Selecting a keyring from the **Issuer Keyring** menu in the **Enable SSL Interception** VPM object causes policy installation to fail. This issue occurs if the keyring name includes spaces.	"Fixes in SGOS 6.6.3.2" on page 56
217492	When you manually configure link settings for a link aggregation member interface, the dialog provides an option to select **Half** under **Link Settings**. Half-duplex is not available for aggregate interfaces.	
217732	**Issue:** A link aggregation member interface might display an incorrect state after you delete an aggregate link. **Workaround:** To display the correct link state, refresh the Management Console page in the browser.	
243995	**Issue:** When entering a new appliance name (**Configuration > General > Identification**), clicking **Preview** applies the name change. **Workaround:** Do not click **Preview**.	

MAPI Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
235747	When the appliance removes attachments from received e-mail, and the message body is HTML, the attachment removal description is appended in UTF-16 instead of UTF-8.	"Fixes in SGOS 6.6.4.3" on page 34

B#	Issue Workaround (if available)	Fixed In (when applicable)
235584	ICAP response headers that the appliance sends to the ICAP server are incorrect.	"Fixes in SGOS 6.6.4.3" on page 34
225510	The **Active Sessions** window does not indicate that ICAP scanning is in progress.	"Fixes in SGOS 6.6.4.3" on page 34
235531	Access logs sometimes do not display the `message-id` for received messages.	"Fixes in SGOS 6.6.4.3" on page 34

Performance

B#	Issue Workaround (if available)	Fixed In (when applicable)
213090	As a result of some internal scheduling changes, ADN performance is lower on some platforms relative to SGOS 6.5.x.	
226241	High CPU utilization is reported when simultaneously intercepting WebEx traffic and downloading categorization or Threat Risk databases.	
234568	Higher DNS utilization occurs under heavy load conditions. This was discovered in some internal performance tests.	

Policy

B#	Issue Workaround (if available)	Fixed In (when applicable)
221464	Issuing the `#restore-defaults keep-console` command does not remove tenant policies.	"Fixes in SGOS 6.6.3.2" on page 56
219508	Issuing the `#(config)policy reset tenant` command does not remove tenant or CachePulse policies.	"Fixes in SGOS 6.6.3.2" on page 56
235181	When the appliance is deployed transparently, and SSL traffic is intercepted, trust-destinationIP policy does not work as intended if the IP address of the SSL site is modified.	"Fixes in SGOS 6.6.5.2" on page 17
235815	Incorrect URL encoding can cause content filtering to report the wrong category when both local policy categorization and an external categorization engine are in use. This issue is restricted to URLs that contain special characters, such as spaces.	"Fixes in SGOS 6.6.4.3" on page 34
236676	**Issue:** Disabling multi-tenant policy without first clearing tenant policy causes the appliance to stop logging the request body although `http.request.log_details(header,body)` exists in policy. **Workaround:** Re-enable multi-tenancy, clear the tenant and landlord policy files, and disable multi-tenancy again.	

<table>
<tr><th>B#</th><th>Issue
Workaround (if available)</th><th>Fixed In
(when applicable)</th></tr>
<tr><td>234634</td><td>
<p>When multitenant policy exists, the <code>http.request.body.inspection_size()</code> property setting for the default tenant is always in effect, even if non-default tenants have different settings for the property. For example, if tenant A's body inspection size is 12 KB and the default tenant's is 10 KB, a request body size of 11 KB triggers an inspection even if tenant A's policy applies to the transaction. When this issue occurs, however, tenant A's <code>http.request.detection.other.threshold_exceeded()</code> setting is respected and applies correctly to the transaction.</p>
<p>Consider the following example:</p>
<pre>
; default tenant policy
; inspect up to 10 KB of the HTTP request body
; monitor requests larger than 10 KB
<Proxy>
 http.request.body.inspection_size(10000) \
   http.request.detection.other.threshold_exceeded(monitor)

