Symantec™
by Broadcom Software

SGOS 7.3.x Release Notes

August 26, 2024

Table of Contents

SGOS Release Index and Maintenance Streams

The following table illustrates the relationship between various 7.x and 6.7.x releases to clarify what fixes and features each 7.x release contains.

The **Base Version** column indicates which software release was used as a starting point for the GA release. The **Maintenance Release Parity** column indicates which releases the GA release is similar to in terms of bug fixes and features.

> **IMPORTANT**
> For product EOL and lifecycle information, refer to KB 151102. Plan to upgrade your appliances to a supported version; refer to the Upgrade/Downgrade documentation for instructions.
>
> As of December 2023, SGOS 6.7.x is end of life. There is no longer a 6.7.x maintenance release in parity with 7.3.x.

GA or PR Release	Base Version	Maintenance Release Parity
7.3.21.2	7.3.21.1	N/A
7.3.21.1	7.3.20.2	N/A
7.3.20.3	7.3.20.2	N/A
7.3.20.2	7.3.20.1	N/A
7.3.20.1	7.3.19.1	N/A
7.3.19.3	7.3.19.2	N/A
7.3.19.2	7.3.19.1	N/A
7.3.19.1	7.3.18.2	N/A
7.3.18.4	7.3.18.3	N/A
7.3.18.3	7.3.18.2	N/A
7.3.18.2	7.3.18.1	N/A
7.3.18.1	7.3.17.1	N/A
7.3.17.4	7.3.17.3	6.7.5.25
7.3.17.3	7.3.17.2	6.7.5.25
7.3.17.2	7.3.17.1	6.7.5.25
7.3.17.1	7.3.16.2	6.7.5.25
7.3.16.4	7.3.16.3	6.7.5.24
7.3.16.3	7.3.16.2	6.7.5.24
7.3.16.2	7.3.16.1	6.7.5.24
7.3.16.1	7.3.15.1	6.7.5.24
7.3.15.5	7.3.15.4	6.7.5.23
7.3.15.4	7.3.15.3	6.7.5.23
7.3.15.3	7.3.15.2	6.7.5.23
7.3.15.2	7.3.15.1	6.7.5.23
7.3.15.1	7.3.14.2	6.7.5.23

GA or PR Release	Base Version	Maintenance Release Parity
7.3.14.6	7.3.14.5	6.7.5.23
7.3.14.5	7.3.14.4	6.7.5.23
7.3.14.4	7.3.14.3	6.7.5.23
7.3.14.3	7.3.14.2	6.7.5.23
7.3.14.2	7.3.14.1	6.7.5.23
7.3.14.1	7.3.13.3	6.7.5.23
7.3.13.5	7.3.13.4	6.7.5.22
7.3.13.4	7.3.13.3	6.7.5.22
7.3.13.3	7.3.13.2	6.7.5.22
7.3.13.2	7.3.13.1	6.7.5.22
7.3.13.1	7.3.12.1	6.7.5.22
7.3.12.1	7.3.11.3	6.7.5.21
7.3.11.1 and 7.3.11.2 are no longer available. These releases are replaced by SGOS 7.3.11.3.	7.3.10.1	6.7.5.19
7.3.10.1	7.3.9.2	6.7.5.19
7.3.9.1 is no longer available. This release is replaced by SGOS 7.3.9.2.	7.3.8.2	6.7.5.18
7.3.8.1 is no longer available. This release is replaced by SGOS 7.3.8.2.	7.3.7.1	6.7.5.17
7.3.7.1	7.3.6.1	6.7.5.16
7.3.6.1	7.3.5.1	6.7.5.14
7.3.5.1	7.3.4.1	6.7.5.13, 7.2.8.1
7.3.4.1	7.3.3.1	6.7.5.12, 7.2.7.2
7.3.3.1	7.3.2.1	6.7.5.10, 7.2.6.1
7.3.2.1	7.3.1.1	6.7.5.9, 7.2.5.1
7.3.1.1	7.2.3.1	6.7.5.7
7.2.8.1	7.2.7.1	6.7.5.13, 7.3.4.1
7.2.7.1	7.2.6.1	6.7.5.11
7.2.6.1	7.2.5.1	6.7.5.10
7.2.5.1	7.2.4.1	6.7.5.9
7.2.4.1	7.2.3.1	6.7.5.8
7.2.3.1	7.2.2.1	6.7.5.7
7.2.2.1	7.2.1.1	6.7.5.6
7.2.1.1	6.7.5.2	7.1.1.1, 7.2.0.1

Information About All 7.x Releases

- Web VPM Releases in SGOS
- Known Issues in SGOS 7.x
- Limitations in SGOS 7.x
- SGAC Releases in SGOS
- Documentation and Feedback

SGOS 7.3.21.2 PR

Release Information

- Release Date: August 26, 2024
- Build Number: 298064

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1 and later
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 3.3.1.1 and later
- Content Analysis : 3.1.2.2 and later
- SSL Visibility: 4.5.1.1 and later, and 5.4.1.1 and later
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of the supporting components:

- Edge SWG Admin Console (SGAC): 2.2.3
- Web Visual Policy Manager (Web VPM): 2.2.3

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following upgrade/downgrade paths are supported for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4 and later, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.21.2

SGOS 7.3.21.2 includes the following bug fix:

Table 1: Drivers

ID	Issue
SG-39488	Fixes an issue where the appliance restarted due to a driver reset caused by certain proxy features and network traffic overrunning the Elastic Network Adapter (ENA) buffers. Depending on your network conditions, the appliance could have restarted frequently. This issue affected Edge SWG virtual appliances running on AWS with an instance type of M5 or M6i.

SGOS 7.3.21.1 GA

Release Information

- Release Date: July 17, 2024
- Build Number: 297278

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1 and later
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 3.3.1.1 and later
- Content Analysis : 3.1.2.2 and later
- SSL Visibility: 4.5.1.1 and later, and 5.4.1.1 and later
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of the supporting components:

- Edge SWG Admin Console (SGAC): 2.2.3
- Web Visual Policy Manager (Web VPM): 2.2.3

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following upgrade/downgrade paths are supported for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4 and later, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.21.1

New Severity Level for Access Log Size Limit

For event log messages that pertain to access logs that have reached the size limit, the severity level for these log messages has changed from `informational` to `severe` . This change ensures you are notified when the access log is close to the limit and that it will stop logging new entries or delete old entries (depending on policy). You can also view the event log to troubleshoot errors that occur when the appliance uploads the access log to a server.

