SGOS 6.7.x Release Notes

Current Version: 6.7.5.3

Document Revision: 4/16/2020

Symantec
A Division of Broadcom

Release Note Directory

These release notes present information about SGOS 6.7.x. Each section for a specific release provides feature descriptions, changes, and fixes. Sections about known issues and limitations for SGOS 6.7.x are listed separately.

Release Index

Information About All Releases

SGOS 6.7.5.3 GA

Release Information

- **Release Date:** April 15, 2020
- **Build Number:** 250069

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, 2.3.x, and 2.4.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to Article ID 169081:

  https://knowledge.broadcom.com/external/article/169081/supported-java-operating-system-and-brow.html
- For information on Java 11 support, refer to Article ID 173228:

  https://knowledge.broadcom.com/external/article?legacyId=tech252566

Upgrading To/Downgrading From This Release

- After upgrading to SGOS 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://knowledge.broadcom.com/external/article?legacyId=TECH254549.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/web-and-network-security/proxysg/6-7/upgrade-downgrade-guide.html

Changes in SGOS 6.7.5.3

- SGOS 6.7.5.3 introduces new features and enhancements. See "New Features in SGOS 6.7.5.3" on the next page.

Fixes in SGOS 6.7.5.3

- SGOS 6.7.5.3 includes a number of fixes. See "Fixes in SGOS 6.7.5.3" on page 9.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://support.broadcom.com/security-advisory/security-advisories-list.html

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

New Features in SGOS 6.7.5.3

The following changes were first made in SGOS 6.7.5.3:

SNMP Monitoring for HTTP Client Workers

New SNMP monitoring fields have been added to the BLUECOAT-SG-PROXY-MIB for HTTP client workers to provide statistics on the number of active workers and the maximum number of client workers that the appliance can create. These statistics are helpful for tracking resource usage in the appliance. When the appliance reaches the maximum number of active client workers, it logs a message in the Event Log to alert you of the resource overload. The following is an example alert:

```
019-09-12 21:35:43-00:00UTC "Maximum concurrent HTTP client worker limit of 5000 reached." 0
80010:1 htp_admin_testable.cpp:87
```

- More information:

  SNMP Critical Resource Monitoring Guide

New Event Log Message for HTTP Client Workers

When the appliance reaches the maximum number of concurrent HTTP Client Workers, a message in the following format is logged in the event log:

```
"Maximum concurrent HTTP client worker limit of 5000 reached."
```

ICAP Monitoring for Deferred and Resumed Transactions

> **Note:** This change was first introduced in SGOS 6.7.5.1.

Monitoring statistics are now available in the Event Log for long-running ICAP REQMOD transactions and deferred ICAP RESPMOD transactions. In the event log, the appliance logs the URL being scanned, the ICAP service name, the number of seconds passed since the appliance started the ICAP transaction, and the amount of bytes that were transferred before the request was logged or deferred. The appliance also logs when long-running REQMOD transactions are finished and when deferred RESPMOD transactions are resumed. The following are example event log messages:

```
REQMOD:
2020-03-06 21:29:23-00:00UTC "ICAP long scanning reqmod transaction for
http://10.169.3.235/policy using cas1 after 60 seconds and 1684703331 bytes"
2020-03-06 21:29:44-00:00UTC "ICAP long scanning reqmod transaction finished for
http://10.169.3.235/policy using cas1 after 81 seconds and 2274059168 bytes"
```

```
RESPMOD
2020-03-06 22:19:26-00:00UTC "ICAP scanning deferred for http://mydomain.com/stream using cas1
after 126 seconds and 4544730464 bytes"
2020-03-06 22:19:41-00:00UTC "ICAP scanning resumed for http://mydomain.com/stream  using cas1
after 141 seconds"
```

SSL Attributes for Access Logs and Policy

> **Note:** This change was first introduced in SGOS 6.7.5.1.

- For SSL traffic which is not intercepted by policy, SSL attributes (such as negotiated cipher or TLS version) are now logged in their respective access log fields and available for use in policy conditions. This enhancement is related to SG-6161. Refer to TECH253316 for more information.

Fixes in SGOS 6.7.5.3

Bug Fixes in this Release

SGOS 6.7.5.3 includes bug fixes. This update:

Access Logging

ID	Issue
SG-11525	Fixes an issue where Kafka continuous upload was slow.
SG-18169	Fixes an issue where config field of the access log was limited to less than 7000 characters.
SG-18470	Fixes an issue where access log uploads via SCP did not recover when a failure in the upload caused an invalid SSH server configuration.

Authentication

ID	Issue
SG-18357	Fixes an issue where authentication was impacted by Google Chrome's option for SamSite secure cookie settings being enabled by default.
SG-19013	Fixes an issue where the appliance could not join the active directory in GCP because its hostname was too long.
SG-12666	Fixes an issue where appliance experienced CAC performance issues.
SG-18417	Fixes an issue where the appliance experienced a page-fault restart in process "`likewise Lwbase_EventThread`" in "`liblikewise.exe.so`" at `.text+0x5311a8`.
SG-8116	Fixes an issue where "undefined" appears instead of "admin" in the logout URL of the Management Console.

CLI Consoles

ID	Issue
SG-18306	Fixes an issue where the appliance did not log a message in the event log when the command # `(config ssh-console)delete client-key` *`client_key_name`* was issued.
SG-17384	Fixes an issue where ProxySG appliances in a group experienced crashes in the process `CLI_Administrator`.
SG-17715	Fixes an issue where the character "?" was removed from data that the appliance imported.

DNS Proxy

ID	Issue
SG-17287	Fixes an issue where the appliance experienced a restart in `DNS_ghbyaddr_send`.

ICAP

ID	Issue
SG-18900	Fixes an issue where the appliance's performance was affected by the monitoring and logging for long-running ICAP REQMOD transactions.
SG-18842	Fixes an issue where the Event Log did not capture the duration of deferred ICAP RESPMOD transactions in the log details.

MAPI Proxy

ID	Issue
SG-15223	Fixes an issue where MAPI handoff broke during the export of large uncached attachments to the PST file from the Online Archive folder.

Policy

ID	Issue
SG-13680	Fixes an issue where Domain Fronting Attack Detection was not functioning for https://cccc.events/.

SSL Proxy

ID	Issue
SG-18971	Fixes an issue where SSL Proxy transactions were restarted when tunneled.
SG-19324	Fixes an issue where an HTTP memory leak would occur when traffic was intercepted on a policy exception.
SG-18241	Fixes an issue where expired trust package certificates were used instead of valid certificates.
SG-16627	Fixes an issue where the appliance experienced a restart in process group `"PG_SSL_HNDSHK"` in process `"cag.subscription"` in `"kernel.exe"` at `".text+0x131e8ba"`.
SG-19710	Fixes an issue where `fwd proxy(no)` and `fwd proxy(on_exception)` policy was not applied to TLS 1.3 tunneled sessions.
SG-18824	Fixes an issue introduced in SGOS 6.7.5.2 where the appliance experienced a restart when a forwarding rule was configured for tunneled SSL traffic.
SG-19040	Fixes an issue where the negotiated-cipher fields in the access log show "unknown" for tunneled TLS 1.3 connections.

SSL/TLS and PKI

ID	Issue
SG-19003	Fixes an issue where Tunneled TLS 1.2 SSL connections failed with an SSL failed error message.
SG-19215	Fixes an issue where the appliance displayed an error message that keylists an keyrings names cannot be identical, but saved configurations that contained identical names.

SSLV Integration

ID	Issue
SG-18207	Fixes an issue where offloading to an SSL Visibility appliance was not working.

TCP/IP and General Networking

ID	Issue
SG-17255	Fixes an issue where updating the WCCP home router in the Management Console would cause the current WCCP group to disappear from the UI.
SG-17191	Fixes an issue where the appliance experienced a restart in process group "PG_TCPIP" in process "WCCP_Admin" in "libstack.exe.so".
SG-18438	Fixes an issue where the appliance experienced a restart in process group "PG_TCPIP" in process "SSLW 13CE432FFB0" in "libstack.exe.so" at ".text+0x579d5b".
SG-18876	Fixes an issue where the appliance experienced a restart in process group "PG_TCPIP" in process "stack-admin" in "libstack.exe.so" at ".text+0x5471ee".

TCP Tunnel Proxy

ID	Issue
SG-9860	Fixes an issue where a large number of idle TCP tunnel connections and a high rate of policy reloading caused a large increase in memory consumption.

Web VPM

ID	Issue
SG-18804	Fixes an issue where user and groups objects were missing in the list of configured realms in the Web VPM.

SGOS 6.7.5.2 LA

Release Information

- **Release Date:** February 25, 2020
- **Build Number:** 248497

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, 2.3.x, and 2.4.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Important Information About This Release

SGOS 6.7.5.2 contains the following issues and has been made a Limited Availability release:

- Tunneled TLS 1.2 SSL connections fail with an SSL failed error message (SG-19003)
- SSL tunneled connections are bypassing forwarding rules (SG-18838)
- 6.7.5.2 crashes when a forwarding rule is configured for tunneled SSL traffic (SG-18824)

- SSL Proxy transactions were restarted when tunneled (SG-18971)
- `fwd proxy(no)` and `fwd proxy(on_exception)` policy was not applied to tunneled TLS 1.3 tunneled sessions (SG-19710)

Please refer to your Symantec point-of-contact for further details.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- After upgrading to SGOS 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://www.symantec.com/docs/TECH254549.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.5.2

- This release includes a fix. See "Fixes in SGOS 6.7.5.2" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.5.2

Bug Fixes in this Release

SGOS 6.7.5.2 includes the following bug fix. This update:

HTTP Proxy

ID	Issue
SG-18737	Fixes an issue where policy that used the gestures `ssl.forward_proxy(no)` and `ssl.forward_proxy(https, on_exception)` received a late verdict and the appliance was not able to not evaluate policy correctly.

SGOS 6.7.5.1 LA

Release Information

- **Release Date:** February 13, 2020
- **Build Number:** 247622

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, 2.3.x, and 2.4.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Important Information About This Release

SGOS 6.7.5.1 contains an issue that causes policy using the gestures `ssl.forward_proxy(no)` and `ssl.forward_proxy(https, on_exception)` to receive a late verdict and the appliance to not evaluate policy correctly and had been made a Limited Availability release. Please refer to your Symantec point-of-contact for further details.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- After upgrading to SGOS 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://www.symantec.com/docs/TECH254549.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.5.1

- SGOS 6.7.5.1 includes a number of fixes. See "Fixes in SGOS 6.7.5.1" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.5.1

Bug Fixes in this Release

SGOS 6.7.5.1 includes bug fixes. This update:

Access Logging

ID	Issue
SG-14575	Fixes an issue where the appliance experienced "-" in access log fields `x-bluecoat-icap-reqmod-delay-time` and `x-bluecoat-icap-reqmod-service-time` when `ICAP_REPLACED` was the response status.
SG-16961	Fixes an issues where the appliance experienced a restart in process group `PG_DNS` in process `ALOGStream:Servers [0x4003b2]` in `libstack.exe.so` at `.text+0x33d5b3`.

Authentication

ID	Issue
SG-14089	Fixes an issue where reloading the Management Console required realm users to re-enter their usernames and passwords.
SG-15249	Fixes an issue where reloading the Management Console required users to re-enter their usernames and passwords.

CLI Consoles

ID	Issue
SG-3726	Fixes an issue where the Advanced URL "/diagnostics/hardware/info" the "write-required" attribute set.

Health Checks

ID	Issue
SG-13609	Fixes an issue where the appliance stopped working during a DNS update.
SG-17057	Fixes an issue where the appliance experienced a restart in the watchdog process.

Kernel

ID	Issue
SG-16873	Fixes an issue where the appliance experienced a restart in process `priviliege.exe` when a hidden CLI command was used. The CLI command has been removed.

Policy

ID	Issue
SG-14544	Fixes an issue where the appliance's IP address is used for outgoing traffic instead of reflecting the client IP address.

SSL Proxy

ID	Issue
SG-6161	Fixes an issue where after upgrading to SGOS 6.7.4.1 , when SSL traffic is not intercepted by policy, SSL attributes (such as negotiated cipher or TLS version) were not available for use in policy conditions and access log fields. Refer to TECH253316 for more information on this issue.
SG-12044	Fixes an issue where the SSL certificate hostname would be invalid when two virtual hosts are running in a reverse proxy configuration.

SSL/TLS and PKI

ID	Issue
SG-15185	Fixes an issue where HTTPS sites the were denied by policy appeared under Sessions > Errored Sessions.
SG-14742	Fixes an issue where the appliance returned a failed SSL exception when using a forwarding host.
SG-15462	Fixes an issue where the appliance could not verify a certificate when the certificate's IP address was contained in a SAN IP address attribute.

TCP/IP and General Networking

ID	Issue
SG-13840	Fixes an issue where interface 0:1 was unavailable.
SG-14848	Fixes an issue where the bandwidth management classes would reach their maximum.
SG-14968	Fixes an issue where the LAG interface continuously synchronized.
SG-15243	Fixes an issue where only one of two possible aggregate interfaces appeared after rebooting the appliance.
SG-16380	Fixes an issue where link aggregation did not properly handle large frames.
SG-16541	Fixes an issue where the appliance looked up the route of UDP packets sent using udp_send every time a packet was sent.
SG-16706	Fixes an issue where the appliance could not establish a WCCP connection when the appliance received traffic on non-UDP-2048 ports.
SG-17097	Fixes an issue where traffic that was bypassed for SSL interception lost packets when the frame size was greater than 1510 bytes.

Transformer

ID	Issue
SG-17839	Fixes an issue where the appliance would stop working when the user accessed a YouTube video.

URL Filtering

ID	Issue
SG-14027	Fixes an issue where the appliance experienced a watchdog restart in process group "" in `kernel.exe` at `.text+0x1249cca` after downloading local database `HWE: 0x0 SWE: 0x11 PFLA: 0x0`.

VPM (Legacy)

ID	Issue
SG-10128	Fixes an issue where the Admin Banner objects would disappear from the Admin Banner rule.

Web VPM

ID	Issue
SG-16315	Fixes an issue where policy pushes from the Web VPM caused rules with a negate decision to validate instead.
SG-16999	Fixes an issue where the font size in layer guard rule comments did not match the font size in standard rule comments.
SG-16332	Fixes an issue where **Perform Request Analysis** and **Perform Reponse Analysis** action objects included an Add button even though ICAP services cannot be added through the VPM.
SG-15367	Fixes an issue where the comment entered for a layer guard rule does not appear in the generated CPL.
SG-16593	Fixes an issue where installing policy including combined objects sometimes resulted in the "Visual Policy Manager seems slow to start" message.
SG-16636	Fixes an issue where non-rule layers could not be closed.

SG-15809	Fixes an issue where combined objects that were negated (for example, `condition=!CombinedDestination`) sometimes were not processed as expected (the negation would apply to the initial rule). For example, in the following definition, the `url.address` should not be negated:
	
	`define condition CombinedDestination`
	` url.address=1.2.3.4`
	` condition=RequestURLCategory1`
	`end condition CombinedDestination`

SG-15956	Fixes an issue where a "Duplicate condition type detected" error occurred when installing **Encrypted Tap** policy.
SG-15841	Fixes an issue where an incorrect subnet mask was generated when entering subnet **/26** in the **Client IP** object.

ID	Issue
SG-15815	Fixes an issue where the **Request Header** source object was not available in the Forwarding layer, and **Request Header** objects in combined source objects created in the legacy Java VPM did not appear in the web VPM.
SG-14023	Fixes an issue where `url.category=` conditions were duplicated when installing policy.
SG-11986	Fixes an issue where `server.connection.encrypted_tap()` did not have a corresponding VPM object. The **Enable Encrypted TAP** action object now has options for enabling and disabling server encrypted tap; refer to the *Web Visual Policy Manager Reference*.
SG-13520	Fixes an issue where the VPM prompted read-only users to keep or remove categories when viewing a category object that contained categories not in the content filter database.
SG-14121	Fixes an issue where layers containing a large number of rules seemed unresponsive when opening or closing them. Now, when opening or closing these layers, the VPM shows a "busy" icon.
SG-13978	Fixes an issue where opening or closing layers containing a large number of rules resulted in increased memory usage.
SG-13461	Fixes an issue where multiple authentication actions could be included in a combined object. Now, attempting to add multiple authentication actions in a combined object results in a "Multiple Authenticate Objects Not Allowed".
SG-9445	Fixes an issue where installing combined objects containing ICAP analysis objects appeared to have no effect.
SG-9461	Fixes an issue where condition names including an ampersand ("&") character did not install correctly. Now, condition names including an ampersand character are enclosed in quotations and installed correctly.

SGOS 6.7.4.14 GA

Release Information

- **Release Date:** March 16, 2020
- **Build Number:** 249043

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.14

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.14" on the next page.
- New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.14

Bug Fixes in this Release

SGOS 6.7.4.14 includes bug fixes. This update:

Authentication

ID	Issue
SG-15249	Fixes an issue where reloading the Management Console required users to re-enter their usernames and passwords.

Health Checks

ID	Issue
SG-18338	Fixes an issue where the HSM health checks would stop functioning and after rebooting, the HSM health checks would not return to a healthy state.

SSL/TLS and PKI

ID	Issue
SG-14742	Fixes an issue where the appliance returned a failed SSL exception when using a forwarding host.
SG-15462	Fixes an issue where the appliance could not verify a certificate when the certificate's IP address was contained in a SAN IP address attribute.

This release also includes fixes from SGOS 6.7.4.13. See "Fixes in SGOS 6.7.4.13" on page 26 for more information.

SGOS 6.7.4.13 GA

Release Information

- **Release Date:** December 11, 2019
- **Build Number:** 245568

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.13

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.13" on the next page.
- New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.13

Bug Fixes in this Release

SGOS 6.7.4.13 includes bug fixes. This update:

TCP/IP and General Networking

ID	Issue
SG-15819	The appliance experienced a restart in `HWE:0xe SWE:0x0 PFLA:0x308` process group `PG_TCPIP` during process `cookie-monster` in `libstack.exe.so` at `.text+0x42ab67`.
SG-17204	When the appliance experienced high traffic on its network interface, the interface became unavailable.
SG-17288	Fixed an issue where the appliance does not accept "0xf00" as the network mask during WCCP configuration.

SGOS 6.7.4.12 PR

Release Information

- **Release Date:** November 18, 2019
- **Build Number:** 244888

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.12

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.12" on the next page.
- New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.12

Bug Fixes in this Release

SGOS 6.7.4.12 includes bug fixes. This update:

TCP/IP and General Networking

ID	Issue
SG-14374	The final Acknowledgment flag from when the TCP connection closed used the default interface instead of the return-to-sender interface.
SG-17015	The process `likewise Lwbase_WorkThread` in `libstack.exe.so` at `.text+0x33dbd3` caused an `HWE:0xe: SWE:0x0 PFLA:0x18` restart in process group `PG_DNS`.

SGOS 6.7.4.11 PR

Release Information

- **Release Date:** November 8, 2019
- **Build Number:** 244613

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.11

- 6.7.4.11 provides a fix for a change AWS made to their metadata service on November 5, 2019. On this date, the ProxySG software began to receive failed requests from the AWS metadata server. SGOS 6.7.4.11 includes a fix to resolve this issue. For more information, see the following KB article: https://support.symantec.com/us/en/article.TECH256820.html
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

SGOS 6.7.4.10 PR

Release Information

- **Release Date:** November 5, 2019
- **Build Number:** 244296

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.10

- The default EDNS payload buffer size has changed from 13398 to 1232. In addition, you can specify a different payload buffer size. (SG-14020)

  To change the payload buffer size and view the EDNS settings:

  1. Enable EDNS using the command:

     ```
     # (config) dns edns enable
     ```

  2. (If needed) Specify a different EDNS payload buffer size:

     ```
     # (config) dns edns size
     ```

     where *size* is a value from 512 to 65535.

  3. View the DNS settings:

     ```
     # show dns
     ```

     If you did not change the payload buffer size, the `# show dns` output shows the new default size.

Fixes in SGOS 6.7.4.10

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.10" on page 35.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.10

Bug Fixes in this Release

SGOS 6.7.4.10 includes bug fixes. This update:

Access Logging

ID	Issue
SG-12563	Fixes an issue where SCP log uploads from the appliance to WSS failed with error "no bytes sent from this queue, error code = -1".
SG-13527	Addresses an issue where the appliance stopped responding with an error in Process group: "PG_ACCESS_LOG" Process: "ALOGStream:ssl" in "libsshd.exe.so",

Authentication

ID	Issue
SG-13039	Fixes an issue where the appliance tried to connect to an unreachable domain controller, causing an outage.
SG-14821	Fixes an issue where CAPTCHA validation forms looped and did not allow users to authenticate in multi-tenant deployments.

DNS Proxy

ID	Issue
SG-14716	Addresses an issue where the appliance stopped responding with DNS-related exceptions in "libmemory.so".

FTP Proxy

ID	Issue
SG-13701	Fixes an issue where the appliance experienced multiple FTP errors, "421 Service not available, closing control connection", after an upgrade to version 6.7.4.5.

IPv6

ID	Issue
SG-9626	Addresses an issue where the appliance experienced a restart in process: "stack-bnd-3:0-rxq-1" in "libstack.exe.so" .

Management Console

ID	Issue
SG-13909	Fixes an issue where the Management Console stopped responding when adding an IPv6 gateway to a routing domain. In addition, the Management Console would not load if the gateway was successfully added via the CLI.

Security

ID	Issue
SG-15870	Fixed a session hijacking vulnerability in the HTTPS Management Console.

Services

ID	Issue
SG-14170	Fixes an issue where proxy services could not be added via Management Console or the CLI.

SNMP

ID	Issue
SG-8026	Fixes an issue where SNMP periodically stopped working and reported an error, "Not in time window".

SOCKS

ID	Issue
SG-12349	Addresses an issue where the appliance experienced restarts in Process: "SOCKS Worker 111D5437D30" in "libpolicy_enforcement.so" at .text+0x3cea6.

SSL/TLS and PKI

ID	Issue
SG-13430	Fixes an issue where the appliance stops responding while adding a new CA certificate.
SG-14843	Addresses an issue where the appliance experienced a restart in HWE:0x3 SWE:0x7 PG:"PG_CFSSL" Process: "SSLW 11A7C84AC90".

TCP/IP and General Networking

ID	Issue
SG-8965	Addresses an issue where the appliance experienced a restart in "stack-deletion-ISR" in "libstack.exe.so" at .text+0x4265b7.
SG-13446	Addresses an issue where the appliance experienced a restart in m_dup_pkthdr HWE:0x3 SWE:0x0 PFLA:0x0 Process group: "PG_TCPIP" Process: "HTTP CW 21830453A40" in "libstack.exe.so" at .text+0x4d625f.
SG-14060	Fixes an issue where the appliance stopped passing traffic upstream when processing very high loads.
SG-14850	Addresses an issue where the appliance experienced a restart in HWE : 0xe SWE: 0x0 PFLA:0x0 PG: "PG_DNS" Process: "likewise Lwbase_WorkThread" in "libstack.exe.so" at .text+0x33d5b3
SG-14937	Fixed an issue where the bytes received statistics report (**Statistics > Network > Interface History > Bytes Received**) did not increment after an upgrade to version 6.7.4.9.
SG-16423	Fixes an issue where IPv4 TCP tunnel throughput was reduced to 1 Gbps.