; tenant A policy
; inspect up to 12 KB of the HTTP request body
; block requests larger than 12 KB
<Proxy>
 http.request.body.inspection_size(12000) \
   http.request.detection.other.threshold_exceeded(block)
</pre>
<p>Given these rules:</p>
<ul>
<li>A request that is subject to tenant A policy and with body size of 11 KB should be inspected in its entirety and not blocked. The request body’s first 10 KB are inspected and the request is blocked.</li>
<li>A request that is subject to tenant A policy and with body size of 13 KB should be inspected up to the first 12 KB and blocked. The request body’s first 10 KB are inspected and the request is blocked.</li>
</ul>
</td><td></td></tr>
</table>

Real Media Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
221475	RTSP Proxy does not release client sessions when requests are made to access a resource at a bad URL.The issue occurs when there is continuous and repeated access to the URL, resulting in a buildup of client workers.	"Fixes in SGOS 6.6.3.2" on page 56

Reverse Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
221233	The event log inaccurately reports "Application Protection database purged" if you try to purge the database while the Application Protection service is enabled. To purge the database, you must first disable the service.	"Fixes in SGOS 6.6.3.2" on page 56
227560	When parameter pollution policy includes an empty string (" ") as the separator, the policy compiles to a comma (",") instead.	"Fixes in SGOS 6.6.4.1" on page 48

SNMP

B#	Issue Workaround (if available)	Fixed In (when applicable)
221475	An appliance with numerous open TCP connections might crash if you perform an snmpwalk against it.	"Fixes in SGOS 6.6.3.2" on page 56
240320	The appliance experiences a watchdog restart in the SNMP subsystem in environments with more frequent connection drops.	

SOCKS Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
235707	Only one remote session can be established using SOCKS client.	"Fixes in SGOS 6.6.4.3" on page 34

SSL Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
220528	**Issue:** If you remove external certificates from the external certificate list (ECL) and then delete those external certificates through the Management Console, the ECL state becomes inconsistent on the appliance. **Workaround:** Remove the external certificates from the ECL and apply the changes. Then, delete the external certificates.	
220218	The Management Console incorrectly lists FIPS ECLs as non-FIPS ECLs.	"Fixes in SGOS 6.6.3.2" on page 56
225794	#**`show config`** output does not enclose the `issuer-keyring` name in quotation marks. When the name includes spaces, subsequent attempts to apply the saved configuration fail.	
225612	When you change the SSL protocol version for a SSL device profile, the appliance selects compatible ciphers from the list of previously selected ciphers instead of selecting all the available ciphers for the new SSL protocol version.	
227420 224017	**Issue:** Some versions of Blue Coat Director and Symantec Management Center cannot connect to an appliance running in FIPS mode. **Workaround:** Connect to an appliance running 6.6.3 (or later) in FIPS mode and change the ciphers available. This can be done via the CLI as follows: #**`en`** #**`conf t`** `#(config)`**`ssh`** `#(config ssh-console)` **`ciphers set aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr`**	
229635	HSM hostnames do not permit the hyphen character even though it is a valid hostname character.	"Fixes in SGOS 6.6.4.3" on page 34

B#	Issue Workaround (if available)	Fixed In (when applicable)
224906	In a reverse proxy deployment, when the origin content server (OCS) downgrades TLS versions or multiple servers with different TLS versions are load-balanced, some SSL connections are dropped.	"Fixes in SGOS 6.6.4.3" on page 34
232907	Certificate cache collisions occur due to cache handling of multiple emulated certificates with the same common name, increasing CPU utilization. In addition, if the appliance cannot reach an OCS, it generates an emulated certificate with 30-day validity to present an exception page to the client. If the appliance accesses the OCS every two hours, it continues to serve the cached emulated certificate even after expiration.	"Fixes in SGOS 6.6.4.3" on page 34

SSL/TLS and PKI

B#	Issue Workaround (if available)	Fixed In (when applicable)
218073	The appliance SSL proxy cannot intercept HTTP 2.0 connections.	"Fixes in SGOS 6.6.3.2" on page 56