To view the access log limits, use the `>show access-log command` . To configure the access log limits and policy, use the `max-log-size` and `overflow-policy` subcommands of the `#(config) access-log` command. To configure the event log notification settings, use the `#(config) event-log` command.

Policy Trace Improvements

In policy traces, authentication entries now include more timestamps. Also, unless you enable the verbose level for authentication entries, authentication entries are filtered out of the trace. To enable different levels for authentication entries, use the `define probe` definition.

SkyUI Removal

The SkyUI user interface is potentially vulnerable to security issues, and was disabled by default in 7.3.1.1. In releases before 7.3.21.1, you could re-enable SkyUI using an option in the `# (config ui)` command. In this release, the `# (config ui)` command has been removed.

The following advanced URLs are also removed:

- /ui
- /ui/index.htm
- /sky
- /sky/index.htm
- /sky/wanop.html
- /sky/wanop-disabled.html
- /sky/system_up.xml

New Size Controls for HTTP/2 Connections and Streams

To enable you to control the speed of data transfers over HTTP/2 connections and streams, the following new CPL properties have been added:

- `http2.client.connection_window_size(`*bytes*`)`
- `http2.client.stream_window_size(`*bytes*`)`
- `http2.server.connection_window_size(`*bytes*`)`
- `http2.server.stream_window_size(`*bytes*`)`

Use these properties to speed up data transfers when specific HTTP/2 domains are experiencing high latency. The server properties affect response data (such as downloads) and the client properties affect request data (such as POST or PUT requests). If the downloading speed is slow, applying the server window properties may improve the speed.

> **NOTE**
> The `http2.client.connection_window_size()` and `http2.client.stream_window_size()` properties must be set before the client connection is upgraded to HTTP/2. These properties commit early because the HTTP/2 client upgrade occurs before the appliance processes HTTPS requests. To ensure the window size is set before the HTTP/2 client upgrade occurs, use the `client.connection.ssl_server_name=` condition to set the client-side window sizes for a specific domain.

Also, the maximum window size for an HTTP/2 stream has increased from 262144 bytes to 1048576 bytes. The default value for the connection window size is 524286 bytes. The default value for the stream window size is 65535 bytes.

More information:

- http2.client.connection_window_size()
- http2.client.stream_window_size()
- http2.server.connection_window_size()
- http2.server.stream_window_size()
- #(config) http2

Exclude Headers from Being Added

To ensure headers and strings are not leaked if a fail open happens, a new parameter has been added to the `set()` action:

> **NOTE**
> This parameter only applies to the request.x_header.header_name headers.

```
set(header, string [, exclude_from_origin])
```

More information:

- Content Policy Language Reference

Update to Event Log Message for PCAP Filters

To make event log messages for PCAP filtering clearer and easier to locate, the message for when you have enabled PCAP filtering now includes the filter keywords.

Increase in the Policy Trace Size

To ensure the appliance provides enough space for advanced policy diagnostics, the default size limit for policy traces has been increased from 1 MB to 10 MB.

Fixes in SGOS 7.3.21.1

SGOS 7.3.21.1 includes the following bug fixes:

Table 2: Authentication

ID	Issue
SG-36502	Fixes an issue where the access log caused the appliance to restart when an authenticated user was logged out because the surrogate expired. This issue occurred on HTTP/2 connections.
SG-37792	Fixes an issue where the appliance restarted when it attempted to parse malformed DNS responses during IWA direct realm processing.
SG-37847	Fixes an issue where the appliance restarted while it was authenticating Kerberos constrained delegation on HTTP/2 connections.
SG-37979	Fixes an issue where the appliance restarted after it left the last domain (for IWA direct realm operations) that it had joined.
SG-38785	Fixes a rare deadlock issue where the appliance stops responding due to a particular lock not being released. This issue occurred in environments that use IWA Direct authentication.
SG-38859	Fixes an issue where the appliance restarted due to a thread signaling that it was no longer running. The call for the signal now has a guard to handle threads that are no longer running.
SG-38904	Fixes an issue where performance degraded and websites would not load. Memory management has been improved to reduce the chance of performance degradation when the appliance processes idle users.

Table 3: FTP Proxy

ID	Issue
SG-38542	Fixes an issue where the FTP proxy would convert a plain control channel into a secure data channel. This issue occurred when the appliance received FTP commands that were intended for secure connections.

Table 4: HTTP Proxy

ID	Issue
SG-38672	Fixes a latency issue where there was a noticeable delay when the appliance proxied small HTTP/2 traffic between a client and server. This issue occurred for sites that send and receive small requests.
SG-38924	Fixes an issue where an "internal_error" page appeared after loading an email that contained links in the browser and, after waiting 10 seconds, clicking the links. This issue only occurred when the appliance was proxying HTTP/2 traffic, and when both the client and server supported HTTP/2 protocol.
SG-39318	Fixes an issue where clients could not download large files over HTTP/2 when ICAP scanning was configured and certain HTTP/2 parameters were set to higher than default values. Now, you can increase the HTTP/2 settings and can download large files with ICAP enabled.

Table 5: Kernel

ID	Issue
SG-38716	Fixes an issue where the appliance restarted due to a rare timing condition that is related to kernel locking.

Table 6: Network Drivers

ID	Issue
SG-39140	Fixes an issue where the appliance restarted when enabling a network interface from either the Admin Console or the CLI. This issue occurred due to static routes of the appliance overlapping the IP route of the interface that was being enabled.
SG-39230	Fixes an issue where the network interface driver incorrectly reset for Edge SWG virtual appliances running in AWS Marketplace. This issue affected M5 and M6i instances. To resolve this issue, a correction to the time calculation for the driver was made.

Table 7: Performance

ID	Issue
SG-38733	Fixes an issue where secure tunnel connections did not properly close, causing the appliance to stop responding. A check has been added to ensure that secure tunnel connections close.

Table 8: Policy

ID	Issue
SG-36889	Fixes an issue where the appliance delayed terminating transactions that policy determined should be terminated (with a verdict of force deny). This issue was more likely to affect environments where an upstream proxy had an Internet connection and a downstream proxy did not have an Internet connection.

Table 9: Security

ID	Issue
SG-39331	Fixes a vulnerability that could allow attackers to craft SSL traffic which would cause the appliance to crash.

Table 10: SOCKS Proxy

ID	Issue
SG-38585	Fixes an issue where the performance of the SOCKS proxy degraded due to the appliance inefficiently handling SOCKS code and it not having enough of a buffer to download content from the server. This issue occurred when the appliance was handling large amounts of policy updates.