Utility Libraries

ID	Issue
SG-15503	Addresses an issue where the appliance experienced a page fault in Process group: "PG_ACCESS_LOG" Process: "sshc.worker".

SGOS 6.7.4.9 PR

Release Information

- **Release Date:** August 13, 2019
- **Build Number:** 240916

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, 2.3.x, and 2.4.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- After upgrading to SGOS 6.7.4 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://www.symantec.com/docs/TECH254549.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.9

- SGOS 6.7.4.9 includes a number of fixes. See "Fixes in SGOS 6.7.4.9" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.9

SGOS 6.7.4.9 includes bug fixes. This update:

Access Logging

ID	Issue
SG-10547	Addresses an issue where the proxy restarted in process group "PG_ACCESS_LOG" in process: "ALOGStream:elk_stream [0xc002f" in "libaccess_log.exe.so".

Authentication

ID	Issue
SG-3044	Fixes an issue where Internet Explorer did not prompt for credentials if a second consecutive login was cancelled. Symantec acknowledges Baskar Borman for reporting this vulnerability.
SG-4795	Fixes an issue where CAC authentication was slow when using an HTTPS console.
SG-4973	Addresses an issue where the the proxy restarted in process group "PG_CFG" in process "IWA Onbox Domain Trust Refresher" in "liblikewise.exe.so".
SG-5102	Addresses an issue where the proxy restarted in process group "PG_LSA" in process "likewise lwmsg server worker" in "libknl_api.so".
SG-5123	Addresses an issue where the proxy restarted in process group "PG_POLICY_HTTP" in process "LDAP Authenticator" in "libopenldap.exe.so".
SG-8302	Fixes an issue where the CPU monitor showed that the LSA (Local Security Authority) was using a high amount of CPU resources.
SG-9272	Fixes an issue where the error "Error connecting to SG" was seen when logging into the Management Console.
SG-9435	Fixes an issue where the admin user was unable to authenticate on the Management Console when a cookie wasn't cleared after the previous log out.
SG-10132	Fixes an issue where a suitable proper error message was not sent when a Kerberos replay attack occurred.
SG-10548	Fixes an issue where rejoining a Windows Domain failed after upgrade to 6.7.4.x from 6.7.3.14.
SG-11002	Fixes an issue where there the Event Log noted that the IWA Direct secure channel (Schannel) had reset many times.
SG-11130	Fixes an issue where CAPTCHA validation could not be implemented because the CAPTCHA request was looping on the proxy.
SG-11447	Fixes an issue where an authentication logout exception page was not returned when a SAML realm was used.
SG-12075	Fixes an issue where the post-setup archive configuration contained the Windows Domain hostname instead of the default hostname in IWA Direct (system created).

ID	Issue
SG-12635	Addresses an issue where the proxy experienced a restart in process "Agent-Admin-CORP-233".
SG-12978	Fixes an issue where, after trying to join the domain, the proxy became unresponsive and stopped passing traffic. The admin could ping the proxy but could not access the Management Console or SSH CLI.

DNS Proxy

ID	Issue
SG-5317	Fixes an issue where the proxy did not accept CNAME as a valid DNS response.
SG-12243	Fixes an issue where DNS resolution failed when EDNS was enabled.

Event Logging

ID	Issue
SG-12392	Fixes an issue where the Syslog was flooded by assert messages.

FTP Proxy

ID	Issue
SG-8108	Addresses an issue where the proxy restarted in process group "PG_TCPIP" in process "FTP CW 102FEDA8430" in "libstack.exe.so".

HTTP Proxy

ID	Issue
SG-9171	Fixes an issue where files could not be downloaded after a successful login to FTP server.
SG-9601	Fixes an issue where client workers maxed out due to DNS (UDP port exhaustion).
SG-9756	Fixes an issue where the proxy experienced a threshold monitor restart after the CPU was high in policy evaluation.
SG-10873	Addresses an issue where the proxy restarted in process group "PG_DNS" in process "HTTP CW 10EC82F0A40" in "libmemory.so".
SG-10937	Addresses an issue where the proxy restarted in process group "PG_HTTP" in process "HTTP CW 10ADA60BA40" in "kernel.exe".
SG-11633	Addresses an issue where the proxy restarted in process group "PG_HTTP" in process "HTTP Admin" in "libhttp.exe.so".

Management Console

ID	Issue
SG-10839	Fixes an issue where ICAP object names did not appear under **Statistics > Content Analysis**.

ID	Issue
SG-11199	Fixes an issue where initial login attempts using the Management Console Launcher did not work.

SSL/TLS and PKI

ID	Issue
SG-9276	Fixes an issue where the proxy restarted while adding a keyring to an existing keylist.
SG-12405	Fixes an issue where the proxy restarted after a slow growth in memory pressure in SSL and Cryptography. This issue occurred when the proxy was operating as a reverse proxy.

SSL Proxy

ID	Issue
SG-4434	Fixes an issue where `ssl_failed` exceptions occurred randomly.
SG-8079	Fixes an issue where the default keyring specified In the keylist did not show up In Sysinfo.
SG-9211	Fixes an issue where exception pages were not served or displayed for blocked websites. This issue occurred as a result of on-exception SSL-interception not being triggered when expected.

TCP/IP and General Networking

ID	Issue
SG-11038	Addresses an issue where the proxy was unable to establish WCCP connectivity to a router that did not support WCCP v2.01.
SG-10832	Addresses an issue where the proxy restarted in process "stack-bnd-0:0-rxq-0" in "libstack.exe.so".
SG-10181	Fixes an issue where the SOCKS proxy did not preserve the source port for outbound connections, causing connections to fail.
SG-10037	Addresses an issue where the proxy experienced a page fault restart in process group "PG_DNS" in process "Mapi.http.worker" when there was a DNS query to the outlook.office365.com domain.
SG-9439	Addresses an issue where the proxy restarted in process group "PG_TCPIP" in process "SSLW 10C2B143FB0" in "libstack.exe.so".
SG-9239	Fixes an issue where CPU usage increased sharply and network throughput degraded when high volumes of (mostly) bypassed traffic were sent to the proxy.
SG-8569	Fixes an issue where an unknown error response (203) on the proxy occurred when the DNS response was truncated and contained more than 50 Nameservers.
SG-4333	Fixes an issue where turning on/off EDNS support on the appliance was not reflected in the event log.
SG-11481	Fixes an issue where the proxy did not adhere to the configured TCP window size, which intermittently caused download slowness.

URL Filtering

ID	Issue
SG-5060	Fixes an issue where the proxy was unable to perform Application Classification or Threat Risk Levels lookups because the Management Console was logged in with a read-only account.

Visual Policy Manager

ID	Issue
SG-12464	Fixes an issue where policy updates in the Web VPM were not showing up in the legacy VPM.

SGOS 6.7.4.804 LA

Release Information

- **Release Date:** October 16, 2019
- **Build Number:** 243223

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
    - S500, S500-30, S400, S200
    - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
    - SWG V100
    - SG-VA high-performance models (refer to specific deployment guide for details)
    - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.804

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.804" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.804

Bug Fixes in this Release

SGOS 6.7.4.804 includes bug fixes. This update:

SGOS 6.7.4.8 GA

Release Information

- **Release Date:** July 24, 2019
- **Build Number:** 239786

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, and 2.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.8

- SGOS 6.7.4.8 includes a number of fixes. See "Fixes in SGOS 6.7.4.8" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.8

SGOS 6.7.4.8 includes bug fixes. This update:

Authentication

ID	Issue
SG-9224	Addresses a restart in Process group: "PG_LSA" Process: "likewise lwmsg server worker" in "liblikewise.exe.so" at .text+0x2b2829 HWE: 0xe, SWE: 0x0.

Health Checks

ID	Issue
SG-13643	Fixes an issue where health checks failed or reported that the monitored component was not found. This issue occurred after upgrading from version 6.6.5.14 to 6.7.4.7.

SSL/TLS and PKI

ID	Issue
SG-13642	Fixes an issue where the appliance stopped responding after the HSM IP address was changed.

TCP/IP and General Networking

ID	Issue
SG-11621	Fixes an issue where client/server-based applications could not communicate via the appliance. PCAPs showed the appliance responded with RESET for SYN on some connections. This issue occurred after an upgrade to version 6.7.4.1.

URL Filtering

ID	Issue
SG-12947	Fixes an issue where creating or editing an **Application Name** object in the legacy or web VPM object failed. This issue occurred after an upgrade to version 6.7.4.5.
SG-8740	Fixes an issue where event logs displayed the error: `CFS error: Failed to create PDM trend group cfs` This issue occurred after an upgrade to version 6.7.4.2.

Web Visual Policy Manager

ID	Issue
SG-11654	Fixes an issue where **Enable HTTPS Interception** was undefined when converting Java-based CPL to web VPM CPL.

ID	Issue
SG-5050	Fixes an issue where installing VPM policy resulted in a "Duplicate definition" error although policy did not include duplicate definitions. This issue occurred when using Symantec Management Center to create tenant/landlord policies in the VPM. **Note:** This issue was fixed in version 6.7.4.6.
SG-13050	Fixes an issue where it was possible to create multiple identical **Client IP Address/Subnet** objects.
SG-10965	Fixes an issue where February 29th was not available in **Time** objects.

SGOS 6.7.4.7 PR

Release Information

- **Release Date:** June 14, 2019
- **Build Number:** 238163

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, and 2.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.7

- SGOS 6.7.4.7 includes a fix. See "Fixes in SGOS 6.7.4.7" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.7

SGOS 6.7.4.7 includes a bug fix. This update:

Authentication

ID	Issue
SG-12836	Fixes an issue where the proxy experienced a restart in process group "PG_CFG_PROPRIETOR" in process "IWA Onbox Domain Trust Refresher" when using IWA Direct in version 6.7.4.6.

SGOS 6.7.4.6 PR

Release Information

- **Release Date:** June 4, 2019
- **Build Number:** 236878

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, and 2.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.6

By default, IWA-Direct realms list groups using sAMAccountNames. You can now specify that IWA-Direct realm lists groups using their Common Names. Use the following command:

```
#(config iwa-direct realm_name)use-cn-group-names {enable|disable}
```

Fixes in SGOS 6.7.4.6

- SGOS 6.7.4.6 includes a number of fixes. See "Fixes in SGOS 6.7.4.6" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.6

SGOS 6.7.4.6 includes bug fixes. This update:

Authentication

ID	Issue
SG-11455	Fixes an issue where the authentication agent rejected a request when using `tenant.request_url()` in landlord policy.

IPv6 Stack and IPv6 Proxies

ID	Issue
SG-9182	Addresses an issue where the proxy experienced a restart in process "stack-bnd-3:0-rxq-1" in "libstack.exe.so" when using IPv6.

Policy

ID	Issue
SG-9039	Addresses an issue where the proxy experienced a restart in process "Parse exception list" in "libpolicy_enforcement.so" after rebooting.
SG-10294	Addresses an issue where the local database should not accept the installation of policy that had a 'define' block that does not terminate with 'end'.

Transformer

ID	Issue
SG-9589	Addresses an issue where the page transformer corrupted data intermittently when the OCS sent chunked Transfer Encoding.

Web Visual Policy Manager

ID	Issue
SG-10656	Fixes an issue where the Web VPM did not allow comments in category definitions.
SG-11034	Fixes an issue in the Web VPM where adding the **Request URL Category** object returned an unknown category error if there was any delay in the network.

SGOS 6.7.4.5 PR

Release Information

- **Release Date:** April 25, 2019
- **Build Number:** 235446

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, and 2.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.5

The following changes were first made in SGOS 6.7.4.4.

This release adds the ability to configure the link aggregation transit delay. The transit delay setting determines how much settle time link aggregation requires to switch from sending packets from an unlinked port to sending from a linked port. Configure link aggregation transit delay time with the following CLI command:

```
#(config interface aggr:number)transit-delay 0-65535
```

Use this command to configure the transit delay time, in milliseconds (ms), for the specified link aggregate. The default value is 3000 ms.

> **Note:** During the settle time, all packets for an unlinked port are dropped. The settle time is required to ensure packets are not received out-of-order when switching to a linked port to send the traffic. Setting a smaller `transit-delay` time will reduce the number of packets lost during the port transition, while increasing the possibility of out-of-order packets.

Fixes in SGOS 6.7.4.5

- Fixes listed in "Fixes in SGOS 6.7.4.5" on the next page were first included in SGOS 6.7.4.4.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.5

SGOS 6.7.4.5 includes security advisory (SA) fixes and bug fixes.

Security Advisory Fixes in this Release

SGOS 6.7.4.5 includes security advisory fixes. This update:

ID	Issue
N/A	Addresses OpenSSL vulnerabilities (CVE-2018-0739). For details, refer to SYMSA1443.

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://www.symantec.com/security-center/network-protection-security-advisories

Bug Fixes in this Release

SGOS 6.7.4.5 includes bug fixes. This update:

Access Logging

ID	Issue
SG-4874	Fixes an issues where the proxy restarted after configuring the access log with an SCP upload client and then performing an `upload log BCReporter` operation.
SG-5340	Fixes an issue where the access log could not be retrieved via the CLI or a URL when there was a "." in the log facility name.
SG-8343	Fixes an issue where the proxy experienced memory pressure when uploading the access log using SSH and authentication failed.

Authentication

ID	Issue
SG-5092	Addresses an issue where the proxy experienced a restart after it received a RADIUS accounting request.
SG-5351	Fixes an issue where LDAP authorization failed when using nested groups.
SG-8361	Fixes an issue where the proxy was unable to join a domain when RC4 encryption type was disabled on the domain controller.

DNS Proxy

ID	Issue
SG-9182	Addresses an issue where the proxy experienced a restart when DNS recursion was enabled.

HTTP Proxy

ID	Issue
SG-1308	Addresses an issue where the proxy experienced a restart in PG_TCPIP in process "HTTP CW 208353A5A40".
SG-4139	Addresses an issue where the proxy experienced a restart in process group "PG_TCPIP" in process "tcpip_protocol_worker_1".
SG-8042	Addresses an issue where the proxy experienced a restart in process group "PG_ACCESS_LOG" in process "ALOGAdmin:main" in "libhttp.exe.so".
SG-8273	Fixes an issue where the proxy served the whole object to clients for byte-range requests when the Cachepulse service was enabled. This issue occurred when the byte range header was greater than 14Kbytes.
SG-8805	Addresses an issue where the proxy experienced a restart in process group "PG_HTTP", Process: "HTTP SW 6093C37AA40 for 7091D8E4A40" in "libhttp.exe.so".
SG-8846	Addresses an issue where the proxy experienced a restart in process group "PG_POLICY_FTP" in Process: "PDW t=1262282600 for=848038BF".

ICAP

ID	Issue
SG-8038	Fixes an issue where the exception page is not returned from the Symantec DLP server (in ICAP request mode) when **Use vendor's "virus found" page** is enabled for the ICAP service.

Policy

ID	Issue
SG-4123	Fixes an issue where event logs displayed a "Failed to create a new tenant statistics node" error after adding tenant policy.
SG-4869	Fixes an issue where rules match but sometimes don't execute when they are contained within a `define policy` macro.
SG-5359	Fixes an issue where coaching policy did not work when tenant policy was present.
SG-8513	Fixes an issue where the Malware Scanning policy file could not be downloaded.

SSL/TLS and PKI

ID	Issue
SG-5162	Addresses an issue where the proxy experienced a restart in the Threshold_Monitor process where the highest consumers of memory were SSL and cryptography.
SG-5172	Fixes an issue where SSL inspection was inconsistent due to an invalid cache certificate.
SG-5328	Fixes an issue where the proxy reverted to version 6.6.5.17 after attempting to upgrade to version 6.7.4.1.
SG-5346	Fixes an issue where importing a CRL failed with an insufficient memory error.

ID	Issue
SG-9067	Fixes an issue where the proxy experienced a restart in process group "PG_SSL_HNDSHK" in process "FTP CW 4098B026430" in "libcfssl.exe.so" .
SG-9252	Fixes an issue where an expanded archive configuration could not be restored when it contained a CCL that started with "bluecoat-".

TCP/IP and General Networking

ID	Issue
SG-4867	Fixes an issue where packets could be dropped after losing a link aggregate. The following CLI command was added to fix this issue: `#(config interface aggr:`*`number`*`)`**`transit-delay`** *`0-65535`* The default value is 3000 milliseconds (ms).
SG-5079	Fixes an issue where `client.interface=` CPL returned 255.255 (an invalid adapter / interface).
SG-7863	Fixes an issue where the TCP three-way handshake was failing because S200 models were intermittently not responding to SYN/ACK.
SG-8062	Addresses an issue where the proxy experienced a restart in process "stack-bnd-2:1-rxq-0" in "libstack.exe.so".
SG-8691	Addresses an issue where the proxy experienced several restarts in process SGRP Worker when using multicast.
SG-8820	Addresses an issue where the proxy experienced a restart in process "stack-bnd-3:0-rxq-1" in "libstack.exe.so" when using WCCP.
SG-8924	Addresses an issue where the proxy experienced a restart in process group "PG_TCPIP" in process "stack-api-worker-1" in "libstack.exe.so".
SG-9599	Fixes an issue where executing a packet capture in a core image (e.g. 'pcap start last capsize XXXX coreimage YYYY') can cause a monitoring violation (error code 0x5b).

URL Filtering

ID	Issue
SG-5333	Fixes an issue where the Threat Risk Level lookup returned `unavailable` or `none`.
SG-8081	Addresses an issue where the proxy experienced a restart in process group "PG_OPP" in process "OPP_Wo 0x42b0bcc720" when using WebPulse.
SG-8410	Addresses an issue where the proxy experienced a restart in process "stack-admin" (0x4000cc) at libstack.exe.so:0x611ddb.

Web Visual Policy Manager

ID	Issue
SG-8624	Fixes an issue where the first installation of policy via the Web VPM caused errors in generated CPL. This issue occurred when condition block names contained quotation marks and whitespace.

ID	Issue
SG-8818	Fixes an issue where the Web VPM changed Bandwidth Management objects from `limit_bandwidth.server.inbound(class_name)` to `limit_bandwidth.server.inbound(no)` by default.

SGOS 6.7.4.4 LA

Release Information

- **Release Date:** April 16, 2019
- **Build Number:** 234965

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x, and 2.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Important Information About This Release

SGOS 6.7.4.4 contains an issue that causes some appliances to restart. Symantec recommends upgrading to "SGOS 6.7.4.5 PR" on page 60 to resolve this issue. SGOS 6.7.4.4 is no longer available for download through MySymantec. Please refer to your Symantec point-of-contact for details.

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

SGOS 6.7.4.3 PR

Release Information

- **Release Date:** January 25, 2019
- **Build Number:** 230901

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Important Information About This Release

SGOS 6.7.4.3 fixes a serious issue where using the new Web Visual Policy Manager caused unintended policy behavior when applying policy save/changes. For details, refer to SG-8612 in "Fixes in SGOS 6.7.4.3" on page 74. Symantec recommends upgrading to this release to use the Web VPM without issue.

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Changes in SGOS 6.7.4.3

- SGOS 6.7.4.3 introduces new features and enhancements. See "New Features in SGOS 6.7.4.3" on the next page.

Fixes in SGOS 6.7.4.3

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.3" on page 74.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

New Features in SGOS 6.7.4.3

SGOS 6.7.4.3 introduces the following new features.

Web Visual Policy Manager

This release includes the new Web Visual Policy Manager (VPM). The Web VPM allows you to manage your organization's policies in a redesigned web-based interface. The improved experience of writing and installing policy includes:

- Re-organized and modern look-and-feel in an easy-to-read browser tab
- Ability to compare current policy with deployed policy before saving changes
- Ability to identify and locate all conditions and actions in both generated and current policy

The legacy VPM is still available. Changes to policy using either VPM persist and are reflected in both VPM instances (except in cases of downgrades).

Minimum Requirements

Supported browsers:

- Google Chrome 60.0.3112 and later
- Mozilla Firefox 57 and later
- Microsoft Edge 42.17134 and later
- Safari 10.1.2 and later

> **Caution:** Microsoft Internet Explorer is not supported. If Internet Explorer is your default browser (or if you use a supported browser that launches the VPM in Internet Explorer), you can right-click and copy the **Visual Policy Manager** link at the top right of the Management Console. Then, paste the URL into a supported browser.

Display resolution:

- 1366 x 768

In addition, the web-based VPM and all of its functionality are available in Symantec Management version 2.1.1.2. Refer to the Management Center 2.1 Configuration & Management Guide for details.

- More information:

  ProxySG Web Visual Policy Manager WebGuide

Periodic Upload of SysInfo Statistics

You can now configure the appliance to upload SysInfo reports at a set interval. Previously, the appliance supported only manual uploads of SysInfo reports. The following CLI commands have been added to support this feature:

`#(config service-info)`**`periodic count`** *`count`* - Specify the maximum number of SysInfo reports to send.

`#(config service-info)`**`periodic disable`** - Disable the periodic upload of SysInfo reports.

`#(config service-info)`**`periodic enable`** - Enable the periodic upload of SysInfo reports.

`#(config service-info)`**`periodic interval`** *`interval`* - Set the interval (in hours) for periodic upload. For example, type **`12`** to send reports every 12 hours.

`#(config service-info)`**`periodic no`** - Clear the periodic upload parameters.

`#(config service-info)`**`periodic sr-number`** *`sr_number`* - Specify an SR number to associate SysInfo reports with a Support case.

- More information:

  Command Line Interface Reference

External Services Access Log Fields

New access log fields have been added to log communication times with external services:

- `x-bluecoat-authentication-start-time`: Authentication start time offset from the start of the transaction
- `x-bluecoat-authentication-time`: Time required to authenticate the user
- `x-bluecoat-authorization-start-time`: Authorization start time offset from the start of the transaction
- `x-bluecoat-authorization-time`: Time required to authorize the user
- `x-bluecoat-ch-start-time`: CH evaluation start time offset from the start of the transaction
- `x-bluecoat-ci-start-time`: CI evaluation start time offset from the start of the transaction
- `x-bluecoat-co-start-time`: CO evaluation start time offset from the start of the transaction
- `x-bluecoat-icap-reqmod-delay-time`: Time taken to connect to ICAP reqmod service
- `x-bluecoat-icap-reqmod-service-time`: Time taken for ICAP reqmod service once connected
- `x-bluecoat-nc-start-time`: NC evaluation start time offset from the start of the transaction
- `x-bluecoat-si-start-time`: SI evaluation start time offset from the start of the transaction
- `x-bluecoat-so-start-time`: SO evaluation start time offset from the start of the transaction

All times are expressed in milliseconds.

- More information:

  Content Policy Language Reference

Fixes in SGOS 6.7.4.3

SGOS 6.7.4.3 includes security advisory (SA) fixes and bug fixes.

Security Advisory Fixes in this Release

SGOS 6.7.4.3 includes security advisory fixes. This update:

ID	Issue
SG-5747	Addresses OpenSSH vulnerabilities (CVE-2018-15473). For details, refer to SYMSA1469.
SG-5361	Addresses OpenSSH vulnerabilities (CVE-2016-10708). For details, refer to SYMSA1469.