220147	When you try to remove an HSM keyring that is not present in the HSM keygroup, and when the HSM keygroup has only one HSM keyring, the CLI displays an inaccurate message:
	`% Keygroup is in use and the last member may not be removed.`
	The CLI should display the following message instead:
	`% HSM keyring <keyring_name> is not in this HSM keygroup`
		"Fixes in SGOS 6.6.3.2" on page 56

221218	A newly-created certificate displays "Not yet valid" for **Certificate expiry** (**Configuration > SSL> Keyrings**). This issue occurs when the ProxySG appliance's clock is ahead of the clock on the client running the Management Console.	
220453	If you issue the `#(config ssl)create signing-request` command and the certificate signing request fails, issuing the command again causes CLI to stop responding.	
232551	The **Client Negotiated Cipher** and **Server Negotiated Cipher** VPM objects do not list all of the appliance's supported cipher values.	"Fixes in SGOS 6.6.4.3" on page 34
225612	When changing the SSL protocol version for an SSL device profile, the appliance selects compatible ciphers from the list of previously-selected ciphers instead of the list of all available ciphers.	
235232	In Windows, the Management Console does not load with Java 7 unless TLS 1.0, TLS 1.1, and TLS 1.2 are all selected in the Java Control Panel (**Java > Advanced Settings > Advanced Security Settings**).	"Fixes in SGOS 6.6.4.3" on page 34

Storage

B#	Issue Workaround (if available)	Fixed In (when applicable)
227880	The ProxySG S200 platform sometimes stops responding with an AHCI page fault. This occurs when a drive or the controller returns an NCQ error.	"Fixes in SGOS 6.6.4.1" on page 48
236541	On the SG-S500 platform, the CLI reports a message, "SCSI: Mode selector page 8" while SGOS is loading.	"Fixes in SGOS 6.6.5.1" on page 26

TCP/IP and General Networking

B#	Issue Workaround (if available)	Fixed In (when applicable)
244691	The appliance may experience high CPU utilization with form-based authentication.	"Fixes in SGOS 6.6.5.8" on page 4
221452	Issuing a `ping6` command might cause the ProxySG appliance to stop responding.	"Fixes in SGOS 6.6.3.2" on page 56
220754	The ProxySG appliance might experience high CPU usage in TCP/IP when the number of connections is large (for example, more than 10,000) with any type of intercepted TCP traffic.	"Fixes in SGOS 6.6.3.2" on page 56
216553	On the **Statistics > Network > Interface History** tab, the statistics of an aggregate interface do not match the sum of statistics of all VLANs configured on the interface. This issue only affects link aggregation interfaces.	"Fixes in SGOS 6.6.3.2" on page 56
220966	Numerous "host" entries in a PCAP filter (**Maintenance > Service Information > Packet Captures**) can greatly increase the size of the filter's internal representation, which in turn might cause the appliance to stop responding.	"Fixes in SGOS 6.6.3.2" on page 56
223570	The `#(config interface` *`number`*`)`**`half-duplex`** command does not work when interface settings are adjusted for a full-duplex 1 Gbps network. In this case, the command inaccurately responds `OK` and the interface link status (as shown in `#`**`show interface`** *`number`* output) reverts to the original mode after a few seconds of mode negotiation.	"Fixes in SGOS 6.6.4.1" on page 48
228663	You cannot use an aggregate interface in a WCCP configuration.	