Table 11: SSL Proxy

ID	Issue
SG-35504	Fixes an issue where the appliance restarted when the appliance initialized the session cache for the SSL device profile.
SG-38735	Fixes an issue where TLS connections that the Edge SWG appliance did not intercept would break. This issue occurred using a browser that had ECH disabled and Kyber PQC enabled.
SG-38767	Fixes an issue where you could delete an external certificate using the CLI when the certificate belonged to an external certificate list.

Table 12: SSL/TLS and PKI

ID	Issue
SG-39179	Fixes an issue where a corrupted device profile prevented the Edge SWG appliance from reloading and a faulty check caused the appliance to restart. If you attempted to upgrade, this issue might have prevented the appliance from loading the new version of SGOS.

Table 13: TCP/IP and General Networking

ID	Issue
SG-38058	Fixes an issue where the appliance incorrectly ignored TCP SYN requests that had a greater sequence number than the previous connection in the same tuple.
SG-38131	Fixes an issue where the appliance rebooted when it encountered Intel-10G cards that have a hardware defect. Now the appliance performs a hardware reboot to re-initialize the defective card.
SG-38638	Fixes an issue that caused the appliance to restart when network traffic was high.
SG-38837	Fixes an issue where download speed was impacted due to a data-processing delay in the Large Receive Offload (LRO) of the appliance. This issue occurred when the LRO was coalescing data packets.
SG-38930	Fixes an issue where the appliance restarted due to a connection closing before a packet could be received.

SGOS 7.3.20.3 PR

Release Information

- Release Date: August 26, 2024
- Build Number: 298063

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1 and later
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 3.3.1.1 and later
- Content Analysis : 3.1.2.2 and later
- SSL Visibility: 4.5.1.1 and later, and 5.4.1.1 and later
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of the supporting components:

- Edge SWG Admin Console (SGAC): 2.2.2
- Web Visual Policy Manager (Web VPM): 2.2.2

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following upgrade/downgrade paths are supported for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4 and later, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.20.3

SGOS 7.3.20.3 includes the following bug fix:

Table 14: Drivers

ID	Issue
SG-39488	Fixes an issue where the appliance restarted due to a driver reset caused by certain proxy features and network traffic overrunning the Elastic Network Adapter (ENA) buffers. Depending on your network conditions, the appliance could have restarted frequently. This issue affected Edge SWG virtual appliances running on AWS with an instance type of M5 or M6i.

SGOS 7.3.20.2 PR

Release Information

- Release Date: June 24, 2024
- Build Number: 296885

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.2
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.2

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.20.2

- See Fixes in SGOS 7.3.20.2.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.20.2

SGOS 7.3.20.2 includes the following bug fixes:

Table 15: Network Drivers

ID	Issue
SG-39140	Fixes an issue where the appliance restarted when enabling a network interface from either the Admin Console or the CLI. This issue occurred due to static routes of the appliance overlapping the IP route of the interface that was being enabled.
SG-39230	Fixes an issue where the network interface driver incorrectly reset for Edge SWG virtual appliances running in AWS Marketplace. This issue affected M5 and M6i instances. To resolve this issue, a correction to the time calculation for the driver was made.

Table 16: SSL/TLS and PKI

ID	Issue
SG-38735	Fixes an issue where TLS connections that the Edge SWG appliance did not intercept would break. This issue occurred using a browser that had ECH disabled and Kyber PQC enabled.

SGOS 7.3.20.1 GA

Release Information

- Release Date: May 21, 2024
- Build Number: 296149

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1 and later
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 3.3.1.1 and later
- Content Analysis : 3.1.2.2 and later
- SSL Visibility: 4.5.1.1 and later, and 5.4.1.1 and later
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): 2.2.2
- Web Visual Policy Manager (Web VPM): 2.2.2

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following upgrade/downgrade paths are supported for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4 and later, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.20.1

- See Features in SGOS 7.3.20.1.

Fixes in ProxySG 7.3.20.1

- See Fixes in SGOS 7.3.20.1.
- To see any Security Advisories that apply to the version you are running, go to: https://support.broadcom.com/security-advisory/security-advisories-list.html

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.20.1

New Command to Test Destination Route

To troubleshoot networking and routing issues, use the following CLI command to test the route that the appliance takes to a host or IP address:

```
>test route {host_name|ip_address} [ipv4|ipv6]
```

More information:

- Command Line Interface Reference

Updates to the CachePulse Database

April 23, 2024, Broadcom published an update to the Edge SWG Cachepulse Database. This update fixed an issue where the appliance displayed the following warning during policy compilation:

```
Warning : some previous subnet specifiers have been made redundant by: '123.128.0.0/13'
```

Customers were more likely to see this error under the following conditions:

- The Edge SWG appliance was running either SGOS 7.3.18.1 and later, or SGOS 7.4.2.1 and later.
- Policy contained subnet definitions that referenced redundant specifiers.

No customer action was required to receive this update. For information on the CachePulse service, see the SGAC Administration guide.

Trust Package Update

The trust package is updated automatically as part of the upgrade process. Obsolete CAs have been removed, and new or updated CAs have been added.

If you are not upgrading, to download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

More information:

- Command Line Interface Reference

Specify a CCL for CA Certificates

When importing your CA certificate, you can now add it to a CCL simultaneously. Before you can add a CA certificate to a CCL, the CCL must exist. To add a certificate to a CCL, use the optional `ccl` parameter in the following command:

```
# (config ssl) inline ca-certificate name ccl eof
```

More information:

- Command Line Interface Reference

Improved Event Log Messages for Buffer Size

For event log messages that are about the maximum buffer size being exceeded, the wording has been clarified. These messages occur when the appliance transforms HTTP responses in a reverse proxy deployment and exceeds the buffer size. Previously, the event log logged the message "Out of memory for Page Factory (resource limit exceeded)." Now, it logs the message "Buffer exceeded max limit 24MB while transforming http response for <*url*>."

Health Check Improvement

To reduce the chance that the appliance incorrectly labels a domain as unhealthy, the schannel status has been removed from the domain health check.

Fixes in SGOS 7.3.20.1

SGOS 7.3.20.1 includes the following bug fixes:

Table 17: Access Logging

ID	Issue
SG-38412	Fixes an issue when adding a filter to an access log tail, where the space character did not apply the filter correctly and prevented some matches from appearing. This value has now been properly encoded.
SG-38441	Fixes an issue when adding a filter to an access log tail, where the `%` and `&` characters did not apply the filter correctly and prevented some matches from appearing. These values have now been properly encoded.

Table 18: Authentication

ID	Issue
SG-36940	Fixes a regression issue that was introduced in version 7.3.8 where LDAP authentication added a small latency.
SG-36104	Fixes an issue during NTLM authentication of an HTTP/2 connection where the following exception page appeared: "Authentication agent rejected request (context lost)".