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://www.symantec.com/security-center/network-protection-security-advisories

Bug Fixes in this Release

SGOS 6.7.4.3 includes bug fixes. This update:

Access Logging

ID	Issue
B#264042 SG-6009	Fixes an issue where access log uploaded over SCP upload failed with a `no bytes sent from this queue error code = -1` error. This issue occurred when the appliance stopped responding abruptly, or had power failures or disk failures.

Authentication

ID	Issue
B#265632 SG-5058	Fixes an issue where the proxy stopped responding while performing LDAP authorizations.
B#265768 SG-5810	Fixes an issue where the proxy stopped responding when **Nested Groups Support** was enabled in LDAP realm configuration.
B#267470 SG-5351	Fixes an issue where LDAP authorization failed when **Nested Groups Support** was enabled.
SG-8425	Fixes an issue where the proxy experienced a restart in PG:"PG_LSA", Process: "likewise Lsass_ ADSyncMachinePassword" in "liblikewise.exe.so" at .text+0x3ff5fc.

HTTP Proxy

ID	Issue
B#258588 SG-5900	Fixes an issue where HTTP debug log filters did not work unless both client and server IP address filters were set.
B#266536 SG-2503	Fixes an issue with memory pressure in the HTTP and FTP components when ProxySG policy or configuration required request body inspection (for example, when performing handoffs from the HTTP proxy, as with with MAPI or WebEx traffic).
B#265880 SG-4411	Fixes an XSS vulnerability in user-defined exception pages. Exception pages could contain unescaped user input within the Symantec Site Review URL.

ICAP

ID	Issue
B#265722 SG-6081	Fixes an issue where the event log did not display queued connection alert notifications. This issue occurred when max connections and thresholds were set to minimum values.

Management Console

ID	Issue
B#250440 SG-5853	Fixes an issue where the Overview, Content Analysis, and Sandboxing tabs displayed "Access Denied" when logging in as a read-only user.
B#265634 SG-5834	Fixes an issue where Bandwidth Management statistics incorrectly showed the CurrentBandwidth value in MBPS whereas the CLI reported values in KBPS.

Policy

ID	Issue
B#264770 SG-5074	Fixes an issue where a SAML exception was generated when trying to authenticate a tunnel request.
SG-8488	Fixes an issue where the presence of a `server_url=` rule in policy, whose condition was not met, prevented a configured exception in a matching rule from being served.

SSL/TLS and PKI

ID	Issue
SG-8429	Fixes an issue where the proxy was unresponsive in HTTP Admin and experienced memory pressure.

Storage

ID	Issue
B#261280 SG-7056	Addresses an issue where a ProxySG virtual appliance with only one defined disk experienced a restart in process "CEA Cache Administrator."

TCP/IP and General Networking

ID	Issue
B#254032 SG-4328	Addresses an issue where the appliance experienced a restart in process "stack-bnd-2:0-rxq-0" in "libstack.exe.so" when using IPv6. This issue occurred due to IP fragmentation.
B#261765 SG-5962	Addresses an issue where the appliance restarted in process group "PG_OBJECT_STORE" in process "CEA Cache Administrator."
B#264551 SG-5046	Fixes an issue with memory pressure in TCP/IP and DNS components when the DNS lookup name had a trailing dot ('.').
B#267052 SG-6152	Addresses an issue where the appliance stopped responding when a packet capture was started with a "coreimage" argument and then stopped via a `pcap stop` command.
B#267347 SG-6165	Addresses an issue where the appliance restarted when /TCP/wccp-routers did not show an IPv6 address correctly.
B#267052 SG-6152	Fixes an issue where taking a PCAP caused the Management Console to stop responding. This issue occurred when the buffer size was increased to the last matching 50000 KB.

URL Filtering

ID	Issue
B#26618, B#257744 SG-5181, SG-4561	Fixes an issue where differential updates of the Intelligence Services database caused increased disk load, which then caused delayed responses.

Web Visual Policy Manager

ID	Issue
SG-8612	Fixes a serious issue where policy that included a **User** object was replaced with a **Group** object when policy was applied. When this issue occurred, the incorrect policy was applied without compilation errors or messages.
SG-8462	Fixes a serious issue where viewing policy in the Web VPM caused the policy to be corrupted. This issue occurred after the policy was first applied in the Web VPM, and then applied again in the legacy Java VPM.
SG-8464	Fixes an issue where the VPM was unable to apply policy where a rule contained a **Destination Host/Port** object with no host defined.

SGOS 6.7.4.2 LA

Release Information

- **Release Date:** December 19, 2018
- **Build Number:** 229236

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Important Information About This Release

SGOS 6.7.4.2 contains an issue where using the new Web Visual Policy Manager causes unintended policy behavior when applying policy save/changes (SG-8612). Symantec recommends upgrading to "SGOS 6.7.4.3 PR" on page 70 to use the Web VPM without issue.

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

SGOS 6.7.4.2 is no longer available for download through MySymantec, but is available as a Limited Availability (LA) release. Please refer to your Symantec point-of-contact for details.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

SGOS 6.7.4.1 GA

Release Information

- **Release Date:** October 30, 2018
- **Build Number:** 226712

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
  - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
  - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.1

- SGOS 6.7.4.1 introduces new features and enhancements. See "Changes in SGOS 6.7.4.1 " on the next page.

Fixes in SGOS 6.7.4.1

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.1" on page 96.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Changes in SGOS 6.7.4.1

SGOS 6.7.4.1 introduces the following feature:

ProxySG SWG VA for the AWS Marketplace

The ProxySG virtual appliance (Secure Web Gateway edition, SGOS version 6.7.x) is now available in the Amazon Web Services (AWS) Marketplace. A ProxySG on AWS permits the same features and functionality as the Secure Web Gateway Virtual Appliance (SWG VA).

- More information:

  ProxySG for AWS Marketplace Deployment Guide

  https://www.symantec.com/docs/DOC11168

This release also introduces the following enhancements:

- The CLI command **#show user** has been renamed to **#show user-info**.
- CA certificates in the browser-trusted CCL have been updated. This updated trust package was posted for appliances on October 16, 2018. For more information, refer to ALERT2309:

  https://www.symantec.com/docs/ALERT2309
- This release includes additional security mechanisms which might result in an error message when using scripts to send CLI commands to the proxy. To prevent the error "Server requires a valid encrypted token in the request" from being returned by CLI command scripts, refer to TECH251582:

  https://www.symantec.com/docs/TECH251582

Changes to Policy

This release introduced a change to how the ProxySG appliance handles HTTPS forward proxy policy. For more information see KB article TECH254549.

Changes from Previous SGOS 6.7.4 Early Availability (EA) Releases

Features and changes in this release are cumulative and include the changes from previous SGOS EA releases:

- "Features in SGOS 6.7.4.141 EA" on the next page
- "Features in SGOS 6.7.4.130 EA" on page 86
- "Features in SGOS 6.7.4.107 EA" on page 88

Features in SGOS 6.7.4.141 EA

Changes to the Bootloader

The following changes have been made in SGOS 6.7.4.1 to the CLI command**`show installed-systems verbose`**:

- The command displays the SHA-256 boot chain signature.
- The command no longer displays the signature for the system image.

Hyper-V VA-20 MACH5 Edition Support

SGOS 6.7.4.1 introduces the ability to deploy a ProxySG virtual appliance (ProxySG VA) VA-20 model MACH5 edition on a Microsoft Hyper-V hypervisor.

Additionally, when creating the ProxySG VA, you now must specify the model type of the VA you are creating using the parameter `-model_type`, and can now specify multiple directories and optionally give your VA a name using the parameter `-vmname`.

- More information:

  ProxySG Virtual Appliance MACH5 Edition Initial Configuration Guide (Hyper-V Hypervisor)

Domain Fronting Detection

You can install policy on the ProxySG appliance to detect attempts at domain fronting. The following VPM **Source** column objects are available in the **Web Access Layer**:

- **HTTP Connect Hostname**: Tests the hostname (the host value in the first line of the HTTP CONNECT request) obtained from the original HTTP CONNECT request URL.

  CPL condition: `http.connect.host=`

  This object (and underlying condition) supports all substitution variables. For example, you can use the `$(url.host)` substitution variable to compare the value of the `url.host` against the value specified by this object.

- **HTTP Connect Port**: Tests the port (the port value in the first line of the HTTP connect request) obtained from the original HTTP CONNECT request URL.

  CPL condition: `http.connect.port=`

You can add the following new access log fields to an access log format to help track possible domain fronting attempts:

- `x-http-connect-host`
- `x-http-connect-port`
- More information:

  Content Policy Language Reference

Visual Policy Manager Reference

SGOS Administration Guide

IPv6 Support for WCCPv2

This release includes support for IPv6 for WCCPv2. To use this feature, select 2.0 for the WCCP version (**Configuration > Network > WCCP**) on the appliance and enable WCCP IPv6 on your routers.

This feature has the following limitations in this release:

- Only **L2** redirection is supported.
- Only **Mask** assignment type is supported; **Hash** is not supported.
- The default **Mask** value is 0x3f is not supported; you must specify a different value.
- Only **Individual Home Router Addresses** are supported; **Multicast Home Router** is not supported.
- **Individual Home Router Addresses** must include only IPv4 or only IPv6 addresses within the same Service Group.
- More information:

  SGOS Administration Guide

Features in SGOS 6.7.4.130 EA

Include Surrogate Realms to `realm=` Tests in Policy

This release supports adding a surrogate realm for user authentication. You can use this property in conjunction with the `realm=` condition. A realm specified in this property is used for surrogate authentication in addition to any other realms specified in `realm=` tests in policy.

The following CPL was added to support this feature:

`user.realm.surrogate(`*`isolation_realm_name`*`|no)`

where:

- *`isolation_realm_name`* is a surrogate authentication realm
- no means not to use a surrogate realm

Consider the following example:

```
; layer 1
<proxy>
  user.realm.surrogate(isolation)

...

; layer 2
<proxy> realm=corporate
  category=gambling exception(content_filter_denied)
```

The proxy evaluates layer 2 as if the layer guard were `realm=(corporate,isolation)` and applies the content filtering policy to users in those realms.

If Symantec Web Isolation is deployed upstream, you can include this property in policy for the proxy to authenticate users based on identity and group membership defined in Web Isolation.

- More information:

  Content Policy Language Reference

Default TCP Window Size Increase

The default TCP window size has been increased from 64k bytes to 256k bytes.

To view the current TCP window size, issue the CLI command:

```
> show tcp-ip
```

To change the TCP window size, issue the CLI command:

`#(config)`**`tcp-ip window-size`** *`value`*

- More information:

  Command Line Interface Reference

SGOS Upgrade/Downgrade WebGuide

Specify Upstream Server CCL for Forwarded Transctions

You can now specify the upstream server CCL certificate for forwarded transactions. Include the existing CPL property `server.certificate.validate.ccl()` in the `<forward>` layer.

- More information:

  Content Policy Language Reference

Features in SGOS 6.7.4.107 EA

Multiple Local Content Filtering Databases

Numerous updates and changes have been made to support multiple local databases on the appliance. In addition to the existing local content filtering database, you can now create up to seven more local databases. Configure each database using the following CLI:

```
#(config local database_name) { clear | download { all-day | auto | between-hours | cancel
| encrypted-password | get-now | password | url | username } } | exit | noparameters | source |
view }
```

where:

- *database_name* is **default** for the default local database or the custom name of an additional database.
- *parameters* are certain parameters that can be negated.

Commands previously used to configure the default database are now available under `#(config local)` and `#(config local default)`.

After you configure additional local databases, enable them using the following command:

```
#(config content-filter) provider local enabledatabase_name
```

Categories in all enabled local databases are available in the following areas:

- In the VPM: the list in **Configuration > Edit Categories**; the **Request URL Category**, **Server URL Category**, and **Server Certificate Category** objects.
- In the new **Categories** report. See "Content Filtering Categories Report" below for details.
- Testing and viewing categories through **Configuration > Content Filtering > General**.
- In access logs, where adding field `cs-categories-qualified` to the log format displays categories qualified by provider in the form *category_name@provider_name*.

You can monitor the health of the local databases in Health Monitoring, under the **Local Database default** and **Local Database *database_name*** Communication Status metrics.

- Full information:

  ***SGOS Administration Guide* — Filtering Web Content *and* Monitoring the Appliance**

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

  ***Visual Policy Manager Reference* — Visual Policy Manager**

Content Filtering Categories Report

The Management Console has a new Categories report (**Statistics > Categories**), which includes data on requests to URLs with categories in enabled provider databases. For example, if you enable the Blue Coat content filtering provider, the report shows statistics for categories according to current WebPulse data. You can refer to the Blue Coat categories statistics to write and maintain your organization's content filtering policies.

The report shows category statistics for the following content filtering providers when enabled:

- Blue Coat (WebFilter or Intelligence Services data source)
- Local databases
- YouTube categories
- Categories defined in on-box policy

The report also shows system-defined categories that indicate content filtering service issues such as `none` and `uncategorized`.

- Full information:

  ***SGOS Administration Guide* — Filtering Web Content**

FTPS Proxy Support

> **Note:** SSLV integration does not support FTPS offload.

The ProxySG appliance can now intercept FTPS connections in both explicit and implicit mode. The appliance intercepts explicit FTPS connections using the FTP proxy type and needs no additional configuration. To intercept implicit FTPS connections, configure the new FTPS proxy service in the following ways:

- In the Management Console (**Configuration > Services > Proxy Services**).
- In the CLI, using new `#(config ftps)` commands.

The following FTP properties can be used for FTPS transactions:

```
ftp.match_server_data_ip()
ftp.server_connection()
ftp.server_data()
ftp.welcome_banner()
```

Symantec recommends using secure ICAP servers for FTPS. The following properties can be used for FTPS transactions:

```
request.icap_service()
response.icap_service()
request.icap_service.secure_connection()
response.icap_service.secure_connection()
```

In addition, `ftp.method=` tests `AUTH`, `PBSZ`, and `PROT` methods in implicit FTPS transactions.

> **Caution:** If you intend to downgrade to a version prior to SGOS 6.7.4, you must first take additional steps to roll back the implicit FTPS configuration. Failure to do so can result in dropped explicit and implicit FTPS connections. Before downgrading, set existing FTPS listeners to **Bypass** and remove any `ftp.method=` policy that specifies implicit FTPS methods.

- Full information:

  SGOS Administration Guide - Managing the FTP Proxy

  Command Line Interface Reference — Privileged Mode Configure Commands

  Content Policy Language Reference — Property Reference* and *Condition Reference

  SGOS Upgrade/Downgrade Guide

EDNS Support in DNS Proxy

This release introduces extension mechanisms for DNS (EDNS), which allows DNS requesters to receive DNS UDP messages longer than the default 512 bytes. Refer to RFC6891 and RFC2671 for information on EDNS.

EDNS request messages consist of the following sections:

- constant section - Includes an acceptable DNS response size. The DNS proxy uses this value to send long responses.
- variable section - The DNS proxy does not parse this section in this release and transparently forwards it to upstream DNS server instead.

Previously, EDNS queries were ignored and transformed into regular DNS queries. Starting with this release, when EDNS is enabled on the appliance, the DNS proxy:

- accepts EDNS queries
- allocates DNS RESPONSE buffers with respect to the original queries
- forwards EDNS variable sections to the upstream DNS server
- saves long DNS server responses in the DNS cache
- creates long responses to EDNS clients

Use the following CLI to enable/disable EDNS:

```
#(config)dns edns {disable | enable}
```

- Full information:

  SGOS Administration Guide - Managing the DNS Proxy

  Command Line Interface Reference — Privileged Mode Configure Commands

IPv6 Support for DNS Proxied Requests

The DNS Proxy checks IPv6 (AAAA) DNS queries for the following CPL conditions:

- `dns.request.category=` can test the content filtering category associated with hostnames in DNS IPv6 queries.
- `dns.request.threat_risk_level=` can test the threat risk level of hostnames in DNS IPv6 queries.

- Full information:

  Content Policy Language Reference — Conditions Reference

ADN Support for MAPI/HTTP Protocol

This release adds ADN support for MAPI/HTTP protocol. In an ADN deployment, the branch peer intercepts and compresses Office 365 traffic before sending it to the concentrator peer. The concentrator then decompresses the traffic before forwarding it.

> **Note:** Accelerating MAPI/HTTP over ADN requires both the branch and concentrator peers to be running version 6.7.4. If you downgrade either the branch or the concentrator peer to a version previous to 6.7.4, disable some configuration settings as appropriate. Refer to the *SGOS Administration Guide* for details.

- Full information:

  SGOS Administration Guide — Managing Outlook Applications

Reverse Proxy SNI Support

This release supports server name indication (SNI) in reverse proxy mode. Previously, SNI was supported for forward proxy only. Proxy chaining and ADN deployments are also supported. When SNI information is available in explicit and transparent HTTPS reverse proxy connections, the SNI is used for the `server.url=` condition.

You can now specify existing keylists in the HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**). When creating or editing an HTTPS reverse proxy service, the **Keyring** menu now displays all keyrings and keylists configured on the appliance.

In addition, you can now set one keyring as the default keyring in a keylist, to ensure that a keyring is used in cases where the client has not implemented SNI or sends incompatible SNI information.

The following CLI commands have been updated:

```
#(config proxy-services) create https-reverse-proxy service-name service-group [keyring|keylist]
```

Create a new HTTPS reverse proxy service with the specified name, service group, and keyring or keylist.

```
#(config service-name)attribute keyringkeyring|keylist
```

Edit an HTTPS reverse proxy service with the specified keyring or keylist.

```
#(config ssl)editkeylist
#(config keylist)default-keyring keyring
```

Specify the default keyring within a keylist.

A `$(ServerName)` extractor has been added; choose **ServerName** in the Field menu when building the extractor in a keylist. As with other supported extractors, **ServerName** does not allow duplicate values on keyrings within a keylist. If no match is found for the domain, and the keylist includes a keyring with a wildcard certificate, that keyring is used.

Caution: If you intend to downgrade to a version prior to SGOS 6.7.4, you must first remove keylists from HTTPS reverse proxy service configurations. Before downgrading, create new services or edit existing ones that do not include keylists.

- Full information:

  SGOS Administration Guide — Configuring and Managing an HTTPS Reverse Proxy

  Command Line Interface Reference — Privileged Mode Configure Commands

  Content Policy Language Reference — Condition Reference

  SGOS Upgrade/Downgrade Guide

Customizable Anti-CSRF Token Name

This release allows you to customize the anti-CSRF token name using the new CPL property:

`http.csrf.token.name(`*`string`*`)`

where *string* is a custom token name.

The anti-CSRF token that is inserted using `http.csrf.token.insert()` has a default name of `CSRF-Token`; thus, by specifying a custom token for legitimate requests, you can make it difficult for malicious users to determine the name of the token and identify the WAF solution in your deployment.

When a custom anti-CSRF token is set in CPL, you can view the source of a browser form to verify that it shows `var antiCsrfTokenName = "<`*`custom_token_name`*`>"`.

A suspected CSRF attack is written to access logs when the expected token name–whether that is the default `CSRF-Token` or the custom name–is not present. Make sure that the access log format includes the `x-bluecoat-waf-monitor-details` and `x-bluecoat-waf-attack-family` fields.

- Full information:

  Content Policy Language Reference — Property Reference

  Web Application Firewall Solutions Guide

Authenticate SCP Uploads Using SSH Client Key

You can create and store SSH client keys on the appliance. These SSH client keys can be used for authentication, as an alternative to using a password, when uploading access logs via SCP.

Specify Authentication Method for SCP Upload Client

To support using SSH keys for authentication, the following CLI was added:

`#(config log `*`log_ID`*`)scp-client authentication {password|client-key|all}`

Specify the authentication method for the SCP client for the log, where:

- `password` means that only password authentication is used
- `client-key` means that only SSH client key authentication is used
- `all` means that client keys are attempted for authentication first; if that fails, password authentication is attempted

Manage SSH Client Keys

To manage SSH client keys, the following CLI was added:

```
#(config ssh-client client-keys)create ecdsa {nistp256 | nistp384 | nistp521}
```

Creates an ECDSA key with the specified curve. The keys are stored in the SSH keyring.

```
#(config ssh-client client-keys)create ed25519
```

Creates an Ed25519 key. The keys are stored in the SSH keyring.

```
#(config ssh-client client-keys)create rsa {2048 | 3072 | 4096}
```

Creates an RSA key with the specified bit size. The keys are stored in the SSH keyring.

```
#(config ssh-client client-keys)delete {rsa | ecdsa | ed25519}
```

Deletes the specified key.

```
#(config ssh-client client-keys)inline {rsa | ecdsa | ed25519} [<passphrase>] <eof-marker>
```

Imports a private key of the specified type. You can import a plain private key or an encrypted one, using the passphrase parameter. The import format can be PEM (PKCS1), PKCS8, or the OpenSSH format. The keys are stored in the SSH keyring.

```
#(config ssh-client client-keys)view private {rsa | ecdsa | ed25519} <passphrase>
```

Displays configured private keys, or the specified type of private key, in the OpenSSH format. You must enter a passphrase that consists of at least eight characters. The passphrase will be used to encrypt the view output.

- Full information:

  Command Line Interface Reference — Privileged Mode Configure Commands

More Secure SSH and SSL Private Key Display in `show config` Output

To improve security, new CLI was added for specifying how `show config` output displays SSH and SSL private keys:

```
#(config) security private-key-display aes128-cbcpassphrase [<passphrase>]
```

Displays private keys using AES128-CBC encryption. Optionally, set the passphrase to use with encryption. The passphrase must be at least eight characters in length.

```
#(config) security private-key-display aes256-cbcpassphrase [<passphrase>]
```

Displays private keys using AES256-CBC encryption. Optionally, set the passphrase to use with encryption. The passphrase must be at least eight characters in length.

```
#(config) security private-key-display none
```

Omits private keys in `show config` output.

`#(config) security private-key-display passphrase [<passphrase>]`

Sets the passphrase to use with encryption.The passphrase must be at least eight characters in length.

`#(config) security private-key-display unencrypted`

Displays private keys in plaintext. Symantec recommends that you do not use this command.

- Full information:

  Command Line Interface Reference — Privileged Mode Configure Commands

  SGOS Upgrade/Downgrade Guide

Enhancements in this Release

This release includes the following enhancements:

SSL Handshake

The SSL handshake has been modified to use the proxy's Client Hello for increased resiliency.

Session ID and Certificate Size Log Fields

The following access log fields have been added to help track session ID and certificate size:

- `x-cs-session-id`: The SSL session ID on the client side returned or resumed by the appliance for the current SSL session.
- `x-rs-session-id`: The SSL session ID returned or resumed by the server for the current SSL session.
- `x-cs-server-certificate-key-size`: Certificate type and size in bytes of server certificate key used by client-side connection, such as "RSA[2048]". Pertains to exchanged public keys, not negotiated ciphers.
- `x-rs-server-certificate-key-size`: Certificate type and size in bytes of server certificate key used by server-side connection, such as "RSA[2048]". Pertains to exchanged public keys, not negotiated ciphers. "Client-side" refers to the server certificate instantiated for the client-side connection (as opposed to the client-side client certificate).

Currently, Symantec does not plan to add fields for client certificates used by the client-side or server-side connection. If no certificate exists (for example, on the client side without client certificate negotiation), the access log field is blank.