URL Filtering

B#	Issue Workaround (if available)	Fixed In (when applicable)
235815	URL filtering might not match correctly when the following conditions exist: • The request URI includes one or more spaces. • Policy includes a local category definition.	"Fixes in SGOS 6.6.4.2" on page 39
221855	An attempt to downgrade from SGOS 6.6.2.1 to any 6.5.x release up to and including 6.5.7.5 fails and the appliance stops responding. If your appliance is in this state, you must power cycle it (detach and re-attach the power cables) in order to reboot.	"Fixes in SGOS 6.6.2.3" on page 61
224279	Licensed components (**Maintenance > Health Monitoring > Licensing**) include a "??? Expiration" item and the list of subscription services (**Maintenance > Health Monitoring > Subscription**) includes an empty line. This occurs after an SGOS upgrade or downgrade.	"Fixes in SGOS 6.6.4.1" on page 48
229395	When you cancel a BCWF database download, you receive an error "Download failed" instead of "Download canceled".	"Fixes in SGOS 6.6.4.3" on page 34
229493	Despite the Application Attribute controls being present the backend data is not available at this time. Once the data is made available this feature will work.	"Fixes in SGOS 6.6.5.2" on page 17
229692	If a backend database service is unavailable, canceling a download does not complete until the network timeout is reached. This could take several minutes to complete.	

B#	Issue Workaround (if available)	Fixed In (when applicable)
232481	**Issue:** When WebPulse is configured to perform dynamic categorization in the background, it might report an incorrect category of "None" instead of "Pending", which could cause unexpected results during policy evaluation. **Workaround:** Configure WebPulse to perform dynamic categorization immediately (in real time) instead of in the background.	
231923	When downgrading to SGOS 6.5 and earlier, an error message "% cannot use forwarding when Secure is enabled" occurs if a forwarding host is configured for the WebPulse connections.	"Fixes in SGOS 6.6.4.3" on page 34
232047	**Issue**: Occasionally the WebPulse service is not able to recover automatically when it gets into a state where all of the services are reporting that they are sick. This results in the following event log message, "Dynamic categorization error: No service specified to use." **Workaround**: Disable and re-enable the WebPulse service.	
237090	After upgrading from SGOS 6.5.x to 6.6.x, the CLI command to enable secure mode for dynamic categorization is unavailable.	

Visual Policy Manager

B#	Issue Workaround (if available)	Fixed In (when applicable)
221851	When you create or edit a **Request URL** object in the Visual Policy Manager, you have to select **Advanced Match** before you can complete the **Name** field.	"Fixes in SGOS 6.6.3.2" on page 56
221756	The **Name** field in the **WebEx Site** VPM object does not accept non-alphanumeric characters.	"Fixes in SGOS 6.6.3.2" on page 56

Web Application Firewall

B#	Issue Workaround (if available)	Fixed In (when applicable)
219649	When using Web Application Firewall (WAF) policy with multi-tenancy, the default tenant must reference at least one WAF property or gesture.	"Fixes in SGOS 6.6.4.1" on page 48
220148	When multiple WAF detection engines match against a request, redundant entries might populate the `x-bluecoat-waf-attack-family` access log field.	"Fixes in SGOS 6.6.3.2" on page 56
235642	HTTP request buffer corruption interferes with header parsing.	
219153	When the Application Protection service is disabled and the subscription is expired, loading associated policy does not generate policy warnings.	
235862	Tolerate request parsing can cause invalid request headers to be passed to WAF, which results in a software restart.	"Fixes in SGOS 6.6.4.3" on page 34
236633 236772	CLI command `#show policy executable` output includes unexpected text `UNIMPL-ACT` and `UNIMPL-ACT`. This has no effect on the operation of policy.	

ProxySG Appliance Resources

ProxySG appliances run the SGOS operating system. This page provides information about supported platforms for this release and where to go for additional hardware information and procedures. SGOS 6.6.x is not supported on any platform not listed here.

Platforms	Resources	Comments
SG-S500	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG-S500	
SG-S400	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG-S400	
SG-S200	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG-S200	
SG300	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG300	
SG600	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG600	
SG900	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG900	
SG9000	https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SG9000	Not supported for 9000-5, 9000-10, or 9000-20 (9000-20B is supported)
VA MACH5 Edition	https://bto.bluecoat.com/documentation/proxysg-va-mach5-edition-initial-configuration-guide	
VA SWG Edition	https://bto.bluecoat.com/documentation/secure-web-gateway-va-initial-configuration-guide	

Additional Resources

Subject	Resources	Comments
Diagnostics	https://bto.bluecoat.com/webguides/hardware/maintenance_upgrade_webguide/Maintenance_Upgrade_WebGuide.htm#02Tasks/Troubleshooting/Getting_Started.htm	

Documentation and Other Self-Help Options

Symantec provides technical and solution documentation in different formats. This section provides a resource locator as well as a record of documentation changes.