Table 19: CLI Consoles

ID	Issue
SG-37783	Fixes an issue when performing a category lookup using the Symantec Management Console (**Administration** > **Content Filtering** > **Test Category Match**) where a URL that contained a protocol scheme (such as "http://") produced no results because the double slash characters require base64 encoding.
SG-38005	Fixes an issue during system reboots, where syslog failure messages were falsely reported in the event log before the network was ready. With this fix, the syslog socket is created when the network is ready.
SG-37057	Fixes a timing issue when an SSH connection was closed while processing data, which caused the appliance to restart.

Table 20: DNS Proxy

ID	Issue
SG-38101	Fixes an issue in DNS proxy that is used in bridge mode where DNS responses were not being sent out by the appliance. The responses were not sent because both the source and destination MAC addresses of the response were addresses of interfaces on the appliance.
SG-38546	Fixes an issue when SSL Proxy tunnels a connection and parallel connectivity is enabled, where the SSL request failed and displayed the error `TE_CONNECT_ERROR_DNS_NO_DATA` . The error occurred because the parallel connectivity manager interpreted the absence of IPv4 or IPv6 records as a DNS connection failure.

Table 21: Hardware Drivers

ID	Issue
SG-38484	Fixes an issue where some memory failed to be written to core images used in SR analysis. This change attempts to better account for which memory has been written into the resulting core images.
SG-38577	Fixes an issue where the networking interface of the Edge SWG virtual appliance (VA) was unresponsive and only recovered after restarting the system. This issue affects VAs running on AWS Marketplace that have the instance type M5 or M6i.

Table 22: Health Checks

ID	Issue
SG-38563	Fixes an issue where concurrent HC health status queries caused the appliance to restart due to an internal timeout.

Table 23: HTTP Proxy

ID	Issue
SG-38483	Fixes an issue during the transition from HTTP to Webex where the appliance restarted after not properly cleaning up transaction data.
SG-37608	Fixes a rare unplanned restart during upstream HTTP/2 connections.
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

Table 24: ICAP

ID	Issue
SG-38480	Fixes an issue where the policy of ICAP RESPMOD header modification action did not take effect when the ICAP RESPMOD service was forced to rescan and the requested object was fresh in the cache.
SG-38532	Fixes an issue where the appliance restarted when both ICAP REQMOD mirror and RESPMOD were enabled.

Table 25: Kernel

ID	Issue
SG-38569	Fixes a very rare race condition at startup where a software assertion triggers incorrectly and causes a restart. A software assertion is an internal check that coding assumptions are correct. This code resolves the race condition so that the assertion is not triggered.

Table 26: Policy

ID	Issue
SG-38162	Fixes an issue where the ws:// and wss:// schemes are not recognized as valid and supported schemes by the content transformer engine of the appliance.
SG-38487	Fixes a potential memory leak issue with tenant policies having numerous `server.certificate.hostname` conditions in the CPL snippet.

Table 27: Proxy Forwarding

ID	Issue
SG-38132	Fixes an issue when creating forwarding hosts, using the Command Line Interface (CLI) or the Secure Gateway Admin Console (SGAC) UI, where the command accepted any string as a domain name. This string was accepted even if it was a hostname not compatible with the specifications. More validation checks for the hostname are now added after domain names are entered.

Table 28: Security

ID	Issue
SG-20816	The libexpat library has been upgraded to resolve vulnerabilities that are related to XML parsing. None of the vulnerabilities were exploitable in SGOS.
SG-35669	Fixes a vulnerability that could allow attackers to consume excessive resources by sending specifically crafted IP fragments to the Edge SWG appliance.

Table 29: SSL Proxy

ID	Issue
SG-37486	Fixes an issue where the appliance restarted due to a configuration change being made while the appliance was processing traffic.
SG-38295	Fixes an issue where, if the ALPN changed from the full TLS v1.3 handshake to the resumed TLS v1.3 handshake, the ALPN selected was incorrectly taken from the full TLS v1.3 handshake. Due to the HTTP protocol mismatch, content was not properly delivered to the browser.

Table 30: TCP/IP and General Networking

ID	Issue
SG-38061	Fixes an issue where there was a discrepancy in the client and server bytes statistics for UDP Tunneling proxy connections when comparing the totals in Proxy Services (**Reports** > **Traffic Details**) to Interfaces (**Reports** > **Interface History**).
SG-38149	Fixes an issue where browser pages loaded slowly due to a delay in the Edge SWG appliance establishing a connection to a downstream device. This delay occurred because the appliance used the incorrect interface when responding to the downstream device. After the appliance established the connection, the pages loaded. This issue might occur in environments where the downstream device uses the same source IP address for most of its connections to an upstream Edge SWG appliance.
SG-38164	Fixes an issue where setting the `expect-proxy-protocol` attribute on the proxy service (for example, explicit http) delayed subsequent connections, if the prior connection did not send any data.

Table 31: Web Application Firewall

ID	Issue
SG-38488	Fixes an issue in http requests by introducing base64-decoding of the argument key and argument value in the http request when the gesture `http.request.normalization.default(auto)` is used.

SGOS 7.3.19.3 PR

Release Information

- Release Date: June 24, 2024
- Build Number: 296886

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.1
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.1

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.19.3

- See Fixes in SGOS 7.3.19.3.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.19.3

SGOS 7.3.19.3 includes the following bug fixes:

Table 32: CLI Consoles

ID	Issue
SG-38005	Fixes an issue during system reboots, where syslog failure messages were falsely reported in the event log before the network was ready. With this fix, the syslog socket is created when the network is ready.

Table 33: Network Drivers

ID	Issue
SG-39140	Fixes an issue where the appliance restarted when enabling a network interface from either the Admin Console or the CLI. This issue occurred due to static routes of the appliance overlapping the IP route of the interface that was being enabled.

Table 34: SSL/TLS and PKI

ID	Issue
SG-38735	Fixes an issue where TLS connections that the Edge SWG appliance did not intercept would break. This issue occurred using a browser that had ECH disabled and Kyber PQC enabled.

SGOS 7.3.19.2 PR

Release Information

- Release Date: May 3, 2024
- Build Number: 295408

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.1
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.1

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.19.2

- See Fixes in SGOS 7.3.19.2.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.19.2

SGOS 7.3.19.2 includes the following bug fixes:

Table 35: HTTP Proxy

ID	Issue
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

SGOS 7.3.19.1 GA

Release Information

- Release Date: April 1, 2024
- Build Number: 294941

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 3.3.x and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 3.1.2.2 and later
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.1
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.1

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following upgrade/downgrade paths are supported for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.19.1

- See Features in SGOS 7.3.19.1.