Enable/Disable Site Awareness

This release introduces a new CLI command to enable or disable AD site awareness:

`#(config security windows-domains)site-aware [enable|disable]`

By default, the setting is enabled. If disabled, a site name will not be returned for the domain, even if one exists.

For details, refer to TECH247930:

http://www.symantec.com/docs/TECH247930

IPv6 Support for IWA Direct

IWA Direct authentication is now supported over IPv4 and IPv6 connections.

View All SSH Client Information

The following CLI was added:

```
#(config ssh-client)view {subcommands}
```

View all SSH client information.

Clear WebPulse Cache

This release introduces the ability to clear the WebPulse cache using the new CLI command:

```
#(config bluecoat)service clear-cache
```

Clearing the WebPulse cache takes effect whether WebFilter or Intelligence Services is the data source.

Use this command instead of disabling and re-enabling the WebPulse service, for example, when a URL is categorized incorrectly.

Increased Number of Categories Per URL

The appliance now supports policy that includes up to 1000 categories per URL without a significant impact on performance. See B#251992 in "SGOS 6.7.x Known Issues" on page 198 for details.

Removed Application Attribute Groups CLI

The application attributes groups CLI was introduced in version 6.7.2.1 but has been non-functional. The CLI is now removed from the appliance.

Improved Application Attribute Lookup Times

Application Attributes lookup performance is improved.

JavaScript Policy Enhancements

The following policy definitions have been enhanced in this release.

Specify <script> attributes in a JavaScript transformer:

```
define javascript transformer_id
    javascript-statement ::= section-type [tag_attributes='attributes'] replacement
end
```

The optional tag_attributes='attributes' adds the specified attributes within the <script> start tag. The tag is applicable to prolog and epilog sections only.

Use a regular expression replacement to rewrite JavaScript:

```
define url_rewrite transformer_id
   rewrite_script_regex "client_substring_with_back_ref" "server_regex_substring"
end
```

Fixes in SGOS 6.7.4.1

SGOS 6.7.4.1 includes bug fixes. This update:

Access Logging

B#	Issue
264727	Fixes an issue where the access log client did not clean up connections to a disconnected host failed to respond to ARP requests.

Build

ID	Issue
B#264981 SG-6038	The virtual appliance image is now marked as signed in the meta.txt file.

CLI Consoles

B#	Issue
264835	Fixes an issue where the proxy restarted in process group "PG_SSH" in process "SSHD Admin".
265188	Fixes an issue where the proxy experienced a watchdog restart in the SSH process when a very large volume of data was being transferred.

FTP Proxy

B#	Issue
258947	Fixes an issue where the proxy restarted in process "FTP CW 101E23EF430" in "libcfssl.exe.so" when trying to establish the data connection after setting "PROT p" with the FTP proxy.

ICAP

B#	Issue
261093	Fixes an issue where the proxy had various page-fault restarts when using an ICAP request mirror.

MAPI Proxy

B#	Issue
262429	Fixes an issue in the "Mapi.http.worker" process in "libmsrpc.exe.so" when there were more than 9,007 entries in the scan cache.

Management Console

B#	Issue
264849	Fixes an issue where read-only admins were unable to retrieve BWM class statistics.

Policy

B#	Issue
257890	Fixes an issue where the management console was unresponsive when certain combinations of customized policy and the DNS server setup could cause a DNS lookup for "cache".
263979	Fixes an issue where the "request.x_header.header_name.exists=" CPL condition does not work with a custom header_name.

SSL/TLS and PKI

B#	Issue
256750	Fixes an issue where the proxy was unable to perform SfB video calling.
256750	Fixes an issue where Skype for Business Video calling and screen sharing did not work.

SSL Proxy

B#	Issue
265084	Fixes an issue where the SSL session cache size was limited to 48000 sessions regardless of available memory space.

SSLV Integration

B#	Issue
258714	Fixes an issue where WebSocket connections failed when SSLV offload was enabled.

TCP/IP and General Networking

B#	Issue
260764	Fixes an issue where the proxy experienced a page fault restart in PG_TCPIP in process "RTMP Live Splitter 1147A3B58A0".
263386	Fixes an issue where the appliance restarted in process "HTTP CW 30AC5946A40" in "libstack.exe.so" at .text+0x319837.

Utility Libraries

B#	Issue
264891	Fixes CVE-2017-7375.

Fixes from Previous SGOS 6.7.4 Early Availability (EA) Releases

Fixes in this release are cumulative and include the fixes from previous SGOS EA releases:

- "Fixes in SGOS 6.7.4.141" on page 102
- "Fixes in SGOS 6.7.4.130" on page 108
- "Fixes in SGOS 6.7.4.111" on page 117
- "Fixes in SGOS 6.7.4.107" on page 120

SGOS 6.7.4.141 EA

Release Information

- **Release Date:** September 18, 2018
- **Build Number:** 224477

> **Note:** SGOS 6.7.4.141 is an Early Availability (EA) release with new/advanced functionality.
>
> Previously, Symantec released new features in Limited Availability (LA) releases to specific customers to access new functionality. This meant other customers were not able to access these new capabilities until the release was General Availability (GA). With Early Availability releases, all customers under valid support entitlement can gain access to this new functionality.
>
> Customers running this release should be considered early adopters of SGOS 6.7.4 to access new and advanced functionality. Early Availability releases are supported like any other current SGOS release. Once the Early Availability release achieves broader adoption and quality metrics, it will transition to LTR status.
>
> SGOS 6.7.4.1 GA was released on October 30, 2018.

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later

- **SSL Visibility:** 4.2.4.1 and later
  - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
  - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893
- For information on Java 11 support, refer to TECH252566

  http://www.symantec.com/docs/TECH252566

Upgrading To/Downgrading From This Release

- When upgrading your ProxySG virtual appliance (VA) from version 6.7.3.x to 6.7.4.x, Symantec Management Center version 1.11.x and later might report that the ProxySG VA's serial number has changed and prompt you to RMA the device. This behavior is expected, and does not indicate a problem with the serial number. In addition, this issue affects only VAs with licenses that allow duplicate serial numbers. For more information on this issue, including resolution steps, refer to TECH251392:

  https://www.symantec.com/docs/TECH251392

  The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.141

- SGOS 6.7.4.141 introduces new features and enhancements. See "Changes in SGOS 6.7.4.1 " on page 82 for details.

Fixes in SGOS 6.7.4.141

- This release includes a number of fixes. See "Fixes in SGOS 6.7.4.141" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.141

Bug Fixes in this Release

SGOS 6.7.4.141 includes bug fixes. This update:

Authentication

B#	Issue
260520	Fixes an issue where the threshold monitor restarted the appliance due to increased memory pressure in SSL and Cryptography.
261934	Fixes an issue where using the CLI to test Windows SSO authentication with nested groups enabled caused the appliance to restart.
262567	Fixed an issue where the domain and IWA direct realm had an unhealthy status when the appliance was functioning properly.
263768	Fixes an issue where the appliance restarted in process "`CLI_Worker_1`" in "`liblikewise.exe.so`" when joining a domain before leaving the current domain.

HTTP Proxy

B#	Issue
252242	Fixes an issue where the appliance restarted in process "`HTTP CW 1093D428A40`" in "`libstack.exe.so`" when SSL interception was on.
263076	Fixes an issue where the sc-bytes and cs-bytes values were incorrect in the access log when protocol detect was enabled.
264217	Fixes an issue where the appliance restarted in process group "`PG_POLICY_HTTP`" in process "`PDW t=58806 for=2C005E9`" in "`libc.so`" when the policy had rules to inspect raw response headers (such as, `response.raw_headers.regex`).

ICAP

B#	Issue
260165	Fixes an issue where the appliance did not send content to ICAP when the HTTP response header "trailer" followed chunked data encoding.
261869	Fixed an issue where the appliance restarted after reconfiguring the ICAP service and then changing the sense-settings feature.

IPv6 Stack and IPv6 Proxies

B#	Issue
263695	Fixes an issue in process "`WCCP_Admin`" in "`libwccp.exe.so`".

Mnanagement Console

B#	Issue
260464	Fixes an issue where the bandwidth statistics in the console displayed incorrect statistics for the parent class.
261869	Fixes an issue where attempting to add an existing CA certificate that had a name containing spaces to a CCL via a Management Console failed.

Policy

B#	Issue
262711	Fixes an issue where some tenant policies were missing after upgrading to SGOS 6.7.3.x.

Services

B#	Issue
261499	Fixes an issue where the default listener for TCP Port 514 could not be removed.

SSL/TLS and PKI

B#	Issue
261878	Fixes an issue where the threshold monitor restarted the appliance due to increased memory pressure in SSL Cryptography when SSL traffic was offloaded to an SSLV appliance.
262151	Fixes a memory pressure issue in the SSL Cryptography cache where the license automatically updated every day.

SSL Proxy

B#	Issue
258828	Fixes an issue where the appliance restarted in `PG_POLICY` when a policy trace was enabled and traffic was sent.
262837	Fixes an issue where the appliance experienced a page-fault restart in process group `PG_CFSSL` in process `HTTP RW EECB14B90`.

System Statistics

B#	Issue
262919	Fixes a service disruption that occurred after executing a clear statistics persistent CLI command.

TCP/IP and General Networking

B#	Issue
256018	Fixes an issue where the appliance restarted in process group "`PG_TCPIP`" in process "`HTTP SW 80F5AE4FA40 for 70FA5135A40`" in "`libstack.exe.so`".

B#	Issue
258974	Fixes an issue where the appliance stalled during start-up if the first DNS server in the primary group was unreachable.
262273	Fixes an issue where the failover did not work correctly if the interface was disabled for the backup appliance.
263272	Fixes an issue where the appliance returned a false attack in the progress status from an SNMP walk.
263341	Fixes an issue that caused a restart in process `cookie-monster` in `libstack.exe.so` on edge boxes that were using ADN after upgrading to 6.7.3.9.

URL Filtering

B#	Issue
256952	Fixes an issue that occurred when renaming a category where the previous category name displayed until rebooting the appliance.
257088	Fixes an issue where the risk level names in the Threat Risk Details UI summary were incorrect.
260887	Fixes an issue where the appliance restarted in process group `PG_POLICY_SOCKS` in process `PDW t=840754458 for=4002E9` in `liburl_filter.exe.so`.
263782	Fixes an issue where configuring WebPulse to use a region based domain (for example, webpulse-us.es.bluecoat.com) added an invalid "service secure enable" which caused an error.

VPM

B#	Issue
263518	Fixes an issue where policy could not be added using the VPM, even though it could be added via the CLI or CPL.

Web Application Firewall

B#	Issue
263811	Fixes an issue where the appliance restarted in process group "`PG_WAF`" in process "`HTTP CW 70FAB6B2A40`" in "`libwaf.so`" when the CPL "`engine=injection.command`" was used.

Windows Media Proxy

B#	Issue
262275	Fixes an issue where RTSP streaming did not work in a reverse proxy deployment.

SGOS 6.7.4.130 EA

Release Information

- **Release Date:** July 9, 2018
- **Build Number:** 220877

> **Note:** SGOS 6.7.4.141 is an Early Availability (EA) release with new/advanced functionality.
>
> Previously, Symantec released new features in Limited Availability (LA) releases to specific customers to access new functionality. This meant other customers were not able to access these new capabilities until the release was General Availability (GA). With Early Availability releases, all customers under valid support entitlement can gain access to this new functionality.
>
> Customers running this release should be considered early adopters of SGOS 6.7.4 to access new and advanced functionality. Early Availability releases are supported like any other current SGOS release. Once the Early Availability release achieves broader adoption and quality metrics, it will transition to LTR status.
>
> SGOS 6.7.4.1 GA was released on October 30, 2018.

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later

- **SSL Visibility:** 4.2.4.1 and later
  - When using TLS offload, SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
  - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1.
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.130

- SGOS 6.7.4.130 introduces new features and enhancements. See "Changes in SGOS 6.7.4.1 " on page 82 for details.

Fixes in SGOS 6.7.4.130

- This release includes a number of fixes and patch release fixes. See "Fixes in SGOS 6.7.4.130" on page 108.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.130

SGOS 6.7.4.130 includes security advisory (SA) fixes and bug fixes.

Security Advisory Fixes in this Release

SGOS 6.7.4.130 includes security advisory fixes. This update:

B#	Issue
258695	Addresses issue where multiple SAML libraries might have allowed authentication bypass via incorrect XML canonicalization and DOM traversal. Refer to SA167.

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://www.symantec.com/security-center/network-protection-security-advisories

Bug Fixes in this Release

SGOS 6.7.4.130 includes bug fixes. This update:

Access Logging

B#	Issue
259923	Fixes a condition where the cache admin gets overloaded with requests from the access log admin. This caused HTTP workers to spike out and resulted in delays.

Authentication

B#	Issue
260100	Fixes an issue where configuring an LDAPS realm might cause a restart during startup due to a race condition.
250240	Fixes an issue where the appliance is not able to decode SAML assertions, causing SAML authentication to fail.
258845	Addresses an issue where the appliance restarted in process group PG_LSA in process "likewise Netlogon_PingCLDAP" in "liblikewise.exe.so".
259915	Fixes an issue where the login dialog was bypassed when accessing the Management Console through port 8082.
259571	Addresses an issue where the proxy restarted in process "likewise lwmsg server worker" in "liblikewise.exe.so" (IWA Direct).
259905	Fixes an issue where the `Federated IDP SLO POST URL` item was missing in the `#(config)security saml view-realm` CLI command output.

Client Manager

B#	Issue
256189	Fixes an issue where an "Invalid archive" error occurred when attempting to upgrade Unified Agent using the **Local File** option.

Collaboration

B#	Issue
257124	Fixes an issue where client protocol detection policy `client.protocol=` condition did not match WebEx operations as expected. Now, the following CPL matches WebEx operations: `client.protocol=https`

Documentation

B#	Issue
260400	Addresses missing information in the description of `response.icap_feedback.force_interactive()` in the *Content Policy Language Reference*. The section now indicates that the property cannot be used to override `Always check with source before serving object` or `always-verify-source`.
260983	Removes erroneous information in the description of custom upload client for access logs in the *SGOS Administration Guide* and online help. The documentation now specifies that the custom client can use IPv4 addresses only.

HTTP Proxy

B#	Issue
257793	Fixes an issue where downloads from www.filefactory.com did not work when CachePulse was enabled.

Licensing

B#	Issue
259628	Fixes an issue where the `licensing request-key` command failed if the password contained special characters (such as a plus sign or percent symbol) or a space.

Management Console

B#	Issue
259239	Fixes a configuration issue that occurred when a user-created CCL name includes a space.
253734	Fixes an issue where a second IPv6 gateway, added via the Management Console, did not appear in the Management Console. When this issue occurred, the CLI command `show ip-default-gateway` output displayed the gateway correctly.
258679	Fixes an issue where the system did not delete the default route from the Management Console, even though it was deleted from the routing table, when the interface IP address was changed or deleted.

Network Drivers

B#	Issue
257086	Addresses an issue where the Secure Web Gateway Virtual Appliance restarted in process group "PG_TCPIP" in process "NIC I/O 0:0-xn_n 0" in "xn.exe".

Policy

B#	Issue
252541	Restores **BlockPopupAds** functionality in the VPM. The object can now be used in VPM policy rules without causing a 'Warning: Unreachable statement' error.
259748	Fixes an issue where the policy parser ignored whether or not an `end` was present when a definition was at the end of the policy.

Proxy Forwarding

B#	Issue
259850	Fixes an issue where the Active count did not decrement on **Statistics > Advanced** pages /Forwarding/StatsIP and /Forwarding/StatsSummary. This issue occurred when a forwarding host was in use and certificate verification failed during a HTTP/FTP-based document transfer.

SNMP

B#	Issue
260655	Fixes an issue where a MIB file could not be loaded into an SNMP monitoring tool that did not support the Integer64 data type.

SOCKS Proxy

B#	Issue
258865	Addresses an issue where the appliance restarted in process group "PG_SOCKS" in process "Socks dpm proprietor" in "libstack.exe.so".

SSL Proxy

B#	Issue
257012	Fixes an issue where the `x-cs-server-certificate-key-size` access log field erroneously displayed `RSA[1024]` in bypass mode.
258274	Addresses an issue where the appliance became unresponsive and failed to intercept traffic when using STunnel.
258130	Fixes an issue where `http.request.apparent_data_type` and `http.request.data.N` policy were not enforced.

SSL/TLS_and_PKI

B#	Issue
260255	Addresses an issue where the appliance failed to import a DER-encoded Certificate Revocation List (CRL) larger than 64k bytes.

SSLV Integration

B#	Issue
256791	Fixes an issue in SSLV offload mode where increasing the TCP window size might have resulted in stalled connections.

Security

B#	Issue
259884	Fixes an issue where the appliance stopped responding due to an authenticated user's specially-crafted HTTP request to the management service.
258634	Restricts some proxy CLI commands and functionality when logged in as read-only user.
257344	Improves the security posture of Client Manager service on port 8084 by removing weak ciphers and TLS versions.
259310	Fixes an issue where, under very specific conditions and for a short duration of time, user data was cached even though the OCS specified not to cache it.
259626	Addresses NULL injection issues in Management Console request handling.
258121	Extends memory resource allocation for proper regex evaluation by policy code.
256740	Fixes an issue where read-only users could access features and information that should be allowed only to read-write users.

TCP/IP and General Networking

B#	Issue
256543	Fixes an issue where DNS resolution failed when the first server in a custom DNS server list stopped working.
255057	Fixes an issue where auto-linklocal IPv6 addresses could not be deleted when the interface had link-aggregation set.
258812	Fixes an issue where the `client.interface` gesture showed an invalid card number (such as 255:255.x) in the policy trace when WCCP had router affinity set to "both" or “client”.
260856	Addresses an issue where the appliance restarted in process "Threshold_Monitor" after about thirty days of operation.
259971	Fixes a performance issue with L2 return WCCP and bypass.
257434	Addresses an issue where the appliance experienced a restart in PG_TCPIP in process "SGRP Worker" in "libstack.exe.so" when the network cable was removed. This issue occurred when SGRP was using the same multicast address.
259677	Addresses an issue where the appliance experienced a restart in TCP/IP process "stack-admin" in "libstack.exe.so.
260330	Addresses an issue where the appliance experienced a watchdog restart with hardware exception 0x2 and software exception 0x11 in process "idler 0" in "kernel.exe".
257272	Fixes an issue where downloads of large files via SOCKS proxy on high-speed networks (speeds of 2 Mbps and higher) timed out. This issue occurred when the proxy did not update the TCP window size.

URL Filtering

B#	Issue
257872	Addresses an issue where the appliance stopped responding during initial bootup.
256858	Fixes an issue where a specific URL took a long time to load when DRTR is running in the background.
255954	Fixes an issue where some SSL websites did not load, even if WebPulse was running in background mode.
256148	Addresses an issue where content filtering consumed high amounts of memory, causing threshold monitor to stop responding.
246810	Fixes an issue where the local content filtering database did not clear a subscription error after connectivity to database server was restored.

Visual Policy Manager

B#	Issue
258598	Fixes an issue where the VPM caused extraneous categories to be appended to the generated policy.
258187	Fixes an issue where the **Service Name** and **Service Group** objects were not visible in the Service column in the Web Request Layer.

SGOS 6.7.4.111 EA

Release Information

- **Release Date:** April 18, 2018
- **Build Number:** 217066

> **Note:** SGOS 6.7.4.141 is an Early Availability (EA) release with new/advanced functionality.
>
> Previously, Symantec released new features in Limited Availability (LA) releases to specific customers to access new functionality. This meant other customers were not able to access these new capabilities until the release was General Availability (GA). With Early Availability releases, all customers under valid support entitlement can gain access to this new functionality.
>
> Customers running this release should be considered early adopters of SGOS 6.7.4 to access new and advanced functionality. Early Availability releases are supported like any other current SGOS release. Once the Early Availability release achieves broader adoption and quality metrics, it will transition to LTR status.
>
> SGOS 6.7.4.1 GA was released on October 30, 2018.

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later

- **SSL Visibility:** 4.2.4.1 and later
  - SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1 when using TLS offload.
  - SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1. SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4.
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.4.111

- This release includes a number of fixes and patch release fixes. See "Fixes in SGOS 6.7.4.111" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.111

SGOS 6.7.4.111 includes bug fixes and changes included in the 6.7.4.108 EA. This update:

Authentication

B#	Issue
259265	Fixes an issue where a RADIUS access request packet showed an incorrect NAS-IP-Address attribute.

SSL Proxy

B#	Issue
258994	Addresses an issue where the proxy experienced a restart in process group "PG_CFSSL" in process "SSLW 111DA576FC0" in "libtransactions.exe.so" during error handling.
259171	Fixes an issue where policy trace handoff transaction IDs were incorrect.

SGOS 6.7.4.107 EA

Release Information

- **Release Date:** March 22, 2018
- **Build Number:** 215655

> **Note:** SGOS 6.7.4.107 is an Early Availability (EA) release with new/advanced functionality.
>
> Previously, Symantec released new features in Limited Availability (LA) releases to specific customers to access new functionality. This meant other customers were not able to access these new capabilities until the release was General Availability (GA). With Early Availability releases, starting with 6.7.4.107, all customers under valid support entitlement can gain access to this new functionality.
>
> Customers running this release should be considered early adopters of SGOS 6.7.4 to access new and advanced functionality. Early Availability releases are supported like any other current SGOS release. Once the Early Availability release achieves broader adoption and quality metrics, it will transition to LTR status.
>
> SGOS 6.7.4.1 GA was released on October 30, 2018.

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.2.4.1 and later

- SGOS 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1 when using TLS offload.
- SSL session reuse was previously not supported when using TLS offload with SGOS 6.7.4 and SSLV 4.2.4.1. SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4.

- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.4.107

- SGOS 6.7.4.107 introduces new features and enhancements. See "Changes in SGOS 6.7.4.1 " on page 82 for details.