SGOS 6.6.x Product Documentation

- Search for PDFs and WebGuides at:

  https://bto.bluecoat.com/documentation/All-Documents/ProxySG/SGOS%206.6

Security Advisory Fixes

- Security Advisories (SAs) are published as security vulnerabilities are discovered and fixed. To see any SAs that apply to the version of SGOS you are running, including ones that were published after this release, go to:

  https://bto.bluecoat.com/security-advisories

Self-Help Deployment Assistance

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

Frequently Asked Questions (FAQ) and Knowledge Base

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

Symantec Blue Coat Forums

- https://forums.bluecoat.com/

Documentation Changes

February 2016:

- The *Content Policy Language Reference* has been updated to include a new chapter on policy variables. Refer to the chapter "Variable Reference" for details on using variables in CPL to support Threat Risk Levels and the policy quotas implementation.

SGOS 6.6.3.2:

- ADN content previously in ProxyClient documentation has been moved to the *SGOS Administration Guide*.
- Online help pages for **Statistics > Clients** and **Configuration > Clients** now refer to the *SGOS Administration Guide* and *Unified Agent Deployment and Administration Guide*.

SGOS6.6.2.1 :

- Risk score policy has been removed from the "Web Application Protection" chapter of the *SGOS Administration Guide*. Refer to the *Web Application Firewall Solutions Guide* on BTO to learn how to use policy to protect your web applications from web attacks in a reverse proxy deployment.

Documentation Errata

SGOS 6.6.5.1:

- The following omissions were reported for some S-Series WebGuides:
  - S-Series WebGuide for S200 states that units have 2 HDDs, but many only have 1 HDD
  - S200 S-Series WebGuides do not cover how to tell if a HDD is faulty for non-SG models.
  - S400 S-Series WebGuides number of HDDs is only valid for SAS models but not SATA

- S400 S-Series WebGuide does not cover how to identify failed HDDs
- S500 S-Series WebGuide does not cover how to identify failed HDDs for non-SG models
- S500 S-Series WebGuides do not cover how to tell if a HDD is faulty for non-SG models.
- S-Series WebGuides do not contain information regarding which port is which on S500s

These omissions will be fixed as time permits.

SGOS 6.6.4.1:

- The *Multi-Tenant Policy Deployment Guide* previously mentioned using a user's authentication or group information to determine a tenant for a request. This information has been removed from the guide, because multi-tenant policy does not support user or group to determine tenants.
- The ProxySG appliance online help for Office 365 traffic includes outdated information. Refer to the "Managing Microsoft Outlook E-mail Traffic" chapter in the *SGOS Administration Guide* on BlueTouch Online (BTO) for current documentation.

SGOS 6.6.3.2:

- The ProxySG appliance online help and some documentation on BTO might include references to Application Attributes, but the feature is unavailable until further notice.

SGOS6.6.2.1 :

- The **Time Quota** and **Volume Quota** object descriptions in the VPM online help include an incorrect CLI command. Both object descriptions should read:

  "Before you can create quota policy, you must enable the quota library in the CLI. Issue the following command: `#(config)`**`policy quota`**

  If quotas are disabled, the VPM displays a 'variable not defined' error when you try to install quota policy."

  The *Visual Policy Manager Reference* and *Command Line Interface Reference* documents on BTO include the correct CLI commands for enabling/disabling quotas.

- Other online help pages include content that was subsequently updated. Refer to the documentation on BTO for the latest information.

Symantec documentation feedback

Please provide the document title and relevant chapter/section with your feedback.

- documentation_inbox@symantec.com