Fixes in ProxySG 7.3.19.1

- See Fixes in SGOS 7.3.19.1.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.19.1

Filter for the Access Tail Log

To easily filter for specific log lines in access logs, filters can be applied. To apply these filters, use Advanced URL query strings. The filters are not case-sensitive.

The advanced query strings filter the output by matching values in the log output to the values that you provide in the strings. For example, if you apply the filter with the parameter `/Accesslog/tail-f/main?filter=example.com` to the access log tail, the appliance displays access log lines that contain `example.com`.

If you supply multiple values in a filter, then the appliance displays lines that contain all values. For example, if you apply the filter with the parameters `/Accesslog/tail-f/main?filter=example.com"&filter=TCP_HIT`, then the appliance displays lines that contain both `example.com` and `TCP_HIT`. Lines that only contain `example.com` or only contain `TCP_HIT` are not displayed.

> **NOTE**
> You cannot use the following special characters in query strings:
>
> - Empty space
> - %
> - &

New CPL Property to Tolerate Errors During SOCKS Authentication

To ensure unimportant errors do not impede SOCKS authentication, the new CPL property `socks_authenticate.tolerate_error()` has been added. This property allows you to specify certain errors that the appliance should allow during SOCKS authentication.

More information:

- Content Policy Language Reference

Track Policy Rule that Disables SSL Interception

To help you track which policy rule disables SSL interception, you can configure the access log to report the policy ID of the rule that contains `ssl.foward_proxy(no)` in the SSL intercept layer. To configure this feature, use the `reference_id.parent_transaction()` property. The following example shows the syntax to configure this feature:

```
<ssl-intercept>
      url.domain=example.com ssl.foward_proxy(no) reference_id.parent_transaction(12345)
```

You can also choose to append the ID of the rule that disables SSL interception to an existing ID of another layer. For example, if you apply the following policy, the policy ID that appears in the access log is “`abc;12345` ”:

```
<proxy>
      url.domain=mysite.com condition=test reference_id(abc)

<ssl-intercept>
      url.domain=mysite.com ssl.foward_proxy(no) reference_id.parent_transaction.append(12345)
```

More information:

- Content Policy Language Reference

Improved Detection Speed for Unreachable Gateways

For networks that distribute traffic through multiple default gateways, the appliance now detects when a gateway is unreachable in 20-30 seconds. Previously, it could take over a minute to detect an unreachable gateway.

More information:

- SGAC Admin Guide

Improved Behavior for http2.server.request(preserve)

The CPL property `http2.server.request(preserve)` has been improved. The `http2.server.request(preserve)` property now only requests HTTP/2 on upstream connections, if the client connection negotiated HTTP/2. Previously, this property requested HTTP/2 on new upstream connections when the client connection originally requested HTTP/2 and then downgraded to HTTP/1.1.

Fixes in SGOS 7.3.19.1

SGOS 7.3.19.1 includes the following bug fixes:

Table 36: Access Logging

ID	Issue
SG-37307	Fixes an issue where, under certain conditions, the appliance could enter in an infinite loop when trying to upload access logs using SCP to a remote server but failing each time.
SG-37630	Fixes an issue where the access log SCP client was stuck in an infinite loop trying to upload access logs that were corrupted on the appliance.
SG-37349	Fixes an issue during the SCP upload of the access log, where random data was uploaded to the SSH server.
SG-37446	Fixes an issue where TCP connections from the appliance might have stalled, resulting in almost no data being transmitted. This issue only occurred for TCP connections that experienced significant packet loss in the network and that used the default New Reno congestion control algorithm. When in a stalled state, the appliance sends 1 byte of application data every 5 seconds. This issue was extremely rare and was detected for long-running connections, such as uploading access logs in continuous mode.

Table 37: Authentication

ID	Issue
SG-38097	Fixes an issue where the appliance was failing to decrypt Kerberos AES tickets because either the machine account name of the appliance or the service account (load balancer) name was too long.

Table 38: CLI Consoles

ID	Issue
SG-37658	Fixes an issue where the encoded invalid character '\' was causing a problem in Symantec Management Center after it was decoded and parsed by Apache libraries. This issue was fixed by base 64 encoding the problematic part of the URL.

Table 39: Event Logging

ID	Issue
SG-30776	Fixes an issue where the appliance restarted after trying to log an event with an empty message, caused by race conditions during accesslog facility creation/deletion.

Table 40: Health Checks

ID	Issue
SG-37960	Fixes an issue where some health checks with a healthy threshold greater than 1 flipped between Unknown and OK very often, even though the remote server being checked would be OK. Now, when the health check returns OK, it sets the health to OK if it was previously Unknown, even if the healthy threshold has not been reached.

Table 41: HTTP Proxy

ID	Issue
SG-37790	Fixes an issue where the appliance restarted during HTTP/2 transactions due to a race condition when creating the categories list.
SG-36813	Fixes an issue where the appliance sent an HTTP/1.1 request to the OCS over an HTTP/2 connection, leading to an invalid response.
SG-35733	Fixes an issue in explicit proxy mode where accessing web applications that use WebSocket requests failed in the Safari browser running on Mac OS.
SG-36791	Fixes an issue where the appliance delayed sending HTTP/2 data to client machines for certain websites that had dependencies between the streams. Users who experienced this issue may have noticed slow responses to requests over HTTP/2 and may have seen the following message in the HTTP debug log: `Triggering primary send after Timer_expired_event.`
SG-38096	Fixes an issue where if the appliance had to restart a websocket upgrade request (HTTP1/1) for any reason (for example, a header larger than 8k, or if the websocket upgrade request was not the first request on the same connection), the appliance attempted to go through the SSL tunnel rather than the plain tunnel.
SG-38473	Fixes an issue where the appliance displayed the incorrect exception pages for certain HTTP error codes when policy referenced those codes. The appliance incorrectly displayed the following default exception pages: • Network Error (dns_server_failure) Your request could not be processed because an error occurred contacting the DNS server • Appliance Error (internal_error) An unrecoverable error was encountered The appliance served these default pages because it could not find the specific error codes in its list of error codes to serve the correct pages.

Table 42: Kernel

ID	Issue
SG-38025	Fixes an issue where a tuning parameter for protecting storage that was introduced in version 7.3.15.1 was causing traffic to be rejected in some bursty connection workloads. The tuning parameter is now disabled by default.
SG-37442	Fixes an issue where the appliance restarted and displayed a 0x5D error due to excessive time spent recovering memory.
SG-38057	Fixes an issue where the appliance restarted because the network stack was allocating packets faster than it was freeing them, causing memory to be exhausted very quickly.