Fixes in SGOS 6.7.4.107

- This release includes a number of fixes and patch release fixes. See "Fixes in SGOS 6.7.4.107" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.4.107

SGOS 6.7.4.107 includes bug fixes and fixes from 6.7.4.105 - Patch Release Fixes. This update:

Access Logging

B#	Issue	Fixed In
251081	Fixes an issue where access log configuration copied from a ProxySG appliance and imported to another ProxySG appliance were not identical. With this fix, the `show config` output shows any changes to the mapi-http and DNS log formats.	6.7.4.101
250158	Fixes an issue where the output for **`#show config`** did not indicate that SCP was set as the upload client.	6.7.4.101
250180	Fixes an issue where the log tail for a selected log in the Management Console (**Statistics > Access Logging > Log Tail**) displayed the same entries multiple times when new entries did not appear.	6.7.4.102
253658	Fixes an issue where continuous access log upload stopped after logging directory slots ran out.	6.7.4.107

Authentication

B#	Issue	Fixed In
253544	Fixes an issue where the appliance could contact only DCs in the local Active Directory (AD) site to which the appliance belonged. As a result, because an appliance requires a read-write domain controller to join a domain, appliances with only local access to a read-only DC were unable to join the AD domain.	6.7.4.105
256029	Fixes an issue where Kerberos authentication failed after the appliance's machine account password was changed in Active Directory and the machine account was enabled for aes-256 bit encryption.	6.7.4.107
252851	Fixes an issue where the SNMP Schannel configuration stored incorrect CLI commands in the configuration archive, which prevented the configuration from being restored.	6.7.4.107
255299	Fixes an issue where the proxy experienced a page fault restart in process "HTTP CW F95FD4B90" in "libc.so" related to the timing of actions when using the auth/debug log URL.	6.7.4.107
253745	Fixes an issue where the domain controller (DC) reset the connection when the appliance sent an SMB1 Echo Request in an SMB2 environment.	6.7.4.107
254717	Fixes an issue where AES authentication with Kerberos failed if the Kerberos load balancer username contained an upper-case letter.	6.7.4.107

CLI Consoles

B#	Issue	Fixed In
255576	Fixes an issue where issuing the `#show config` command might have caused the appliance to restart if the URL set using `#(config)`**`statistics-export config-path`** was invalid.	6.7.4.107

Health Monitoring

B#	Issue	Fixed In
254545	Fixes an issue where the power supply severity setting (`alert severity sensor power-supply`) did not persist after an upgrade.	6.7.4.107

Kernel

B#	Issue	Fixed In
252191	Fixes an issue where policy did not install if it contained non-existent AD groups.	6.7.4.107

Management Console

B#	Issue	Fixed In
250120	Fixes an issue where the dialog for creating a new HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**) on a Secure Web Gateway Virtual Appliance or ProxySG Virtual Appliance MACH5 Edition did not allow you to scroll.	6.7.4.105
254660	Fixes an issue where the Management Console did not accept system image download URLs consisting of more than 227 characters.	6.7.4.107

MAPI Proxy

B#	Issue	Fixed In
249746	Fixes an issue where email attachment scan results were cached, but subsequent attachment downloads were sent to the ICAP server again instead of using previously cached data.	6.7.4.105

Network Drivers

B#	Issue	Fixed In
255462	Fixes an issue where the Secure Web Gateway virtual appliance (ESX) might have restarted in process "NIC I/O 1:0-vmx_n 0-rxq-txq" in "vmxnet3.exe".	6.7.4.107

SSL Proxy

B#	Issue	Fixed In
252087	Fixes an issue where the appliance did not use the SNI extension in the server-side connection, which was required by some servers to respond with the correct server certificate in the TLS handshake.	6.7.4.105

SSL/TLS and PKI

B#	Issue	Fixed In
250120	Fixes an issue where you could not create a new HTTPS Reverse Proxy service in the Management Console (**Configuration > Services > Proxy Services > New Service**).	6.7.4.105

TCP/IP and General Networking

B#	Issue	Fixed In
252086	Fixes an issue where the appliance might have experienced a restart in PG_TCPIP when Virtual IP was configured in failover mode.	6.7.4.107

URL Filtering

B#	Issue	Fixed In
254474	Fixed an issue where differential database updates for Intelligence Services were causing increased loads on disks, which caused delayed responses.	6.7.4.107
249253	Fixes an issue where the WebPulse tab (**Configuration > Threat Protection > WebPulse**) did not display database download status if Intelligence Services was enabled.	6.7.4.105
256160	Fixes an issue where WebPulse did not categorize websites in a child/parent configuration when a valid forwarding host was not supplied.	6.7.4.107
248868	Fixes an issue where enabling the Application Classification service took longer.	6.7.4.107

Visual Policy Manager

B#	Issue	Fixed In
255321	Fixes an issue where the appliance sent an `invalid_request` exception error page if you logged out of the Management Console and then tried to access the consent banner URL again with same browser.	6.7.4.107

SGOS 6.7.3.12 PR

Release Information

- **Release Date:** September 24, 2018
- **Build Number:** 224754

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.3.12

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.12" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.12

SGOS 6.7.3.12 includes the following security advisory fixes and bug fixes.

SSL Proxy

B#	Issue
265084	Fixes an issue where the cache size for the SSL session was limited to 48000 sessions, regardless of available memory space.

SGOS 6.7.3.11 PR

Release Information

- **Release Date:** September 14, 2018
- **Build Number:** 224391

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.3.11

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.11" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.11

SGOS 6.7.3.11 includes the following security advisory fixes and bug fixes.

Authentication

B#	Issue
258695	Fixes CVE-2018-5241.
263768	Fixes an issue where the appliance restarted in process "CLI_Worker_1" in "liblikewise.exe.so" when joining a domain before leaving the current domain.
253544	Fixes an issue where the appliance was not able to join the active directory (AD) domain if it only had access to a local, read-only domain controller (RODC). This issue occurred because the appliance needs a read-write domain controller (RWDC) to join an AD domain. In prior versions, the appliance could contact other RWDCs in remote locations to join. The fix is a newCLI command that allows you to configure “Active Directory Site Awareness” under "security windows-domains". By default, it is enabled. If disabled, a site name will not be returned for the domain, even if one exists. Please see http://www.symantec.com/docs/TECH247930 for more information.
262019	Fixes an issue where the appliance was unresponsive after HTTP workers spiked.

CLI_Consoles

B#	Issue
254410	Fixed an issue where the proxy restarted in process group "PG_CLI" in process "CLI_Worker_2" in "libc.so" when the "(config ssh-client known-hosts)fetch-host-key" command was executed in the CLI.

HTTP Proxy

B#	Issue
257452	Fixes a software restart in process group "PG_CFSSL" in process "HTTP SW 3B4CB2CB50 for 2E394F2B50".
252242	Fixes an issue where the appliance restarted in process "HTTP CW 1093D428A40" in "libstack.exe.so" when SSL interception was on.
264217	Fixes an issue where the appliance restarted in process group "PG_POLICY_HTTP" in process "PDW t=58806 for=2C005E9" in "libc.so" when the policy had rules to inspect raw response headers (such as, response.raw_headers.regex).

SSLV Integration

B#	Issue
258714	Fixes a case of websocket connection failure that occurred when SSLV offload was setup.

TCP/IP and General Networking

B#	Issue
255319 SG-6805	Fixes an issue where the appliance experienced a restart in process "HTTP SW 40047170A40 for 30F29CC2A40" in "libstack.exe.so".
256018	Fixes an issue where the appliance restarted in process group "PG_TCPIP" in process "HTTP SW 80F5AE4FA40 for 70FA5135A40" in "libstack.exe.so".
260654	Fixes an issue where a unit with a 10Gb fiber NIC stopped processing packets.

URL Filtering

B#	Issue
254474	Fixes an issue where Intelligence Services differential database updates caused increased disk load, which sometimes caused delayed responses.

SGOS 6.7.3.10 PR

Release Information

- **Release Date:** August 10, 2018
- **Build Number:** 222765

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.3.10

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.10" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.10

SGOS 6.7.3.10 includes the following security advisory fixes and bug fixes.

Authentication

B#	Issue
262567	Fixes an issue where the domain and IWA direct realm displayed as unhealthy when the system was functioning properly.
260100	Fixes an issue where configuring an LDAPS realm might have caused a restart during start-up due to a race condition.
260520	Fixed an issue where the threshold monitor restarted the proxy due to increased memory pressure in SSL and Cryptography.

Policy

B#	Issue
262711	Fixes an issue where some tenant policies were missing after upgrading to 6.7.3.x.

SSL/TLS and PKI

B#	Issue
261878	Fixes an issue where the threshold monitor restarted the appliance due to an increase in memory pressure in SSL Cryptography. The increase in pressure occurred when the appliance was offloading SSL traffic to an SSLV appliance.

TCP/IP and General Networking

B#	Issue
263341	Fixes a restart in process "`cookie-monster`" in "`libstack.exe.so`" on edge boxes that use ADN. This issue occurred after upgrading to 6.7.3.9.

SGOS 6.7.3.9 PR

Release Information

- **Release Date:** July 9, 2018
- **Build Number:** 220719

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.3.9

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.9" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.9

SGOS 6.7.3.9 includes the following security advisory fixes and bug fixes.

Authentication

B#	Issue
255998	Fixes an issue where the appliance hung when the Windows SSO realm was performing self-authorization. A CLI command (return-ldap-dn) was added to enable or disable the retrieval of the user's LDAP FQDN from Active Directory. By default, this command is enabled for backward compatibility.

HTTP Proxy

B#	Issue
258976	Fixes an issue where a webpage did not load and a 503 error was returned.

Proxy Forwarding

B#	Issue
259850	Fixes an issue where the 'Active' count did not decrement on advanced-URL pages "`/Forwading/StatsIP`" and "`/Forwarding/StatsSummary`". This issue occurred when a forwarding host was used and the certificate verification failed during an HTTP/FTP-based document-transfer process.

SSLV Integration

B#	Issue
261964	Fixes an issue where the appliance restarted after it received a TLS1.3 cipher suite value in the emulated server handshake from an SSLV appliance.

TCP/IP and General Networking

B#	Issue
259460	Fixes an issue where the appliance restarted in process group "`PG_TCPIP`" in process "`stack-bnd-2:0-rxq-0`" in "`libstack.exe.so`".

URL Filtering

B#	Issue
246810	Fixes an issue where the local content-filter database did not clear a subscription error after connectivity to the database server was restored.

VPM

B#	Issue
258187	Fixes an issue in the Web Request Layer where the service name or service group objects were not displayed in the service column.

SGOS 6.7.3.8 PR

Release Information

- **Release Date:** June 1, 2018
- **Build Number:** 219260

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Fixes in SGOS 6.7.3.8

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.8" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.8

SGOS 6.7.3.8 includes the following security advisory fixes and bug fixes.

TCP/IP and General Networking

B#	Issue
260856	Fixes an issue where the proxy restarts in Threshold_Monitor in "" at .text+0x0 where the TCPIP component is the biggest consumer of memory.

SGOS 6.7.3.7 PR

Release Information

- **Release Date:** May 1, 2018
- **Build Number:** 217919

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x andlater
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.3.7

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.7" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.7

SGOS 6.7.3.7 includes the following security advisory fixes and bug fixes.

Security Advisory Fixes in this Release

SGOS 6.7.3.7 includes security advisory fixes. This update:

B#	Issue
253827	Addresses security vulnerabilities. Refer to SA162.

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://www.symantec.com/security-center/network-protection-security-advisories

Bug Fixes in this Release

SGOS 6.7.3.7 includes bug fixes. This update:

Authentication

B#	Issue
254934	Improves the performance of a proxy operating in a heavily utilized IWA direct environment using KCD.

Client Manager

B#	Issue
256189	Fixes an issue where Unified Agent could not be updated using a local file on the proxy. The following error message was received, "Error: Invalid archive: Bad checksum".

Collaboration

B#	Issue
251617	Fixes an issue where a proxy may experience a restart in process "WebExWorker" in "libforwarding.exe.so" when WebEx Proxy connections were forwarded to different hosts or proxies.

Event Logging

B#	Issue
253715	Fixes an issue where the proxy experienced a restart in SNMP due to memory pressure. This issue occurred when the mail server was not reachable but mail requests continued to be added to the queue.

HTTP Proxy

B#	Issue
256743	Fixes an issue the proxy experienced a restart at 0x7fff0003 in process "HTTP CW 84E43DB50" when implementing a "request.icap_mirror(yes)" policy on a specific ICAP server.
259310	Fixes an issue where, under very specific conditions and for a short duration of time, user data was cached even though the OCS specified not to cache it.

Management Console

B#	Issue
253734	Fixes an issue where a subsequent IPv6 gateway added through the Management Console was not displayed in the Management Console; however, the `show ip-default-gateway` CLI command output did display the gateway.
258679	Fixes an issue where the default route was not removed from the Management Console even though it was deleted from the routing table when the interface IP address was changed or deleted.

SOCKS Proxy

B#	Issue
251496	Fixes an issue where the SOCKS UDP Associate failed to work with certain applications.

SSL Proxy

B#	Issue
252087	Fixes an issue where the appliance did not use the SNI extension in server-side connections. The extension is required by some servers in order to respond with the correct server certificate in the TLS handshake.
255761	Fixes an issue where the SSL session cache size was set too low on the SG-VA-C4L platform, resulting in high CPU usage.
258274	Fixes an issue where the proxy became unresponsive and failed to intercept traffic when using STunnel.

TCP/IP and General Networking

B#	Issue
256543	Fixes an issue where DNS resolution failed when the first listed server in a custom DNS group stopped working.
257053	Fixes an issue where the appliance became slow due to packets that were not processed within the queues associated with each NIC.
257272	Fixes an issue where attempts to download large files via SOCKS proxy on high-speed networks (2Mbps+ speed) timed out. This issue occurred because the proxy did not update the TCP window size.
257434	Fixes an issue where the proxy experienced a restart in PG_TCPIP in process "SGRP WOrker" in "libstack.exe.so" when the network cable was removed while SGRP was using the same multicast address.

B#	Issue
258812	Fixes an issue where the `client.interface` property showed an invalid card number (such as 255:255.x) in the policy trace. This issue occurred when WCCP had router affinity set to "both" or “client”.
258918	Fixes an issue where the proxy experienced slowness on a model with an ixgbe driver when using VLAN, bridging, and bypass.
259677	Fixes an issue where the proxy experienced a restart in TCP/IP process "stack-admin" in "libstack.exe.so.

URL Filtering

B#	Issue
256148	Fixes an issue where the proxy experienced a Threshold Monitor restart with content filtering consuming the highest amount of memory.
256160	Fixes an issue where WebPulse did not categorize websites in a child/parent configuration when a valid forwarding host was not supplied.

Visual Policy Manager

B#	Issue
255321	Fixes an issue where a user who logs out of the Management Console, and then tries to access the consent banner URL again, receives an invalid_request exception error page.

SGOS 6.7.3.6 GA

Release Information

- **Release Date:** March 30, 2018
- **Build Number:** 216168

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Fixes in SGOS 6.7.3.6

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.6" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.6

SGOS 6.7.3.6 includes the following bug fixes. This update:

Access Logging

B#	Issue
253658	Fixes an issue where continuous access log upload stopped after logging directory slots ran out. The workaround for this issue was to reset the log facility slots by deleting the log objects using the `commands delete-logs` CLI command.

Authentication

B#	Issue
256029	Fixes an issue where Kerberos authentication failed after the appliance's machine account password was changed in Active Directory and the machine account was enabled for AES-256 bit encryption.

CLI Consoles

B#	Issue
255358	Addresses an issue where the Advanced Secure Gateway appliance under load might have experienced a restart in process "tenable@ssh" in "libcli.exe.so".
255576	Fixes an issue where issuing the `#show config` command might have caused the appliance to restart if the URL set using `#(config)`**`statistics-export config-path`** was invalid.

Kernel

B#	Issue
252191	Fixes an issue where policy might not have installed when it included non-existent groups.

Network Drivers

B#	Issue
255462	Addresses an issue where the Secure Web Gateway virtual appliance (ESX) might have restarted in process "NIC I/O 1:0-vmx_n 0-rxq-txq" in "vmxnet3.exe".

SGOS 6.7.3.5 GA

Release Information

- **Release Date:** February 13, 2018
- **Build Number:** 213938

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Changes in SGOS 6.7.3.5

- You can now track policy setting updates for diagnostics purposes. The event log tracks the changes with the text "Policy update settings from...".

Fixes in SGOS 6.7.3.5

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.5" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.5

SGOS 6.7.3.5 includes the following bug fixes. This update:

Access Logging

B#	Issue
256116	Fixes an issue where the ProxySG appliance occasionally failed to boot. In this state, the appliance was not accessible using the Management Console but was accessible via SSH console.

Authentication

B#	Issue
257199	Addresses an issue where the ProxySG might have restarted in Process: "LDAP Authenticator" in "libopenldap.exe.so" when follow referrals were enabled on the LDAP realm.

Kernel

B#	Issue
256335	Addresses an issue where the ProxySG appliance might have restarted in process "SSLW 10A271CA060" in "libservices.exe.so".

MAPI Proxy

B#	Issue
251762	Fixes an issue where the ProxySG appliance might have restarted in Process: "EPM Worker" when MAPI was enabled.

Management Console

B#	Issue
255167	Fixes an issue where adding an "Authentication required" comment in policy in version 6.7.3.1 caused the Management Console to automatically log out after a successful policy installation.

Policy

B#	Issue
254751	Fixes a memory leak in configuration (Process group PG_CFG).

SSL Proxy

B#	Issue
253406	Fixes an issue causing increased SSL memory utilization.
254374	Fixes an issue where accessing an HTTPS site failed with an error "Client certificate not received" due to the appliance being unable to send the imported client certificate.
255468	Addresses an issue where the appliance might have restarted in Process group: "PG_CFSSL"in process "HTTP SW 1097B7B5A40 for 10968ABBA40".

TCP/IP and General Networking

B#	Issue
255160	Addresses an issue where the ProxySG 9000 might have become unresponsive during an upgrade to version 6.7.3. When this issue occurred, the serial console was still responsible.
255536	Fixes an issue where bandwidth management did not work correctly when used in a nested class.
255540	Fixes an issue where Connection Forwarding (CCM) may cause the appliance to restart in Process "NIC I/O 0:0-em_n 0 Deallocation worker" when forwarding a connection to another ProxysySG appliance via IPIP.
256204	Fixes an issue where the appliance might have restarted in Process: "cookie-monster" in "libmemory.so" when CCM (Connection Forwarding) is enabled.
256213	Fixes an issue where the appliance restarted when starting or stopping a packet capture (PCAP) with filters and the PCAP reaches its limit.
256391	Fixes an issue where the appliance might have restarted in Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so" with encapsulated IPv6 traffic.
256718	Fixes a memory leak In TCP/IP when port spoofing was configured.

SGOS 6.7.3.2 GA

Release Information

- **Release Date:** 12/12/2017
- **Build Number:**211128

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Changes in SGOS 6.7.3.2

- SGOS 6.7.3.2 introduces the following new CLI to allow you to configure the defer threshold and maximum connections:

```
#(config)content-analysis
#(config content-analysis)edit bluecoat-local-request
#(config icap bluecoat-local-request)max-conn <number_of_connections>
ok
#(config icap bluecoat-local-request)exit
#(config content-analysis)edit bluecoat-local-response
#(config icap bluecoat-local-response)defer-threshold <threshold_as_percentage>
ok
#(config icap bluecoat-local-response)max-conn <number_of_connections>
ok
```

Note the following about the commands:

- `max-conn<number_of_connections>` applies to both request and response service.
- `defer-threshold <threshold_as_percentage>` applies to only the response service.

> **Note:** These settings are not persistent across reboots. This limitation will be addressed in a future release.

Fixes in SGOS 6.7.3.2

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.2" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.3.2

SGOS 6.7.3.2 includes bug fixes. This update:

TCP/IP and General Networking

B#	Issue
253748	Fixes an issue where the appliance might have restarted in process "cookie-monster" due to a small race condition affecting connections that were required to retransmit packets over a long period.
254461	Fixes an issue where the appliance might have become unresponsive during the upgrade to 6.7.3.1 when IWA Direct authentication was used.

SGOS 6.7.3.1 GA

Release Information

- **Release Date:** 11/21/2017
- **Build Number:** 210008

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Director:** 6.1.x
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x; 2.1.x and later
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.3.1

- SGOS 6.7.3.1 introduces new features and enhancements. See "New Features in SGOS 6.7.3.1" on the next page.

Fixes in SGOS 6.7.3.1

- This release includes a number of fixes. See "Fixes in SGOS 6.7.3.1" on page 158.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

New Features in SGOS 6.7.3.1

SGOS 6.7.3.1 introduces the following new features.

Policy for Specifying Cookie Persistence in Authentication

You can now control cookie persistence during user authentication. The following CPL action was added:

`authenticate.persist_cookies(auto|no|yes)`

where:

- `auto` means that the cookie persistency value configured in the realm will be used.
- `no` means that the session cookie will be used in authentication in this transaction.
- `yes` means that the persistent cookie will be used in authentication in this transaction.
- Full information:

  Content Policy Language Reference

Specify the Client Certificate Validation CCL via VPM

A **Set Client Certificate Validation CCL** object is available in the Visual Policy Manager (VPM). Use this object to specify the client certificate list (CCL) to use for matching intercepted SSL connections.

This policy object generates the following CPL (the condition was added in version 6.7.2):

`client.certificate.validate.ccl(`*`CCL_ID`*`)`

To use the policy object, add a rule to the **SSL Intercept Layer** and select **Set Client Certificate Validation CCL** from the Action column.

- Full information:

  Visual Policy Manager Reference

Enhancements and Changes in ProxySG 6.7.3.1

ProxySG 6.7.3.1 introduces the following enhancements and changes:

- For integration with Content Analysis on-box sandboxing, specify port 8082 (requires CA v2.1 or later).

SSL Intercept and DNS Layers Supported in Tenant Policy

SSL Intercept and DNS transactions now evaluate tenant determination policy in the landlord policy file. This allows `<ssl-intercept>` and `<dns>` layers to be defined and executed in tenant-specific policy. Previously, these layers were supported in the default tenant policy only.

ICAP Outbound Source IP Selection

When a network interface on the appliance is configured to use multiple IP addresses, the outbound source IP address used in the connection from the ProxySG appliance to the ICAP server is now selected in a round-robin manner. This selection process helps prevent port saturation under heavy load, especially when the connection is not persistent.

Data Leak Exception Page

Users now see a data leak exception page when HTTP/HTTPS POST requests are sent to Symantec DLP and a policy violation occurs.

HTTP Log Shows Reasons for Non-Cacheable Transaction

The HTTP log now indicates the reason(s) that a transaction is not cacheable. The information is logged as follows:

`"Server response made transaction Non-Cacheable:reason(s)=<set of reasons>"`

OpenLDAP Upgrade

This release supports OpenLDAP version 2.4.44.

Fixes in SGOS 6.7.3.1

SGOS 6.7.3.1 includes bug fixes. This update:

Access Logging

B#	Issue
251081	Fixes an issue where access log configuration copied from a ProxySG appliance and imported to another ProxySG appliance were not identical. With this fix, the `show config` output shows any changes to the mapi-http and DNS log formats.
250158	Fixes an issue where the output for **`#show config`** does not indicate that SCP was set as the upload client.
250180	Fixes an issue where the log tail for a selected log in the Management Console (**Statistics > Access Logging > Log Tail**) displayed the same entries multiple times when new entries did not appear.

Authentication

B#	Issue
251438	Setting the windows-domains LDAP ping protocol as UDP might cause the appliance to restart.

CLI Consoles

B#	Issue
250624	Fixes an issue where exceptions viewed via the Management Console (exceptions_config.html) had links that did not show current exceptions.

Collaboration

B#	Issue
252297	Fixes an issue where a failure during handoff caused the WebEx proxy to restart in process "WebExWorkerManager" in "libc.so".
249338	Fixes an issue where the **Details** field in Active Sessions didn't display information for 'symc.webex.com' connections.

HTTP Proxy

B#	Issue
247731	Fixes an issue where pipelined requests did not follow routing domain rules.

Kernel

B#	Issue
246322	Fixes an issue where the appliance restarted due to a page fault at 0xfffffffffffffc0 in process group "PG_CFSSL" in process "HTTP CW 3D18931B50" in "kernel.exe".

B#	Issue
250933	Fixes an issue where the appliance was unresponsive until it was rebooted. The issue was caused by a large memory allocation from CFS downloader.

Policy

B#	Issue
250453	Fixes an issue where the CPU0 usage was high when policy was updated in a multi-tenant policy configuration.
250179	Fixes an issue where the exceptions file (**Configuration > Exceptions > View > Exceptions Configuration**) did not show currently-defined exceptions. Clicking any link of a known exception displayed the message "No exception found called '<*exception_name*>'".

SSL Proxy

B#	Issue
252794	Fixes an issue where the RSA public exponent was always 3 for emulated certificates. For best security, the public exponent now copies the existing public exponent for RSA server certificates.

SSL/TLS and PKI

B#	Issue
248792	Fixes an issue where the threshold monitor restarted the proxy. This issue occurred when the SSL and crypto memory usage were high.

TCP/IP and General Networking

B#	Issue
249805	Fixes an issue where both proxies in a failover group reported as master. This issue occurred when the group was configured with link aggregate (LAG) interfaces.
252709	Fixes an issue where the proxy stopped sending requests to the origin content server (OCS).
251889	Fixes an issue where Bandwidth Management Class with a child configured stopped a TCP connection. This issue occurred when the parent's maximal bandwidth was reached.
244784	Fixes an issue where packets might have exited an incorrect interface in IPv6 configuration when static routes were configured.

SGOS 6.7.2.3 PR

Release Information

- **Release Date:** November 14, 2017
- **Build Number:** 209751

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 through 1.10.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x, and 2.1.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- An incompatibility exists between SGOS 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:
  http://www.symantec.com/docs/TECH246741

Fixes in SGOS 6.7.2.3 PR

- For fixes in this release, see "Fixes in SGOS 6.7.2.3 PR" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.2.3 PR

ProxySG 6.7.2.3 includes bug fixes. This update:

SSL Proxy

B#	Issue
253377	Fixes an issue where random HTTPS pages did not load when SSL Proxy was used. Refer to TECH248154 for details: http://www.symantec.com/docs/TECH248154

TCP/IP and General Networking

B#	Issue
250616	Fixes an issue where the appliance might have restarted in Process group: "PG_TCPIP", Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so". This issue occurred when delayed intercept was enabled.
250637	Fixes an issue where the appliance might have restarted in Process group: "PG_TCPIP" in Process: "stack-api-worker-0" in "libmemory.so". This issue occurred when dynamic bypass was enabled.

SGOS 6.7.2.2 PR

Release Information

- **Release Date:** September 12, 2017
- **Build Number:** 206438

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 through 1.10.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x, and 2.1.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

- An incompatibility exists between SGOS 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:
  http://www.symantec.com/docs/TECH246741

Fixes in SGOS 6.7.2.2 PR

- For fixes in this release, see "Fixes in SGOS 6.7.2.2 PR" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.2.2 PR

HTTP Proxy

B#	Issue
250638	ProxySG may restart in Process: "HTTP SW 100C7373A40 for 4062EB83A40" in "libce_admin.exe.so" when FSH caching is enabled, disk is full and reinitializing.

SSL Proxy

B#	Issue
251011	When running SGOS 6.7.2.1, accessing some HTTPS sites will fail with Chrome or Fire Fox, when Protocol Detection is enabled or SSL Interception is not enabled.
250323	SG may restart in process: "CFSSL Cert Proprietor" in deployments with hundred(s) of CCL's and 600+ certificates.

TCP/IP and General Networking

B#	Issue
250732	Bandwidth Management may stop working after a while for higher limits (range of 100 Mbps and up).
250495	ProxySG may experience a software exception code: 0x810001 in Process group: "PG_TCPIP" in Process: "stack-admin" causing the unit to restart when Bandwidth Management is enabled.

SGOS 6.7.2.1 GA

Release Information

- **Release Date:** July 31, 2017
- **Build Number:** 204664

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 through 1.10.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x, 1.3.x, and 2.1.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **ProxySG Appliances:**
  - S500, S500-30, S400, S200
  - 300, 600, 900, 9000 (supported: 9000-20B, 9000-30, 9000-40; not supported: 9000-5, 9000-10, or 9000-20)
  - SWG V100
  - SG-VA high-performance models (refer to specific deployment guide for details)
  - MACH5 VA-5, 10, 15, 20

  See "ProxySG Appliance Resources" on page 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- An incompatibility exists between SGOS 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:

  http://www.symantec.com/docs/TECH246741

- SGOS 6.7.2.1 is the first 6.7.x release that supports Application Delivery Network (ADN). ADN performance issues reported previously in SGOS 6.6.x are fixed in this release. Consider using this release or the latest 6.7.x release if you use ADN in your environment.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.2.1

- SGOS 6.7.2.1 introduces new features and enhancements. See "New Features in SGOS 6.7.2.1" on the next page.

Fixes in SGOS 6.7.2.1

- For fixes in SGOS 6.7.2.1, see "Fixes in SGOS 6.7.2.1" on page 174.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

New Features in SGOS 6.7.2.1

SGOS 6.7.2.1 introduces the following new features.

Authenticate Outbound SSH Connections

You can add host keys, select ciphers, and select HMACs to use for outbound SSH connections, such as the SCP upload client for access logs. See "Configure SCP Upload Client " below for details.

To configure host keys, ciphers, and HMACs in the Management Console, select **Configuration > Authentication > SSH Outbound Connections**.

To obtain a host key from a remote host, use the Management Console (**Configuration > Authentication > SSH Outbound Connections > Known Hosts**).

The following CLI commands were added to support this feature:

```
#(config ssh-client)ciphers
#(config ssh-client)hmacs
#(config ssh-client)known-hosts
```

- Full information:

  ***SGOS Administration Guide* — Controlling Access to the Internet and Intranet**

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

Configure SCP Upload Client

SGOS supports the secure copy protocol (SCP) upload client for access log uploads. To configure SCP for access log upload, select **Configuration > Access Logging > Logs > Upload Client**. Select **SCP** for the Client type.

The following commands were added to support this feature:

```
#(config log log_name)client-type scp
#(config log log_name)scp-client
```

> **Note:** Before you can configure the SCP upload client, you must add host keys and select ciphers and HMACs for outbound SSH connections, as described in " Authenticate Outbound SSH Connections " above.

Kerberos Constrained Delegation

In deployments where the User Principal Name (UPN) is not included in client certificates, configure Kerberos Constrained Delegation (KCD) to use the authorization username for authentication. Use the following CLI command:

```
#(config)security iwa-direct edit-realm realm_name
#(config iwa-direct realm_name)kcd-use-authz-name enable
```

where *realm_name* is your IWA realm name.

- Full information:

  Using Kerberos Authentication in a Reverse Proxy Environment

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

Support for Application Groups

This release introduces CASB policy that organizes similar web applications into named groups. This feature improves ease of use by providing you with the ability to write policy for groups of similar applications instead of writing multiple rules for individual applications. In addition, note that:

- Applications can belong to more than one group.
- As new application are added, removed, or modified, the group information automatically reflects the change. Application group policy and reporting are also updated.

To use this feature:

- Ensure that the appliance has a valid subscription for the CASB Audit AppFeed for SG. Modifications to CASB data are automatically provided in database updates via the subscription feed.
- Enable the Application Classification service.
- Select Intelligence Services as the content filtering data source.

The following were added to support this feature:

- The ability to look up application groups for a URL and display the list of groups (in the Management Console, **Configuration > Application Classification > General**).
- In the `bcreportermain_v1` and `bcsecurityanalytics_v1` access log formats, an `x-bluecoat-application-groups` field.
- An **Application Group** VPM object used to apply policy actions to a specified application group.
- A CPL condition `request.application.group=` to test the specified application group for a URL
- A CLI subcommand that displays supported application groups or the groups to which the specified application belongs:

  `#(config application-classification)`**`view groups`** `[`**`application`** `<`*`application_name`*`>]`

- Full information:

  ***SGOS Administration Guide* — Filtering Web Content, Creating Custom Access Log Formats, *and* Access Log Formats**

  ***Visual Policy Manager Reference* — The Visual Policy Manager**

  ***Content Policy Language Reference* — Condition Reference**

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

Possible Values of Application Attributes

> **Note:** The data feed for this feature will be in SGOS 6.7.4. To use this feature, upgrade to 6.7.4 when that release is available.

This release introduces a CLI subcommand to display possible values for a specified application attribute:

- `#(config application-attributes)view possible-values <attribute_name>`

  If an attribute name contains spaces, enclose it in double quotation marks ("). When writing policy that includes the `request.application.<attribute_name>=` condition, use this subcommand to ensure that the CPL parameters are valid.

To use this feature:

- Ensure that the appliance has a valid subscription for CASB Audit AppFeed for SG. Modifications to CASB data are automatically provided in database updates via the subscription feed.
- Enable the Application Classification and Application Attributes services.
- Select Intelligence Services as the content filtering data source.
- Full information:

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

SGOS on Cisco Cloud Services Platform

SGOS 6.7.2 introduces the ability to deploy a ProxySG virtual appliance (Secure Web Gateway edition) running on the Cisco Cloud Services Platform (CSP) 2100. To start, you require a valid license and a QCOW2 image downloaded from Symantec Support Center.

SGOS on CSP permits the same features and functionality as the Secure Web Gateway Virtual Appliance (SWG VA). Refer to Symantec documentation for deployment steps.

- Full information:

  SGOS on Cisco Cloud Services Platform Deployment Guide

  > **Tip:** For details beyond the scope of Symantec documentation, refer to the CSP documentation: http://www.cisco.com/c/en/us/support/switches/cloud-services-platform-2100/products-installation-guides-list.html

Enhancements and Changes in SGOS 6.7.2.1

SGOS 6.7.2.1 introduces the following enhancements and changes:

Ability to Add Kafka `MessageSet` Headers to Access Logs

If an access log has Kafka client and gzip file type selected, you can configure the appliance to add a `MessageSet` header to the compressed log files so that the Kafka broker processes the data correctly as gzip-compressed data.

Use the following command to enable/disable the header (by default, the setting is disabled):

`#(config log` *`Log_name`*`)`**`kafka-client`** `[`**`no`**`]` **`message-set-codec`**

Refer to the *Command Line Interface Reference* for details on this command.

Making any change to an access log's upload client configuration that reverses the previous `MessageSet` header state (that is, the header's presence or absence in the log files) can cause future log uploads to fail. You must take additional steps to ensure that logs are processed correctly; for details, refer to the *SGOS Administration Guide*.

Cipher and HMAC Support in FIPS Mode

After booting the appliance in FIPS mode, issue the following CLI commands to view the default cipher/HMAC lists, current selections, and available ciphers/HMACs:

```
#(config ssh-console)view ciphers
#(config ssh-console)view hmacs
#(config ssh-client ciphers)view
#(config ssh-client hmacs)view
```

AES-GCM and SHA384 Ciphers Support

The appliance now supports the following cipher suites for reverse proxy, Management Console, SSL device profiles, and the SSL client as well as the existing forward proxy support:

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-GCM-SHA384

Enhanced CCL Policy

This release adds support for configuring the CA Certificate List (CCL) to use for a specific IP address or hostname. When this object is not used, the default server certificate validation CCL is applied.

- Full information:
- ***SGOS Administration Guide* - Specifying an Issuer Keyring and CCL Lists for SSL Interception**
- ***Visual Policy Manager Reference* - The Visual Policy Manager**
- ***Content Policy Language Reference* - Properties Reference**

Skype for Business Support

In previous versions of SGOS, some Skype For Business and Microsoft Lync application connections failed when the appliance intercepted SSL traffic on port 443 and UDP port 5061 was firewall-restricted. Some issues occurred with logging in, joining meetings, meeting audio, and starting presentations. Issues occurred due to the following limitations:

- Lack of OCSP stapling/Certificate Revocation List (CRL) distribution point support
- Partial support for Session Initiation Protocol (SIP)
- Lack of support for Microsoft Traversal Using Relay NAT (MS-TURN) protocol

To restore chat client communications, this SGOS release supports:

- CRL distribution points on emulated certificates, which you configure in the SSL proxy service
- SIP and MS-TURN protocol detection and policy control, which you configure in the <ssl-access> layer
- Full information:
- ***Office 365 Integration & Best Practices WebGuide*** **- Skype/Lync Fix: SGOS Configuration**
- ***SGOS Administration Guide*** **- Managing Outlook 365 Applications**
- ***Visual Policy Manager Reference*** **- The Visual Policy Manager**
- ***Content Policy Language Reference*** **- Conditions Reference *and* Properties Reference**
- ***Command Line Interface Reference*** **- Privileged Mode Configure Commands**

Fixes in SGOS 6.7.2.1

SGOS 6.7.2.1 includes the following security advisory fixes and bug fixes.

Bug Fixes in this Release

SGOS 6.7.2.1 includes bug fixes. This update:

ADN

B#	Issue
243691	Fixes ADN performance issues. ADN is supported in SGOS 6.7.2.1 and later.

HTTP Proxy

B#	Issue
244110	Fixes an issue where HTTP(S) proxy upstream requests didn't have `Host` header canonicalized per RFC7230.

Management Console

B#	Issue
249339	Fixes an issue where using links (for example, from your site's internal webpages) to ProxySG advanced URLs could result in "400 Bad Request" errors.

SSLV Integration

B#	Issue
243726	Fixes an issue where `#show config` output did not reflect spaces in SSLV device IDs.

SGOS 6.7.1.3 PR

Release Information

- **Release Date:** May 26, 2017
- **Build Number:**202038

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 through 1.8.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **ProxySG Appliances:**
  - S500, S500-30, 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 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Fixes in SGOS 6.7.1.3

- SGOS 6.7.1.3 is a patch release that includes a number of fixes. See "Fixes in SGOS 6.7.1.3 PR" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.1.3 PR

SGOS 6.7.1.3 is a Patch Release that includes the following bug fixes:

Hardware Driver

B#	Issue
247078	Output errors from the Intel 10GB (ixgbe) interface card on SG-S400 and SG-S500. These "Output errors" are not indicating any issues and can be ignored in 6.7.1.1 and 6.7.1.2. This is fixed in SG 6.7.1.3 and later.

Kernel

B#	Issue
246096	ProxySG may restart with a page fault at 0x2073f349000 in Process group: "PG_POLICY_HTTP" in Process: "PDW t=6084547 for=ED801C9F" in "libc.so".

Network Drivers

B#	Issue
243485	Proxy SG ESX VA: once the e1000 interface is disabled, re-enabling it may not activate the link until a reboot.
247235	Added NDIO Statistics for packets, errors and drops for the ixgbe driver.
247185	After upgrading SG 9000 to either 6.7.1.1 or 6.7.1.2, it is not possible to manually set the speed link to 1Gbps. Workaround: Ensure all NICs are using auto negotiate for speed and duplexing configurations.

SSL Proxy

B#	Issue
247892	ProxySG may trigger a threshold monitor restart due to high SSL memory pressure.
245923	Hardware restart in Process group: "PG_TCPIP" in Process: "SSLW 40599BD2060" in "libstack.exe.so".

TCP/IP and General Networking

B#	Issue
247788	ProxySG CLI and MC may become unresponsive after enabling CCM on peers.
246441	After upgrading to 6.7.1.1 or 6.7.1.2, when using IWA Direct, in case the Active Directory server is not responding to LDAP pings, CPU usage might be increasing to 100% and the SG would restart in threshold monitoring after reaching acceptance regulation.
245737	After upgrading to 6.7.1.1 or 6.7.1.2, transparent interception using WCCP/GRE is not working correctly.
247512	Netflow interface configuration is not showing details of interfaces (no information under interface, in & out).
245625	Page fault in Process group: "PG_DNS" in Process: "libnet_admin" in "libstack.exe.so" in case of a truncated DNS response and a timed out connection request.
247645	ProxySG may become unresponsive and restart in Process group: "PG_TCPIP", Process: "stack-api-worker-1" when running NFS traffic.
246724	Page fault at 0x70 in Process group: "PG_TCPIP" in Process: "stack-bnd-1:0-rxq-0" in "libstack.exe.so. Workaround: disable CCM configuration.

Visual Policy Manager

B#	Issue
245701	VPM: When a new rule is created in a VPM Web Request Layer, the incorrect action object is being used as the default. As a result, the policy generated by the Web Request Layer is incorrect.

SGOS 6.7.1.2 PR

Release Information

- **Release Date:** March 27, 2017
- **Build Number:**199292

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 through 1.8.x
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.x
- **ProxySG Appliances:**
  - S500, S500-30, 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 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.1.2

- The Secure Web Gateway Virtual Appliance (SWG VA) supports multi-CPU VMware models. For details, refer to the *Secure Web Gateway Virtual Appliance Initial Configuration Guide for High-Performance Models*.

Fixes in SGOS 6.7.1.2

- SGOS 6.7.1.2 is a patch release that includes a number of fixes. See "Fixes in SGOS 6.7.1.2" on the next page.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

Fixes in SGOS 6.7.1.2

SGOS 6.7.1.2 includes bug fixes. This update:

Authentication

B#	Issue
242849	Fixes an issue where policy rules that included the caret ("^") or at character ("@") did not match correctly when the user belonged to a group whose name includes those characters.

DNS Proxy

B#	Issue
242704	Fixes an issue where the DNS proxy ignored or dropped DNS SOA dynamic update queries instead of transparently forwarding them to the DNS server.

Flash Proxy

B#	Issue
243109 243673	Fixes an issue where the appliance stopped responding after RTMP handoff.

Management Console

B#	Issue
243943	Fixes an issue where you could not scroll when creating a new HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**).
244020	Fixes an issue where TLS and SSL protocols could not be specified when adding or editing an HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**).

Real Media Proxy

B#	Issue
241170	Addresses an issue where the ProxySG appliance experienced a page fault in process "RTSP_WM_ Dispatcher" in "libce_admin.exe.so" at .text+0x21ccd9.

SSL Proxy

B#	Issue
243379	Fixes an issue where SSL interception of HTTPS traffic did not work when SOCKS proxy handoff was enabled.

B#	Issue
244692	Fixes an issue where TLS 1.3 websites could not be accessed through Google Chrome. Refer to ALERT2335 for details.

SSLV Integration

B#	Issue
243084 245244	Fixed an issue where the appliance did not create upstream OCS connections, resulting in connection failure.
242252	Addressed an issue where non-HTTP traffic work did not work and a "Request Error" exception page appeared when SSLV offload was configured.

System Statistics

B#	Issue
244021	Fixed an issue where the Management Console displayed incorrect interface statistics.

TCP/IP and General Networking

B#	Issue
243862 244770	Fixed an issue where the Management Console did not display interface statistics (**Statistics > Summary > Interface Utilization** and **Statistics > Network > Adapters**) when using a Secure Web Gateway Virtual Appliance.
242591	Addressed an issue where adding a second aggregate VLAN interface caused the appliance to stop responding.
243917	Addressed an issue where appliance experiences exception in process group "PG-TCPIP" and process "stack-api-worker-0" in "libstack.exe.so".
244356	Addressed an issue where appliance experiences exception in process group "PG-TCPIP" and process "stack-bnd-4:0-rxq-0" in "libstack.exe.so".

URL Filtering

B#	Issue
232481	Fixed an issue where WebPulse reported an incorrect category of "None" instead of "Pending" when it was configured to perform dynamic categorization in the background.

Visual Policy Manager

B#	Issue
243431	Fixed an issue where you could not install policy after adding multiple **Email** objects containing a new email list in the **Track** column in the Visual Policy Manager (VPM).
242892	Fixed an issue where **Threat Risk** objects were missing from the **Combined Condition** object.
	Fixed an issue where the VPM attempted to install a truncated policy if you clicked **Install Policy** more than once in the VPM within the same browser session.

SGOS 6.7.1.1 GA

Release Information

- **Release Date:** February 22, 2017
- **Build Number:**198020

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 through 1.8.x
- **SSL Visibility Appliance:** 4.0.1
- **ProxyAV:** 3.5.x
- **Content Analysis:** 1.2.x and 1.3.x
- **ProxyClient:** 3.4.x
- **Unified Agent:** 4.7.x and 4.8.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 219 for links to platform documentation.

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to TECH245893:

  http://www.symantec.com/docs/TECH245893

Upgrading To/Downgrading From This Release

- The Application Delivery Network (ADN) feature is not supported in SGOS 6.7.1.1. Upgrade to SGOS 6.7.2.1 or later to use ADN in your deployment. (B#243691)

- Universal policy settings are not retained after a downgrade if you install VPM policy in the downgraded version. This is expected behavior. See "New Features in SGOS 6.7.1.1" on the next page for details on universal policy support.
- After an upgrade or downgrade, the current list of SSH ciphers and the current list of HMACs—as shown in `view` subcommand output—may change. If you modify the current list using the `add`, `remove`, and `set` subcommands, the changes persist after system upgrades, downgrades, and reboots; however, the current list will not be identical to the list prior to upgrade/downgrade if the SGOS version must consider deprecated ciphers and HMACs. (B#241332)

  To understand the behavior after upgrade/downgrade, refer to `#(config ssh-console)`**`ciphers`** and `#(config ssh-console)`**`hmacs`** in the "Privileged Mode Configure Commands" chapter in the *Command Line Interface Reference*.
- The *SGOS Upgrade/Downgrade Guide* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC9794

Changes in SGOS 6.7.1.1

- SGOS 6.7.1.1 introduces new features and enhancements. See "New Features in SGOS 6.7.1.1" on the next page.

Fixes in SGOS 6.7.1.1

- Because this is the inaugural 6.7.x release, Symantec is reporting only security fixes for SGOS 6.7.1.1. See Security Fixes in 6.7.1.1.
- To see any Security Advisories that apply to the version of SGOS you are running, go to:

  https://www.symantec.com/security-center/network-protection-security-advisories

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

Limitations

- See "SGOS 6.7.x Limitations" on page 196 for a description of limitations in this release.

Known Issues

- See "SGOS 6.7.x Known Issues" on page 198 for a list of all issues that Symantec is aware of in SGOS 6.7.x.

New Features in SGOS 6.7.1.1

SGOS 6.7.1.1 introduces the following new features.

Support for Universal Policy

Universal policy is a set of global rules that you create in Symantec Management Center and apply to users in any location. The policy can include global rules that apply to both on-premises and Web Security Service (WSS) users, as well as individual rules that apply to only one or the other. It can also include location-specific policy when necessary. In essence, universal policy comprises the various rules that reflect your organization's acceptable use policy. Using Management Center to distribute the policy to on-premises devices and the WSS makes it easy to apply the relevant policy to all users in your organization.

To support universal policy, this release of SGOS allows you do the following on the ProxySG appliance:

- Specify and change enforcement domains in the Visual Policy Manager.
- Designate sections of policy as being appliance- or WSS-specific using the `#if enforcement=appliance` and `#if enforcement=wss` variables, respectively.
- Specify the ICAP service type in the Management Console or in the CLI.
- Configure the enforcement classification file in the CLI.

Caution: Universal policy settings are not retained after a downgrade if you install VPM policy in the downgraded version. For example, if you enable enforcement domains, downgrade to a previous version of SGOS (that does not support universal policy), install VPM policy, and then upgrade to 6.7.x again, enforcement domains are disabled and universal policy is lost. If you do not install VPM policy in the downgraded version, however, universal policy settings are preserved if you upgrade to 6.7.x. This is expected behavior.