ID	Issue
SG-37793	Fixes an issue where the appliance restarted because the kernel recursed during memory management, leaving it in an inconsistent state.

Table 43: Policy

ID	Issue
SG-37980	Fixes an issue where a stack overflow occurred in certain situations during a dynamic categorization lookup (drtr), as part of policy evaluation.

Table 44: SSL/TLS and PKI

ID	Issue
SG-38098	Fixes an issue where the Certificate Signing Requests (CSRs) generated by the appliance used an incorrect version number that is not defined in the Internet Engineering Task Force (IETF) specifications.
SG-37258	Fixes an issue where the appliance restarted due to multiple threads accessing the certificate store and corrupting entries.

Table 45: SSL Proxy

ID	Issue
SG-37821	Fixes an issue where the appliance restarted when "diffie-hellman-group14-sha1" was selected as a key exchange algorithm with the SSH servers for archive uploads, or the access log upload functionality on the appliance.

Table 46: TCP/IP and General Networking

ID	Issue
SG-36656	Fixes an issue where the source MAC address used for different types of requests (such as ARP requests, ARP responses, TCP ACKs, Neighbor solicitation, Neighbor advertisements) is not consistent when the outgoing interface is part of a bridge. This inconsistency can cause other devices in the network to drop packets intended for the appliance.
SG-38014	Fixes an issue for networks that distribute traffic through multiple default gateways, where the appliance was taking longer than a minute to detect an unreachable gateway.
SG-38159	Fixes an issue in versions 7.3.15.1 to 7.3.18.1 using SOCKs and tunneling UDP traffic, where the appliance stopped processing traffic (GUI, proxy data, and so on) due to a lock order race condition.
SG-38182	Fixes an issue where VLAN traffic that passes through a bridge was very slow due to inefficiencies in traffic processing.
SG-38155	Fixes an issue where a network with multiple ISG appliances was experiencing slowness because incorrect TSO settings were used when VLAN traffic was being sent on a bridge.
SG-38489	Fixes an issue where VLANs on the bridge of the appliance could not accept traffic, resulting in users being unable to access the Internet. This issue occurred due to the appliance mistakenly dropping ARP requests. When the appliance dropped ARP requests due to this issue, you may have noticed the advanced URL /TCP/Statistics TCP1.416 'ARP don't resolve on auto created VLAN' reported the number of ARP requests that the appliance dropped.

Table 47: URL Filtering

ID	Issue
SG-38115	Fixes an issue where the appliance restarted when a portion of the Content Filtering database was missing due to missing data on a failing disk.
SG-37820	Fixes an issue where IPv6 addresses that are IPv4-compatible were not being correctly converted to IPv4 addresses.

SGOS 7.3.18.4 PR

Release Information

- Release Date: June 28, 2024
- Build Number: 296882

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.1
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.1

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.18.4

- See Fixes in SGOS 7.3.18.4.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.18.4

SGOS 7.3.18.4 includes the following bug fixes:

Table 48: CLI Consoles

ID	Issue
SG-38005	Fixes an issue during system reboots, where syslog failure messages were falsely reported in the event log before the network was ready. With this fix, the syslog socket is created when the network is ready.

Table 49: SSL/TLS and PKI

ID	Issue
SG-38735	Fixes an issue where TLS connections that the Edge SWG appliance did not intercept would break. This issue occurred using a browser that had ECH disabled and Kyber PQC enabled.

SGOS 7.3.18.3 PR

Release Information

- Release Date: May 1, 2024
- Build Number: 295507

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.5
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.18.3

- See Fixes in SGOS 7.3.18.3.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.18.3

SGOS 7.3.18.3 includes the following bug fixes:

Table 50: Access Logging

ID	Issue
SG-37446	Fixes an issue where TCP connections from the appliance might have stalled, resulting in almost no data being transmitted. This issue only occurred for TCP connections that experienced significant packet loss in the network and that used the default New Reno congestion control algorithm. When in a stalled state, the appliance sends 1 byte of application data every 5 seconds. This issue was extremely rare and was detected for long-running connections, such as uploading access logs in continuous mode.

Table 51: HTTP Proxy

ID	Issue
SG-38473	Fixes an issue where the appliance displayed the incorrect exception pages for certain HTTP error codes when policy referenced those codes. The appliance incorrectly displayed the following default exception pages: • Network Error (dns_server_failure) Your request could not be processed because an error occurred contacting the DNS server • Appliance Error (internal_error) An unrecoverable error was encountered The appliance served these default pages because it could not find the specific error codes in its list of error codes to serve the correct pages.
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

Table 52: Kernel

ID	Issue
SG-38025	Fixes an issue where a tuning parameter for protecting storage that was introduced in version 7.3.15.1 was causing traffic to be rejected in some bursty connection workloads. The tuning parameter is now disabled by default.

Table 53: TCP/IP and General Networking

ID	Issue
SG-38159	Fixes an issue in versions 7.3.15.1 to 7.3.18.1 using SOCKs and tunneling UDP traffic, where the appliance stopped processing traffic (GUI, proxy data, and so on) due to a lock order race condition.
SG-38489	Fixes an issue where VLANs on the bridge of the appliance could not accept traffic, resulting in users being unable to access the Internet. This issue occurred due to the appliance mistakenly dropping ARP requests. When the appliance dropped ARP requests due to this issue, you may have noticed the advanced URL /TCP/ Statistics TCP1.416 'ARP don't resolve on auto created VLAN' reported the number of ARP requests that the appliance dropped.

SGOS 7.3.18.2 PR

Release Information

- Release Date: February 6, 2024
- Build Number: 293668

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.5
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.18.2

- See Fixes in SGOS 7.3.18.2.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.18.2

SGOS 7.3.18.2 includes the following bug fixes:

Table 54: Authentication

ID	Issue
SG-37943	Fixes an issue where users that the Edge SWG appliance successfully authenticated by SAML received a 404 error when attempting to log into the appliance. This error occurred because the appliance incorrectly appended a comma to the request URL.

Table 55: Policy

ID	Issue
SG-37956	Fixes an issue where an incorrect SNI was sent upstream when the Edge SWG appliance was intercepting traffic. This issue occurred when the client did not supply an SNI in the SSL Client Hello and the Reverse DNS was not restricted.