- Full information:

  ***Visual Policy Manager Reference* — The Visual Policy Manager**

  ***Content Policy Language Reference* — Overview of the Content Policy Language**

  ***Command Line Interface Reference*— Standard and Privileged Mode Commands *and* Privileged Mode Configure Commands**

Cloud Policy Configuration in Management Console

You can now configure cloud policy in the Management Console (**Configuration > Cloud Configuration > Cloud Registration**); previously, only CLI commands were available.

- Full information:
  Auto Policy Synchronization

Web Application Firewall Features

This release includes the following enhancements for Web Application Firewall (WAF):

Command Injection Engine Version Logging

If WAF engines detect a command injection attack, the `x-bluecoat-waf-block-details` and `x-bluecoat-waf-monitor-details` fields in the bcreporterwarp_v1 access log format include the version of the command injection engine used for the detection:

- `version 2` - Indicates the legacy version used in versions prior to 6.6.5.1. This version targets chained command sequences, and requires command-separation characters to be present in the payload to be effective.
- `version 3` - Indicates the current default version. The command injection engine detects a wider set of attacks, including non-chained command injection payloads. Symantec recommends that you use this version.

WAF Scan Details Logging

If policy includes the `http.request.detection.bypass_cache_hit(yes)` property, the `x-bluecoat-waf-scan-info` field in the bcreporterwarp_v1 access log format indicates if WAF processing is intentionally skipped due to cache hit optimization being enabled.

- If WAF engines scan a transaction, the field reports `WAF_SCANNED`.
- If WAF evaluation does not occur due to the presence of the `http.request.detection.bypass_cache_hit(yes)` property during a cache hit transaction, the field reports `WAF_SCAN_BYPASSED`.
- If no WAF policy is present, the field reports `WAF_DISABLED`.

SOAP Request Handling

The appliance can now interpret SOAP messages in accordance with the normalizations present in policy and parse attachments in SOAP content. SOAP content is normalized correctly before it is sent to WAF engines for evaluation. Attachments are sent for further scanning based on their content type. SOAP request handling occurs without additional configuration when XML-related WAF policy exists.

Deep Multipart Inspection

The appliance now parses and normalizes sub-parts of multipart HTTP request bodies. Sub-part content is parsed based on the `content-type`. For example, if one of the sub-parts is JSON, and another is XML, each part is parsed correctly.

The `http.request.detection.other.invalid_form_data(block)` property blocks a matching request when an invalid multipart format is encountered.

Cross Site Request Forgery (CSRF) Attack Protection

Through the use of secure tokens, the appliance validates authentication on subsequent requests and protects POST requests in static and AJAX forms. This feature includes new CPL gestures:

- `http.csrf.authentication_link(`***`userid`***`,`*`client_ip`*`)`
- `http.csrf.detection(`*`action`*`)`
- `http.csrf.token.insert(`*`n`*`)`

Masking Sensitive Data in Access Log Details

This feature works when `http.request.log_details[header](yes)` or `http.request.log_details[body](yes)` is used to output header or body data to an access log. The following new CPL obfuscate sensitive information from access logs:

- `http.request.log.mask_by_name[`*`regex_pattern`*`](yes)`
- `http.request.log.mask_by_value[`*`regex_pattern`*`](yes)`

Obscured content appears as asterisks (****) in the log.

The following is an example of access logging policy:

```
; mask social security number (ssn) values from body text
; when reported in an access log
<proxy>
     http.request.log.mask_by_value["[0-9]{3}[ -]?[0-9]{2}[ -]?[0-9]{4}"](yes)
```

Invalid/Multiple Encoding Details in Access Logs

The appliance now reports the normalization function that triggered an invalid encoding or multiple encoding policy match. When invalid encoding or multiple encoding requests are detected are identified in process the function that caused it is added to the `x-bluecoat-waf-block-details` or `x-bluecoat-waf-monitor-details` access log fields as appropriate. No additional configuration is required for this feature.

Access logs include details for following functions:

- Multiple encoding: base64Decode, cssDecode, htmlEntityDecode, jsDecode, urlDecode, urlDecodeUni, utf8toUnicode
- Invalid encoding: utf8toUnicode

Identify Transactions in Exception Pages and Access Logs

Exception pages now include the transaction ID (a unique, per-transaction identifier) by default. As an example, an exception page includes the following text:

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

To aid in general troubleshooting:

- Include the `x-bluecoat-transaction-uuid` field in the access log format
- Instruct users who receive exception pages to report the transaction ID
- Locate the transaction ID in the log to learn more about the transaction

If you do not want exception pages to show the transaction ID, you can:

- Remove it from the exceptions definition under `$(exception.help)`
- Override the HTTP exceptions format with one that omits the `$(x-bluecoat-transaction-uuid)` substitution using the following CLI command:

  `#(config exceptions)inline http format eof_marker`

> **Tip:** After an SGOS upgrade, the default exceptions definitions are updated but the current exceptions are unchanged; you must edit your current exceptions manually to get the changes. See the *SGOS Upgrade/Downgrade WebGuide* for instructions.

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 I 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

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

Integration with WAF App for Splunk Plugin

A Symantec WAF App for Splunk plugin is available from Splunkbase (https://splunkbase.splunk.com/). The plugin presents WAF log data visually on dashboards, allowing you to:

- Aggregate log files passed into the database
- Specify how log files are parsed
- Search WAF log files
- Pivot search WAF logs and Symantec Security Analytics logs
- Full information:
  Symantec ProxySG Web Application Firewall App for Splunk Enterprise Product Installation Guide

DNS Access Logging

A new DNS access log for the DNS proxy was added as a default access log. It is available in the Management Console Default Logging Policy list, the default access Log Formats list, and as a default log facility.

- The CLI has been extended to include DNS; dns is included in the `#(config access-log) default-logging` command.
- In the Management Console, to configure the DNS (or any) Access Log, go to **Configuration > Access Logging > Upload Client**. To trigger log transfers to the client, go to **Configuration > Access Logging > Upload Schedule**.
- IPv6 is not supported at this time.
- On downgrade, the DNS default log facility remains visible in the Management Console, though logging will not work. Issue the `#restore-defaults factory-defaults` command to remove DNS access log objects.

SSLV Offload

In this release, you can connect one or more ProxySG appliances to an SSL Visibility appliance running version 4.0.1 to offload SSL/TLS traffic processing. Configuring SSLV offload requires that you identify the ProxySG and SSLV appliances to each other using their respective serial numbers.

Configure SSLV offload on the ProxySG appliance using one of the following methods:

- Managing SSLV appliances in the Management Console (**Configuration > SSL > SSLV Offload**)
- Issuing the `#(config ssl)`**`sslv-offload`** command

You must also add ProxySG appliance information to the SSLV appliance(s). Refer to the following documentation for complete steps.

- Full information:
  SSL Visibility Appliance Administration & Deployment Guide

  ***SGOS Administration Guide* — Managing the SSL Proxy**

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

Routing Domains Configuration in Management Console

Use routing domains to route traffic for unique networks through the same appliance, where each network has its own gateway and DNS server. This release introduces this feature as a configurable option in the Management Console (**Configuration > Network > Routing > Routing Domains**).

Network HSM Failover

The ProxySG appliance HSM Failover ability applies to HSM keyrings contained in an HSM keygroup. If the ProxySG appliance encounters an error when attempting to use an HSM keyring, it is flagged as failed. The signing operations will be tried on another member of the HSM keygroup, if applicable. The ProxySG appliance will periodically attempt to see if the error has been corrected. Once it has been, the HSM keyring will be put back into service.

- Full information:
  Intercepting SSL with the SafeNet Java HSM

IWA Direct Feature Enhancements

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

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

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

- By default, the appliance now uses the SMB2 protocol for connecting to the Active Directory server. If the server still uses the SMB1 protocol, issue the following command:

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

User Email Address Reporting

The ProxySG appliance can report on the email address of an authenticated SAML or IWA Direct user. This allows you to include the email address in:

- HTTP/S requests to the Elastica Cloud Access Security Broker (CASB) Gateway
- Access log formats, using the new field `x-cs-user-email-address`
- Exception pages and policy, using the new `$(user.email_address)` substitution variable

For unsupported authentication realms, the field returns an empty string.

Refer to TECH246128 for an example of how to send the email address in requests to the CASB service.

The following CLI subcommands were added for IWA Direct:

```
#(config iwa-direct realm_name)email-address enable
```

Enable the feature to report on the user's email address. Use in conjunction with the **email-attribute** subcommand.

```
#(config iwa-direct realm_name)email-attribute attribute
```

Specifies the attribute that represents the user's email address. Enable retrieval of this attribute with the **email-address enable** subcommand.

The following CLI subcommand was added for SAML:

```
#(config saml realm_name)email-address-attribute attribute
```

Specifies the attribute that represents the user's email address and retrieves the value of the attribute.

> **Tip:** Map the SAML email address attribute to the relevant field on the IDP. For example, if your IDP is Shibboleth, map the `emailAddress` attribute to the `mail` field.

- Full information:

  Support article TECH24612: http://www.symantec.com/docs/TECH246128
  ***Command Line Interface Reference* — Privileged Mode Configure Commands**

  ***SGOS Administration Guide* — Access Log Formats**

Client Certificate Emulation

To facilitate choosing signing certificates for the client in a reverse proxy deployment, this release includes client certificate emulation. When this feature is enabled:

- The appliance requests a certificate from the client.
- If the client returns a certificate, the appliance copies the certificate attributes to a new client certificate (so that it appears to originate from the client). Emulation does not occur if the client does not return a certificate.
- The appliance presents the certificate during the SSL/TLS handshake when an OCS requests a client certificate.

The following CPL action was added to support this feature:

```
server.connection.client_issuer_keyring(no|<keyring_id>|
 <hsm_keyring_id>|<hsm_keygroup_id>)
```

where:

- no disables client certificate emulation; this is the default setting
- *<keyring_id>* means to use the specified keyring for client certificate emulation. This must be a valid keyring, specified on the appliance with a CA certificate.
- *<hsm_keyring_id>* means to use the specified HSM keyring for client certificate emulation.
- *<hsm_keygroup_id>* means to use the specified HSM keygroup for client certificate emulation.
- Full information:
  ***SGOS Administration Guide*- Managing X.509 Certificates**

  ***Content Policy Language Reference*— Action Reference**

New TLS and Cipher Defaults

On an initial upgrade to version 6.7.x, TLS 1.1 and 1.2 are the default protocol selections for the Management Console and the SSL device profiles. TLS 1.1 will be used if 1.2 is not available. TLS 1.0 has been disabled by default. The default ciphers suites have been correspondingly updated as well.

If the default protocols (TLS 1.0, 1.1, and 1.2) for the SSL device profile (as with the HTTPS Console service) were selected previously, only TLS 1.1 and 1.2 are selected by default now. If the SSL device profile protocols were changed from the defaults previously, the selections do not change.

- The predefined SSL passive-attack-protection device profile can be used by many services, such as Authentication, Access-log, ICAP, Secure ADN, and OCSP.

- Interoperability issues may arise if a default or user-configured device profile is used to connect to a remote service which does not understand TLS 1.1 or 1.2.
- Management Console will no longer connect to browsers which don't support TLS 1.1 or 1.2 (Chrome before v21, Firefox before v23, Internet Explorer 8 and 9).
- If an SSL device profile uses a custom cipher suite, that cipher suite will be overwritten on upgrade.
- BCAAA may or may not support TLS 1.1. or 1.2. If the BCAAA connection fails, enable TLS 1.0 on the default SSL device profile.
  Notes:
  - Windows XP and Windows Server 2003 do not support TLS 1.1 or TLS 1.2.
  - Windows Vista and Windows Server 2008 do not support TLS 1.1 or TLS 1.2.
  - If you are using a Windows version later than those listed here, do not edit the default SSL device profile.
- User-configured SSL device profiles and Management Console settings retain their previous settings. Symantec strongly recommends updating the settings as soon as possible. If Director or Management Center attempts to copy a configuration containing these older protocols to a different device, the operation will fail, as the client device treats copied device profiles as new profiles.
- The reverse proxy is unchanged. The defaults are TLS 1.0, 1.1, and 1.2 enabled. SSLv3 and SSLv3 are options.
- For the forward proxy, SSLv2 and v3 are disabled by default.
- SSLv2 and SSLv3 have been removed from the CLI for the Management Console and SSL device protocol; attempting to use them will generate errors.
- On a downgrade from version 6.7.x , your selections do not change (whether you kept the default selections or changed them).

Any subsequent upgrades to 6.7.x, for example after a downgrade, do not change the protocol selections; the protocols selected prior to the subsequent upgrade are retained.

- Full information:
  ***SGOS Administration Guide* — Configuring Management Services, Authenticating a ProxySG Appliance, Managing SSL Traffic**

  ***SGOS Command Line Interface Guide* — Privileged Mode Configure Commands**

Enhancements and Changes in SGOS 6.7.1.1

SGOS 6.7.1.1 also introduces the following enhancements and changes:

Pipelining Disabled by Default for Better Network Performance

Due to recent advances in web browsers, pipelining provides limited benefits and can increase CPU utilization in certain workloads. Thus, in a new installation of 6.7.x, or upon an upgrade to this release, pipelining is disabled by default.

ECDSA Signed Certificate Support

The ProxySG appliance can now verify ECDSA certificates during the SSL handshake, as well as DSA and RSA.

- Full information:

  ***SGOS Administration Guide* – Managing the SSL Proxy**

Increased Key Sizes for Emulated Server Certificates

The key size supported for emulated DSA and ECDSA server certificates has been increased to 2048 bits. The key size for emulated RSA server certificates is now matched up to a maximum of 4096 bits. For example, when the ProxySG appliance intercepts a 4k RSA server certificate, it will emulate a 4k certificate.

On downgrade, the previous RSA 2k and DSA/ECDSA 1k limits will be enforced.

> **Caution:** High volumes of intercepting web sites with 4K RSA keys might affect performance on smaller-scale models such as the SG-S200 series. For details and a workaround for this issue, refer to TECH253498: https://www.symantec.com/docs/TECH253498

AES-GCM and SHA384 Ciphers Support

The appliance now supports the following cipher suites for SSL forward proxy:

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384

SGOS 6.7.x Reference Information

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

SGOS 6.7.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.

CASB AppFeed Uses Default BRR

When writing policy rules based on Business Readiness Rating (BRR), note that the CASB AppFeed applies its own Default BRR; it does not apply tenants' BRR modified from Symantec CloudSOC. TECH247736 describes this behavior: http://www.symantec.com/docs/TECH247736

Dynamic Categorization in Secure Mode

The CLI command to enable secure mode for dynamic categorization is not available in verson 6.7.x.

Before upgrading, enable secure mode in 6.5.x. If you have already upgraded, downgrade to version 6.5.x, enable secure mode, and upgrade again.

This deprecation was previously documented as B#237090.

Secure Web Gateway Virtual Appliance

SGOS 6.7.x does not support VMware's suspend and resume feature. Until further notice, do not suspend the VM.

Non-Functional Application Attributes Command

SGOS 6.7.2.1 added the following CLI:

```
#(config application-attributes)view groups [attribute <attribute_name>]
```

This subcommand is visible in CLI output if you issue the **?** help parameter; however, this CLI is non-functional. Do not use this subcommand.

> **Note:** This CLI was removed in version 6.7.4.

Cached SkyUI After Downgrade

After an upgrade to version 6.7.4.x or later followed by a downgrade to an earlier release, you are unable to log in to SkyUI. The browser displays a "loading data" page and does not load the SkyUI console. To work around the issue, issue the following CLI commands after the downgrade to clear the cached UI:

```
#(config)ui
#(config ui)reset
Resetting UI to bound system version...
ok
```

SGOS 6.7.x Known Issues

Symantec is aware of the following issues in SGOS 6.7.x.

Access Logging

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#250158	The output for **`#show config`** does not indicate that SCP is set as the upload client (through either the CLI or the Management Console).	"Fixes in SGOS 6.7.3.1" on page 158
B#250180	The log tail for a selected log in the Management Console (**Statistics > Access Logging > Log Tail**) displays the same entries multiple times when new entries do not appear. This issue occurs when there is a burst of traffic through the appliance, followed by no traffic or very slow traffic. This issue does not occur if traffic through the appliance is continuous.	"Fixes in SGOS 6.7.3.1" on page 158
B#253658	Continuous access log upload stops after logging directory slots run out.	"Fixes in SGOS 6.7.4.107" on page 120 "Fixes in SGOS 6.7.3.6" on page 146
SG-5340 B#267383	Access log objects are not created when the name includes a period (".")	

ADN

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#237722 SG-3397	Policy rules that include the caret ("^") or at character ("@") do not match correctly when the user belongs to a group whose name includes those characters.	"Fixes in SGOS 6.7.1.2" on page 181

Authentication

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-9435	Admin authentication does not work when a BCSI-AC cookie is present in the browser.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#261934 SG-5812	When testing Windows SSO authentication from the CLI and when nested groups are enabled, the appliance might restart.	Fixes in 6.7.4.140
B#242849	Policy rules that include the caret ("^") or at character ("@") do not match correctly when the user belongs to a group whose name includes those characters.	"Fixes in SGOS 6.7.1.2" on page 181
B#251438	Setting the windows-domains LDAP ping protocol as UDP might cause the appliance to restart.	"Fixes in SGOS 6.7.3.1" on page 158
B#253544	A fix for a previous issue (B#246848) was implemented to prevent latency/firewall-related issues while contacting domain controllers (DCs) in remote geographical locations. The fix introduced an issue where the appliance can contact only DCs in the local Active Directory (AD) site to which the appliance belongs. As a result, because an appliance requires a read-write domain controller to join a domain, appliances with only local access to a read-only DC are unable to join the AD domain.	"Fixes in SGOS 6.7.4.107" on page 120
B#256029	Kerberos authentication fails after the appliance's machine account password is changed in Active Directory and the machine account is enabled for AES-256 bit encryption.	"Fixes in SGOS 6.7.3.6" on page 146
B#252851	The SNMP Schannel configuration stores incorrect CLI commands in the configuration archive, which prevents the configuration from being restored.	"Fixes in SGOS 6.7.4.107" on page 120
B#255299	The proxy experiences a page fault restart in process "HTTP CW F95FD4B90" in "libc.so" related to the timing of actions when using the auth/debug log URL	"Fixes in SGOS 6.7.4.107" on page 120
B#253745	The domain controller (DC) resets the connection when the appliance sends an SMB1 Echo Request in an SMB2 environment.	"Fixes in SGOS 6.7.4.107" on page 120
B#254717	AES authentication with Kerberos fails if the Kerberos load balancer username contains an upper-case letter.	"Fixes in SGOS 6.7.4.107" on page 120

Build

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#264981 SG-6038	The virtual appliance image is not marked as signed in the meta.txt file, which prevents the system from entering FIPS mode from the CLI.	"Fixes in SGOS 6.7.4.1" on page 96

CLI Consoles

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255576 SG-6637	Issuing the `#show config` command might cause the appliance to restart if the URL set using `#(config)`**`statistics-export config-path`** is invalid.	"Fixes in SGOS 6.7.3.6" on page 146

Client Manager

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#256189 SG-5897	An "Invalid archive" error occurs when attempting to upgrade Unified Agent using the **Local File** option.	"Fixes in SGOS 6.7.4.130" on page 108

DNS Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#242704	The DNS proxy ignores or drops DNS SOA dynamic update queries instead of transparently forwarding them to the DNS server.	"Fixes in SGOS 6.7.1.2" on page 181

Documentation

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#253226	The *SGOS Administration Guide* incorrectly states that you can specify a hostname for the custom access log upload client. In both the Management Console and the CLI, only an IP address is supported.	Fixed in February 2018.

Flash Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#243109	The appliance stops responding after RTMP handoff.	"Fixes in SGOS 6.7.1.2" on page 181

FTP Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#258715 SG-4623	When ICAP REQMOD mirroring is enabled for the FTP proxy, the `s-action` access log field is occasionally not populated.	

Hardware Drivers

B#	Issue Workaround (if available)	Fixed In (when applicable)
247078	Output errors occur with the Intel 10GB (ixgbe) interface card on the SG-S400 and SG-S500. These errors do not indicate any issues and can be ignored.	6.7.1.3

HTTP Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
247731	Pipelined requests do not follow routing domain rules.	"Fixes in SGOS 6.7.3.1" on page 158
258588	HTTP debug log filters do not work unless both client and server IP filters are set.	"Fixes in SGOS 6.7.4.3" on page 74

ICAP

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#219269 SG-2750	**Issue:** Adding an ICAP server to or removing an ICAP server from a load balancing group can, under some circumstances, cause the ProxySG appliance to stop responding. **Workaround:** Temporarily disable the health check for the ICAP object to reduce the chances of this issue occurring. Symantec recommends that you do the following: 1. In the Management Console, select **Configuration > Health Checks > General**. 2. Select the health check for the ICAP object and click **Edit**. The console displays an Edit Health Check dialog. 3. For Enabled state, select **Disabled: Unhealthy**. 4. Click **OK > Apply** to save your changes. 5. Add or remove the ICAP server to/from the load balancing group. 6. Repeat steps 1 -2. Then, re-enable the health check and save your changes.	
SG-8038	The exception page from the DLP server (request modifier) is not displayed when the ICAP service is configured to use the vendor's 'virus found' page.	Fixes in 6.7.4.4

Kernel

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#246096	The appliance might restart with a page fault at 0x2073f349000 in Process group: "PG_POLICY_HTTP" in Process: "PDW t=6084547 for=ED801C9F" in "libc.so".	6.7.1.3
B#250933 SG-4107	The appliance stops responding intermittently due to large memory allocation from the CFS downloader.	"Fixes in SGOS 6.7.2.2 PR" on page 166
B#252191	Policy does not install if it contains non-existent AD groups.	"Fixes in SGOS 6.7.3.6" on page 146

Management Console

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#260464	**Issue:** In the GUI, the bandwidth stats displays incorrect statistics for the parent class. **Workaround:**To view bandwidth management statistics, view the CLI output (show bandwitdh-management statistics) or access the JavaMC via the HTTP-Console.	
B#243943	When creating a new HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**), the dialog does not allow you to scroll.	"Fixes in SGOS 6.7.1.2" on page 181
B#217492 SG-2794	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.	
B#217732 SG-2804	**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.	
B#249339	Using links (for example, from your site's internal webpages) to ProxySG advanced URLs might result in "400 Bad Request" errors.	"Fixes in SGOS 6.7.2.1" on page 174
B#244020	When you add or edit an HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**), you are unable to specify TLS and SSL protocols. Instead, the dialog displays only a **secure_ssl_protocol_v2** option.	"Fixes in SGOS 6.7.1.2" on page 181
B#250440 SG-5853	The **Overview**, **Content Analysis**, and **Sandboxing** tabs display an "Access Denied" message when you are logged in as a read-only user.	"Fixes in SGOS 6.7.4.3" on page 74
B#250120	When creating a new HTTPS Reverse Proxy service (**Configuration > Services > Proxy Services**) on a Secure Web Gateway Virtual Appliance or ProxySG Virtual Appliance MACH5 Edition, the dialog does not allow you to scroll.	"Fixes in SGOS 6.7.4.107" on page 120
B#254660	The Management Console does not accept system image download URLs consisting of more than 227 characters.	"Fixes in SGOS 6.7.3.6" on page 146
B#260464	**Statistics > Bandwidth Mgmt** shows incorrect statistics for parent class.	Fixes in 6.7.4.140
B#261869 SG-7026	Adding an existing CA certificate whose name contains spaces to a CCL fails when using the Management Console.	Fixes in 6.7.4.140

MAPI Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#249746	Email attachment scan results are cached, but subsequent attachment downloads are sent to the ICAP server again instead of using previously cached data.	"Fixes in SGOS 6.7.4.107" on page 120

Network Drivers

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#243485	After the E1000 interface is disabled on the Secure Web Gateway Virtual Appliance on ESX, re-enablingthe interface might not activate the link unless the VA is rebooted.	6.7.1.3
B#247235	Added NDIO Statistics for packets, errors and drops for the ixgbe driver.	6.7.1.3
B#247185	After upgrading the SG 9000 to 6.7.1.1 or 6.7.1.2, it is not possible to manually set the speed link to 1Gbps.	6.7.1.3
B#255462	The Secure Web Gateway virtual appliance (ESX) might restart in process "NIC I/O 1:0-vmx_n 0-rxq-txq" in "vmxnet3.exe".	"Fixes in SGOS 6.7.4.107" on page 120 "Fixes in SGOS 6.7.3.6" on page 146

Performance

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#242394 SG-3672	The appliance experiences performance degradation if CPU usage is greater than 70% and the appliance is in transparent bridging mode with a significant portion of traffic being bridged.	
B#234568 SG-3252	Higher DNS utilization occurs under heavy load conditions. This was discovered in some internal performance tests.	

Policy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#262506	If changing malware scanning from an internal to an external content analysis service and tenant policy is used or pushed from Management Center, you must manually install a VPM policy.	Fixes in 6.7.4.140
B#262197	In a transparent deployment, if authentication policy allows access for specific users/groups, users might not be able to join a meeting or log-in with Skype for Business.	Fixes in 6.7.4.140

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#236676 SG-3349	**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.	
B#242737 SG-2969	**Issue:** Users on mobile devices receive an Invalid Certificate Authority error when connecting to Google +. The issue occurs when using Google Chrome, Mozilla Firefox, Internet Explorer, and the device's default web browser. **Workaround:** Install the ProxySG appliance's SSL certificate on the mobile device.	

B#231634
 	
SG-2852
	When multitenant policy exists, the `http.request.body.inspection_size()` 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 `http.request.detection.other.threshold_exceeded()` setting is respected and applies correctly to the transaction.
	
	Consider the following example:
	
	`; 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)`
	
	Given these rules:
	
	■ 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.
	
	■ 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.	

ID	Issue Workaround (if available)	Fixed In (when applicable)

B#249884
 	
SG-4058
	Issue: When policy includes multiple forms of county names (such as short names, ISO codes, and full names), IP addresses in geographical regions are allowed or denied as intended, but policy traces show regions with an incorrect verdict. For example, consider the following CPL:
	
	`<proxy>`
	`supplier.allowed_countries[uS, US, "Us", Ca, "United States"] (deny)`
	
	This policy results in denials of IP addresses in Canada and the United States, but a policy trace shows that "United States" is denied whereas "uS" is allowed.
	
	Workaround: Do not use multiple formats for country names in policy. Use a consistent format for all instances of country names, as follows:
	
	`<proxy>`
	`supplier.allowed_countries["United States", Canada] (deny)`	

B#250179	The exceptions file (**Configuration > Exceptions > View > Exceptions Configuration**) does not show currently-defined exceptions. Clicking any link of a known exception displays the message "No exception found called '<*exception_name*>'".	"Fixes in SGOS 6.7.3.1" on page 158
B#251992 SG-4129	Policy performance is adversely affected when policy includes a large number of categories assigned to a single URL.	Fixes in 6.7.4.140
B#252806 SG-4248	Changing base user-defined exception fields does not update a policy-defined exception.	
B#252541	Rules with a **BlockPopupAds** object result in a 'Warning: Unreachable statement' error when installing VPM policy.	"Fixes in SGOS 6.7.4.130" on page 108
SG-7926	The `$(cs-categories)` and `$(cs-category)` substitutions do not display the correct URL rating on the coaching (NotifyUser) page.	Fixes in 6.7.4.4
SG-5359 B#267518	Coaching policy does not work when tenant policy is installed.	

Real Media Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#241170	The ProxySG appliance experiences a page fault in process "RTSP_WM_Dispatcher" in "libce_admin.exe.so" at .text+0x21ccd9.	"Fixes in SGOS 6.7.1.2" on page 181

Serviceability

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-8213	Enabling monitor also unexpectedly enables periodic uploads.	Fixes in 6.7.4.4

Services

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#261499	You might not be able to remove the default TCP Port 514 listener.	Fixes in 6.7.4.140

SSL Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-13361	HTTPS sites the were denied by policy appear under Sessions > Errored Sessions.	
SG-18488	If tunnel-on-error is enabled, SSLv2 traffic is blocked, which might cause an outage.	
SG-18488	SSLv2 traffic cannot interpret the CH and tunnel-on-error cannot tunnel the session.	
SG-9211	**Issue:** SSL intercept policy set to `on_exception` does not work when policy includes any of the following: ▪ `server.certificate.hostname.category=` ▪ malware scanning policy The issue occurs because these policies involve server certificate category lookups. **Workaround:** Use full SSL interception for URLs or categories that should be blocked.	
B#252087	The appliance does not use the SNI extension in the server-side connection, which is required by some servers to respond with the correct server certificate in the TLS handshake.	"Fixes in SGOS 6.7.4.107" on page 120
B#247892	The ProxySG appliance might trigger a threshold monitor restart due to high SSL memory pressure.	6.7.1.3
B#245923	Hardware restart in Process group: "PG_TCPIP" in Process: "SSLW 40599BD2060" in "libstack.exe.so".	6.7.1.3
B#246275 SG-3880	The `client.connection.negotiated_ssl_version=` condition does not block SSLv3 traffic.	
B#243379	SSL interception of HTTPS traffic does not work when SOCKS proxy handoff is enabled.	"Fixes in SGOS 6.7.1.2" on page 181
B#220528 SG-2866	**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.	
B#225793 SG-2985	**Issue:** **`#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. **Workaround:** Copy and paste the relevant sections of **`#show config`** output into a text editor. In the text editor, add the quotation marks around the keyring name manually, and re-apply the inline configuration.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#225611 SG-2970	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.	
B#248792	Threshold monitor restarts occur with high memory usage by SSL connections.	Partial fix available in version 6.7.3. The behavior is improved in this release. "Fixes in SGOS 6.7.3.1" on page 158
B#227420 B#224017	Some versions of Director and Management Center cannot connect to an appliance running in FIPS mode. **Note:** SGOS 6.7.x introduces changes to how the appliance handles ciphers upon upgrade. Refer to the security fix for B#241332 to learn about this behavior change.	This issue is resolved. If managing from Director, upgrade to Director 6.1.22.1, which supports OpenSSH 7.1p2. Refer to the *Director version 6.1.x Release Notes* for details. If managing from Management Center, add one of the following ciphers to the managed device: ■ aes256-ctr ■ aes192-ctr ■ aes128-ctr
B#252450 SG-4320	In STunnel and Bypass modes, the `x-cs-session-id` and `x-cs-server-certificate-key-size` access log fields are not populated.	
B#253905 SG-3605	The appliance stops responding when the **CRL distribution point** host name field (**Configuration > Proxy Settings > SSL Proxy**) includes special characters.	
B#253926 SG-4323	In some cases, the appliance creates a certificate with the OCS IP address in the SAN **DNS Name** field when providing the client with a server-side TCP error message.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255423 SG-4373	On a resumed connection, the `x-cs-server-certificate-key-size` access log field always displays `RSA[1024]`.	
B#257012 SG-6902	In bypass mode, the `x-cs-server-certificate-key-size` access log field displays `RSA[1024]`. In bypass mode, this information is not available and the field should not be populated.	"Fixes in SGOS 6.7.4.130" on page 108
B#257835 SG-4574	When adding a keyring through the CLI, whitespaces in field values are not ignored. This issue does not occur when creating keyrings through the Management Console.	
B#258130	`http.request.apparent_data_type` and `http.request.data.N` policy are not enforced.	"Fixes in SGOS 6.7.4.130" on page 108

B#258141
 	
SG-4598
	Issue: Setting the **Client Certificate Validation CCL** or **Server Certificate Validation CCL** object in the **SSL Intercept Layer** in the VPM results in the error "Invalid action for <ssl-intercept> layer", and policy does not compile.
	
	Workaround: These gestures have been moved to the `<ssl>` layer. Write the policy in CPL instead, as follows:
	
	`<ssl>`
	`server.certificate.validate.ccl(CertList)`	

SG-6161 B#267269	After upgrading to SGOS 6.7.4.1 , when SSL traffic is not intercepted by policy, SSL attributes (such as negotiated cipher or TLS version) are not available for use in policy conditions and access log fields. Refer to TECH253316 for more information on this issue.	"Fixes in SGOS 6.7.5.1" on page 17

SSL/TLS and PKI

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-18246	**Issue:** If you are running SGOS 6.7.4.9 and later, and the appliance is configured as a reverse proxy, the server persistence does not work. **Workaround:** Use SGOS 6.7.4.8 or earlier until this issue is fixed.	
SG-18196	If the appliance is running SGOS 6.7.5.1, the memory footprint increases by 3-5% due to the fix for SG-14742. If the footprint is around 70-75%, memory consumption can easily be pushed into memory regulation.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#250120	You cannot create a new HTTPS Reverse Proxy service in the Management Console (**Configuration > Services > Proxy Services > New Service**).	"Fixes in SGOS 6.7.4.107" on page 120
B#221218 SG-2885	A newly-created certificate displays "Not yet valid" for **Certificate expiry** (**Configuration > SSL> Keyrings**). This issue occurs when the appliance's clock is ahead of the clock on the client running the Management Console.	
B#220453 SG-2861	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.	
B#225612 SG-2971	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.	
B#248731 SG-3988	In the access log for the SSL reverse proxy service, `client-side negotiated-cipher` fields are populated incorrectly when GCM or SHA384 ciphers are used.	
B#253377	Random HTTPS pages do not load when SSL Proxy is used. Refer to TECH248154 for details: http://www.symantec.com/docs/TECH248154	6.7.2.3 PR
B#256750 SG-4462	In Skype for Business, video calling and screen sharing do not work.	"Fixes in SGOS 6.7.4.1" on page 96
B#257920 SG-4583	You receive the following error when uploading a signed configuration file that was just downloaded: **% Attempt to load configuration failed: signature verification failed: The message did not match the PKCS7 signature.** The error occurs when any signing keyrings are set on the appliance.	
B#256750 SG-4462	Skype for Business Video calling and screen sharing do not work.	"Fixes in SGOS 6.7.4.1" on page 96

SSLV Integration

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-18207	**Issue:** If changes are made to the SSLV appliance configuration (such as adding or removing an SSLV box), the SSLV offload stops working. **Workaround:** Restart the ProxySG appliance to update the SSLV configuration.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#242864 SG-3692	When SSL connections are denied using a server-negotiated cipher policy, access log values for negotiated cipher, negotiated cipher strength, and negotiated cipher size are not populated.	
B#243726	**Issue:** When the appliance is configured with SSLV devices whose IDs include spaces, the **`#show config`** output does not display the spaces. These omitted spaces can cause configuration restoration to fail. **Workaround:** Before restoring a configuration, edit it manually to correct the SSLV device IDs.	"Fixes in SGOS 6.7.2.1" on page 174
B#243084	In some cases, the appliance does not create upstream OCS connections, resulting in connection failure. When this issue occurs: ■ the browser presents an exception page to the user ■ on the SSLV appliance, the **SSL Session Log** summary displays "Cut (Connection to Proxy)", which is incorrect; rather, the ProxySG appliance terminated the connection unexpectedly	"Fixes in SGOS 6.7.1.2" on page 181
B#242252	When SSLV offload is configured, non-HTTP traffic is broken and a "Request Error" exception page appears. This issue occurs when the ProxySG appliance does not perform any HTTP proxy offloading.	"Fixes in SGOS 6.7.1.2" on page 181
B#256905 SG-4482	In SSLV offload mode, the `x-cs-session-id` access log field displays incorrect session ID values and the `x-cs-server-certificate-key-size` field always returns `RSA[1024]` for key size.	
B#258272 SG-4612	With SSLV offload enabled and policy enforcing cipher based properties, some SSL cipher access log fields present SSLV values instead of ProxySG appliance values. For example, instead of displaying `AES256-SHA` a field shows `RSA-AES256-CBC-SHA`.	
B#256791	In SSLV offload mode, Symantec recommends using the default TCP window size of 65535. Increasing the TCP window size might result in stalled connections.	"Fixes in SGOS 6.7.4.130" on page 108

System Statistics

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#262919 SG-4890	When the appliance is experiencing a heavy load, running the `clear-statistics persistent` CLI command might cause the appliance to stop passing traffic.	Fixes in 6.7.4.140

TCP/IP and General Networking

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#258974 SG-4633	When booting up the appliance, if the first DNS server in the primary group is unreachable, the appliance might stop booting.	Fixes in 6.7.4.140
B#263272 SG-7127	The appliance might return a false attack in progress status from an SNMP walk.	Fixes in 6.7.4.140
B#257272	Downloads of large files via SOCKS proxy on high-speed networks (2Mbps+ speed) time out.	"Fixes in SGOS 6.7.4.130" on page 108 "Fixes in SGOS 6.7.3.7" on page 141
B#247788	The ProxySG CLI and Management Console might have become unresponsive after enabling CCM on peers.	6.7.1.3
B#246441	When using IAW Direct and the Active Directory server did not respond to LDAP pings, an issue might have occurred where CPU usage increased to 100% and the appliance restarted in threshold monitoring after reaching acceptance regulation. This issue occurred after upgrading to 6.7.1.1 or 6.7.1.2.	6.7.1.3
B#245737	After upgrading to 6.7.1.1 or 6.7.1.2, transparent interception using WCCP/GRE was not working correctly.	6.7.1.3
B#245625	Page fault in Process group: "PG_DNS" in Process: "libnet_admin" in "libstack.exe.so" occurred when there was a truncated DNS response and a timed out connection request.	6.7.1.3
B#247512	NetFlow interface configuration did not show interface details.	6.7.1.3
B#247645	The ProxySG might have become unresponsive and restarted in Process group: "PG_TCPIP", Process: "stack-api-worker-1" when running NFS traffic.	6.7.1.3
B#246724	Page fault at 0x70 in Process group: "PG_TCPIP" in Process: "stack-bnd-1:0-rxq-0" in "libstack.exe.so.	6.7.1.3

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#243862	When using a Secure Web Gateway Virtual Appliance, the Management Console does not display interface statistics (**Statistics > Summary > Interface Utilization** and **Statistics > Network > Adapters**).	"Fixes in SGOS 6.7.1.2" on page 181
B#242591	Adding a second aggregate VLAN interface causes the appliance to stop responding.	"Fixes in SGOS 6.7.1.2" on page 181
B#244784	Packets might exit an incorrect interface in IPv6 configuration when static routes are configured.	"Fixes in SGOS 6.7.3.1" on page 158
B#253548 SG-4155	Restart occurs due to high volume of IPv6 network traffic.	
B#250616	The appliance might have restarted in Process group: "PG_TCPIP", Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so". This issue occurred when delayed intercept was enabled.	6.7.2.3 PR
B#250637	The appliance might have restarted in Process group: "PG_TCPIP" in Process: "stack-api-worker-0" in "libmemory.so". This issue occurred when dynamic bypass was enabled.	6.7.2.3 PR
B#255319 SG-6805	The appliance might experience a restart in process "HTTP SW 40047170A40 for 30F29CC2A40" in "libstack.exe.so".	"Fixes in SGOS 6.7.3.11" on page 128
B#249425 SG-4032	The default gateway cannot be removed unless it is reachable from a configured interface's IP address.	
B#255291 SG-4333	Enabling and disabling EDNS support is not reflected in the event log.	
B#252086	The appliance might experience a restart in PG_TCPIP when Virtual IP is configured in failover mode.	"Fixes in SGOS 6.7.4.107" on page 120
B#255057	You cannot delete auto-linklocal IPv6 addresses when the interface has link-aggregation set.	"Fixes in SGOS 6.7.4.130" on page 108
B#259669 B#256543	The proxy does not fail over when the DNS server fails in a custom DNS group.	"Fixes in SGOS 6.7.3.7" on page 141

URL Filtering

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#232481	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.	"Fixes in SGOS 6.7.1.2" on page 181

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#232047 SG-5404	**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.	
B#249253	The WebPulse tab (**Configuration > Threat Protection > WebPulse**) does not display database download status if Intelligence Services is enabled.	"Fixes in SGOS 6.7.4.107" on page 120
B#255954	**Issue:** Some SSL websites do not load, even if WebPulse is running in background mode. **Workaround:** Perform a drt.rating_servic service health check. In the Management Console (**Configuration > Health Checks > General**), select **drt.rating_service** and click **Perform health check**.	"Fixes in SGOS 6.7.4.130" on page 108
B#256515 SG-4437	When the content filtering categorization and Application Classification providers are both disabled, the **Statistics > Category Details** page does not load.	
B#256858	A specific URL takes a long time to load when DRTR is running in the background.	"Fixes in SGOS 6.7.4.130" on page 108
B#256952	After downloading an updated content filtering database with changed category names, previous category names are still visible when you view the categories list.	Fixes in 6.7.4.140
B#257351 SG-4536	The `#show system-resource-metrics` CLI output shows empty statistics for custom local databases that are not defined.	
B#257872	During an initial boot of the appliance, a page fault might occur in Process Group "PG_CFS" Process:"Subscription.download_worker" in "liburl_filter.exe.so". Rebooting the appliance usually resolves the issue.	"Fixes in SGOS 6.7.4.130" on page 108
B#256160	WebPulse is not categorizing websites in a child/parent configuration when a valid forwarding host is not supplied.	"Fixes in SGOS 6.7.4.107" on page 120 "Fixes in SGOS 6.7.3.7" on page 141
B#259289 SG-4670	When using the **Configuration > Content Filtering > General > Test URL** function, URLs with Unicode characters do not match against local database-defined categories. Matching works with live traffic.	

Visual Policy Manager

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#243431	You cannot install policy after adding multiple **Email** objects containing a new email list in the **Track** column in the VPM. Policy installation fails with a message stating that installation was abandoned.	"Fixes in SGOS 6.7.1.2" on page 181
B#242892	Some **Threat Risk** objects are missing from the **Combined Condition** object.	"Fixes in SGOS 6.7.1.2" on page 181
B#243817	If you click **Install Policy** more than once in the Visual Policy Manager (VPM) within the same browser session, the VPM could attempt to install a truncated policy. This truncated CPL might install successfully, which could lock all non-console administrators defined in policy out of the ProxySG appliance and install a subset of the policy defined in VPM.	"Fixes in SGOS 6.7.1.2" on page 181
B#245701	When a new rule was created in the **Web Request Layer**, an incorrect action object was used as the default. As a result, policy generated by the Web Request Layer was incorrect.	6.7.1.3
B#255321	The appliance sends an `invalid_request` exception error page if you log out of the Management Console and then try to access the consent banner URL again with same browser.	"Fixes in SGOS 6.7.4.107" on page 120
B#258187	**Service Name** and **Service Group** objects are not visible in the Service column in the Web Request Layer.	"Fixes in SGOS 6.7.4.130" on page 108

Web Application Firewall

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#222156 SG-2829	When the Application Protection service is disabled and the subscription is expired, loading associated policy does not generate policy warnings.	
B#248897 SG-4003	Some WAF policy is not supported in WSS cloud deployments.	

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 6.7.x is not supported on any platform not listed here.

Platforms	Resources	Comments
SG-S500	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145525	All hardware-specific documents for the specified model
SG-S400	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145524	
SG-S200	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145523	
SG300	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145516	
SG600	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145518	
SG900	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145520	
SG9000	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145521	
Supported virtual appliances	https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145514	Documents for SWG VA high-performance models, SWG VA and MACH5 for Hyper-V, SWG VA for V100, SGOS on AWS, and SGOS on CSP

Additional Resources

Subject	Resources	Comments
Diagnostics	http://www.symantec.com/docs/DOC9795	S-Series Maintenance and Upgrade Guide

About Security Certification

SGOS 6.7.2.102 is designed for FIPS 140-2 validation. The following hardware platforms are FIPS-certified:

- ProxySG: S400-20/30/40 and S500-10/20/30
- Reverse Proxy: S400-20/30/40 and S500-10/20/30
- Advanced Secure Gateway: S400-20/30/40 and S500-10/20

To meet the security requirements of our customers, Symantec maintains Federal Information Processing Standard (FIPS) 140-2 and Common Criteria certifications on Symantec appliances. For more information about the current FIPS and Common Criteria certifications, refer to the *Using FIPS Mode on the ProxySG* document:

http://www.symantec.com/docs/DOC10145

Cryptographic Algorithms in FIPS Mode

In FIPS mode, the appliance can use only the cryptographic algorithms and functions listed below for security relevant and administrative actions (proxy operations are not limited):

- Advanced Encryption Standard (AES) 128-,192- and 256-bit key sizes
- Triple-DES
- Diffie-Hellman: SHA-1, SHA-256
- Rivest Shamir Adleman (RSA):
    - RSA sizes for keys created by the appliance: 2048-bit
    - RSA sizes for keys imported by the appliance: 1024-, 2048-, 3072-, 4096-, 8192-bit
- Secure Hash Algorithm (SHA-1):
    - SHA-1 is used where permitted for protocol and signature verification purposes.
    - SHA-224, SHA-256, SHA-384, SHA-512
- Keyed-Hash Message Authorization Code (HMAC):
    - HMAC with SHA-1
    - HMAC with SHA-2
- Random Number Generation
    - NIST SP 800-90A CTR Deterministic Random Bit Generator
    - ANSI x9.31 Appendix A.2.4 Pseudo Random Number Generator

Updated FIPS Mode Restrictions

- Windows domain configuration for IWA Direct is enabled in FIPS mode.
- Keyrings containing legacy RSA keys of less than 2048-bits may be imported and used.
- In the event a power up self test (software or hardware) fails, the appliance presents options to reboot and retry the self test, and to boot into the last successfully booted release.

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.

Product Documentation and Articles

- Search for articles and downloads at MySymantec:

  https://support.symantec.com/

- Refer to MySymantec for product documentation:

  https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145522

- Access online help from within the ProxySG Management Console; however, note that documentation posted on MySymantec supersedes online help.

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://www.symantec.com/security-center/network-protection-security-advisories

Symantec Connect Forums

- Connect with other users at Symantec Connect Forums:

  https://www.symantec.com/connect/

Documentation Errata

- 6.7.1.1: The **Help** buttons on the **SSH Ciphers** and **SSH HMACs** tabs in the Management Console are not active. To learn about these features, refer to the *SGOS Administration Guide* and the *Command Line Interface Reference*.

Provide Feedback

- Send any questions or comments about documentation:

  documentation_inbox@symantec.com

- For Customer Care requests, send email to:

  NP_customercare@symantec.com