SGOS 7.3.18.1 GA

Release Information

- Release Date: January 25, 2024
- Build Number: 293160

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.5
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.18.1

- See Features in SGOS 7.3.18.1.

Fixes in ProxySG 7.3.18.1

- See Fixes in SGOS 7.3.18.1.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.18.1

Deny and Exception Properties in Pre-Authentication Rules

You can create rules to deny users or return an exception to users without being overridden by subsequent authentication rules. The following properties are added to support this feature:

- deny.preauth()
- force_deny.preauth()
- exception.preauth()
- force_exception.preauth()

HTTP/2 Enhancements

To further protect against HTTP/2-based attacks, enhancements to how the appliance tracks HTTP/2 connections have been made, including the appliance logging a new message in the event log when HTTP/2 connections are reset.

Trust Package Update

The trust package is updated automatically as part of the upgrade process. Obsolete CAs have been removed.

If you are not upgrading, to download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

More information:

- Command Line Interface Reference

Transaction Variables Now Display Alphabetically

In a policy trace, the appliance lists the variable values that policy evaluation determines at the end of the rule evaluation trace. You can find these variables after the heading "Assigned values of transaction variables." To allow you to easily find variable values, these variables now display in alphabetical order. This change does not affect policy evaluation.

Improvement to Logging Errors for SNMP Packets

To help troubleshoot SNMP packets that could not be sent, the appliance now logs the reason why the packets could not be sent.

Improvements to TCP Statistics

The following improvements have been made to TCP statistics:

Statistic	New or Updated	Description
TCP2.213—retries due to collision	Updated	This statistic reports failures due to collision. A new counter has been added to track the number of times the appliance tries to find an available port. Use this statistic as an early warning that port space is becoming full.
TCP2.214—failures due to collision	Updated	This statistic reports the number of times that the TCP connection has failed during connection setup. Now, the number indicates that the call could not be completed due to a free port not being available.
TCP2.436—connect setup failures	New	This statistic reports the number of times the call could not be completed.

Fixes in SGOS 7.3.18.1

SGOS 7.3.18.1 includes the following bug fixes:

Table 56: Access Logging

ID	Issue
SG-37425	Fixes an issue where the appliance wrote Kafka logs to only one partition per broker. Now, it writes logs to all the partitions of all the brokers.

Table 57: Authentication

ID	Issue
SG-36973	Fixes an issue with the `deny.unauthorized` property where the pending authorization results were not committing early enough to return a 407 response code.
SG-37097	Fixes an issue where the redirection back to the OCS URL might not have succeeded after successful SAML authentication if the OCS URL contained complex query string syntax.
SG-37107	Fixes an issue where the appliance restarted due to a missing keytab entry in the memory keytab list.
SG-37485	Fixes an issue where the appliance stopped responding due to the authentication subsystem attempting to write the Kerberos keytab to the disk before the subsystem was initialized.

Table 58: CLI Consoles

ID	Issue
SG-37015	Fixes an issue where a typo in the `tcp-ip icmp-drop-redirect` command caused invalid output when attempting to install a configuration.

Table 59: FTP Proxy

ID	Issue
SG-37014	Fixes an issue where the appliance restarted due to an invalid memory location access.

Table 60: Health Monitoring

ID	Issue
SG-37167	Fixes a rare race condition that can occur with any Edge SWG configuration but only when the device first boots. The crash is reported in the PDM_Timer process.

Table 61: HTTP Proxy

ID	Issue
SG-33537	Fixes an issue where the appliance restarted because of a race condition that is related to resolving the server IP address.
SG-36496	Fixes an issue where the appliance restarted when processing HTTP/2 requests because the process was corrupted by mistaken failure signals.

Table 62: Kernel

ID	Issue
SG-36373	Fixes an issue in ICAP configurations where the appliance restarted due to a race condition when converting objects in RAM to disk.
SG-37772	Fixes an issue where TCP connections that were closed (either normally or by RST) while the Edge SWG appliance was sending data caused a memory leak. These connections are mostly handled by the proxy code for TCP Tunnel but they can be handled by other proxy codes, such as HTTPS.

Table 63: Licensing

ID	Issue
SG-37294	Fixes an issue where the auto-update feature for licenses was disabled on boot up for Edge SWG applications running on the SSP.

Table 64: Network Drivers

ID	Issue
SG-37569	Fixes an issue where the appliance ignored the ARP response from VLANs when ARP strict matching was disabled (`# (config)` **`tcp-ip arp-strict-matching disable`**).

Table 65: Policy

ID	Issue
SG-36458	Fixes a memory accumulation issue where the appliance did not dispose of policy execution records fast enough.
SG-37149	Fixes an issue where an unnecessary is_numeric check was introduced while generating server.certificate.hostname.list conditions.
SG-37216	Fixes an issue where the diagnostics probe captured unnecessary transactions when a condition contained a late-guard condition.
SG-37217	Fixes an issue where specific IE conditional comments were not properly parsed when rewriting the URL in the HTTP response.

Table 66: Proxy Forwarding

ID	Issue
SG-36972	Fixes an issue where a new firewall rule caused the Edge SWG appliance to drop failover advertisements for appliances using non-virtual IPs in Active/Active HA configurations. This issue caused both appliances in the configuration to be the primary machine.

Table 67: Security

ID	Issue
SG-36752	Fixes an issue where HTML form data entered in the Bridge/fwtable and Bridge/stats pages was not properly encoded, which could potentially allow an attacker to insert malicious code.

Table 68: SNMP

ID	Issue
SG-34988	Updates the Net-SNMP Library to resolve multiple vulnerabilities.

Table 69: SSL Proxy

ID	Issue
SG-36253	Fixes an issue where the appliance incorrectly issued the "IfYouSeeThisCertificateThisIsAnError" certificate when the TLS 1.3 session resumption between the appliance and the OCS resulted in a downgrade to TLS 1.2 or lower.
SG-36775	Fixes an issue where the ssl-device-profile configuration could not be applied correctly due to the order of the configuration settings in the `show config` output.
SG-37058	Fixes an issue where the appliance could not tunnel on protocol errors when the client only offered TLSv1.3 and the server selected an ECDSA server certificate for the signature algorithm.

Table 70: System Statistics

ID	Issue
SG-36923	Fixes an issue where the time base of the SNMP transactions mismatched the CPU time measurements.

Table 71: TCP/IP and General Networking

ID	Issue
SG-36354	Fixes an issue where, after upgrading to 7.3.14, S200 (single core) appliances experienced unexpected failover events due to delays in receiving timer signals. These delays caused failover to switch between the primary and secondary machines.
SG-36886	Fixes a FreeBSD IPv6 fragment assembly vulnerability.
SG-37293	Fixes an issue where the netflow timer that cleans up old connections stopped working after 49 days. This issue caused a memory leak in the appliance.
SG-37837	Fixes an issue in the Edge SWG network stack that occurred when the Edge SWG instance was deployed on SSP hardware or other virtual appliance platform. After 49 days, the Edge SWG appliance leaked connections that were in the 'last ACK wait' state. This leak prevented new TCP connections from being created.

SGOS 7.3.17.4 PR

Release Information

- Release Date: June 28, 2024
- Build Number: 296881

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.2.1
- Web Visual Policy Manager (Web VPM): Web VPM 2.2.1

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.17.4

- See Fixes in SGOS 7.3.17.4.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.17.4

SGOS 7.3.17.4 includes the following bug fixes:

Table 72: CLI Consoles

ID	Issue
SG-38005	Fixes an issue during system reboots, where syslog failure messages were falsely reported in the event log before the network was ready. With this fix, the syslog socket is created when the network is ready.

Table 73: SSL/TLS and PKI

ID	Issue
SG-38735	Fixes an issue where TLS connections that the Edge SWG appliance did not intercept would break. This issue occurred using a browser that had ECH disabled and Kyber PQC enabled.

SGOS 7.3.17.3 PR

Release Information

- Release Date: May 1, 2024
- Build Number: 295505

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.5
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.17.3

- See Fixes in SGOS 7.3.17.3.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.17.3

SGOS 7.3.17.3 includes the following bug fixes:

Table 74: Access Logging

ID	Issue
SG-37446	Fixes an issue where TCP connections from the appliance might have stalled, resulting in almost no data being transmitted. This issue only occurred for TCP connections that experienced significant packet loss in the network and that used the default New Reno congestion control algorithm. When in a stalled state, the appliance sends 1 byte of application data every 5 seconds. This issue was extremely rare and was detected for long-running connections, such as uploading access logs in continuous mode.

Table 75: HTTP Proxy

ID	Issue
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

Table 76: TCP/IP and General Networking

ID	Issue
SG-36728	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance caused packets to show up out of order. This issue occurred when TCP packets had options or were fragmented.
SG-38159	Fixes an issue in versions 7.3.15.1 to 7.3.18.1 using SOCKs and tunneling UDP traffic, where the appliance stopped processing traffic (GUI, proxy data, and so on) due to a lock order race condition.

SGOS 7.3.17.2 PR

Release Information

- Release Date: February 6, 2024
- Build Number: 293639

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.5
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.17.2

- See Fixes in SGOS 7.3.17.2.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.17.2

SGOS 7.3.17.2 includes the following bug fixes:

Table 77: Kernel

ID	Issue
SG-37772	Fixes an issue where TCP connections that were closed (either normally or by RST) while the Edge SWG appliance was sending data caused a memory leak. These connections are mostly handled by the proxy code for TCP Tunnel but they can be handled by other proxy codes, such as HTTPS.

Table 78: Policy

ID	Issue
SG-37956	Fixes an issue where an incorrect SNI was sent upstream when the Edge SWG appliance was intercepting traffic. This issue occurred when the client did not supply an SNI in the SSL Client Hello and the Reverse DNS was not restricted.

Table 79: TCP/IP and General Networking

ID	Issue
SG-37293	Fixes an issue where the netflow timer that cleans up old connections stopped working after 49 days. This issue caused a memory leak in the appliance.
SG-37837	Fixes an issue in the Edge SWG network stack that occurred when the Edge SWG instance was deployed on SSP hardware or other virtual appliance platform. After 49 days, the Edge SWG appliance leaked connections that were in the 'last ACK wait' state. This leak prevented new TCP connections from being created.

SGOS 7.3.17.1 GA

Release Information

- Release Date: November 9, 2023
- Build Number: 291392

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.17.1

- See Features in SGOS 7.3.17.1.

Fixes in ProxySG 7.3.17.1

- See Fixes in SGOS 7.3.17.1.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.17.1

ProxySG Admin Console 2.1.5

This release includes the ProxySG Admin Console (SGAC), which is a next-generation web interface.
The SGAC 2.1.5 release includes the contents of SGAC 2.1.4. The SGAC is the default interface that opens in the browser. The Java-based Management Console will be removed in a future release. To learn more about the SGAC, refer to the following KB article:

https://knowledge.broadcom.com/external/article/251426

- 2.1.5 changes and fixes: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/22864
- ProxySG Admin Console documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started.html
- SGAC Releases in SGOS

Web Visual Policy Manager 2.1.6

This release includes the Web Visual Policy Manager (Web VPM) 2.1.6 with the following enhancements:

- You can now search all levels of nested objects.
- Installing policy that includes the Set Effective Client IP object no longer triggers a deprecation warning.

For information on the Web VPM release, refer to the following documentation:

- Release announcement: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/22180
- Web VPM documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager.html
- Web VPM 2.1.6

New Health Monitoring Threshold for HTTP Client Utilization

The health monitoring metric for HTTP client utilization provides the percentage of the maximum number of simultaneous HTTP client sessions that the appliance is processing. You can view the HTTP Client Utilization in the Admin Console (**Reports > Health Monitoring > General**). To configure warning and critical thresholds and intervals for HTTP client utilization, use the following CLI command:

```
#(config)alert threshold http-client-utilization
 warning_threshold warning_interval critical_threshold critical_interval
```

To configure notifications for when the percentage of HTTP client utilization reaches the warning and critical thresholds, use the following CLI command:

```
#(config)alert notification http-client-utilization {email|log|trap|none}
```

If you want to configure notifications for email, ensure you have added an email recipient to the event log (`#(config event-log)mail`) and that you have configured the SMTP server settings (`#(config smtp)server`). If you want to configure notifications for trap, ensure you have set up an external SNMP trap listener to receive notifications and configured the ProxySG SNMP options (`#(config)snmp`).

More information:

- Command Line Interface Reference

Improvements to Hourly Snapshots

To assist with troubleshooting the appliance, more information on access log objects and statistics has been added to the hourly snapshot of the system.

Define a Failover Sequence for Policy

To make your forwarding policy more efficient, define a sequence of forwarding hosts and groups to use throughout your policy. When the primary forwarding host or group is unavailable, the appliance goes through the sequence of forwarding hosts and groups that you specify until it finds a host or group to successfully forward traffic. Use the following CPL to define a failover sequence that you can then reference in your forwarding policy:

```
define forward.failover_sequence(failover_sequence | no)
```

More information:

- Content Policy Language Reference

Assign a String Definition to a String Variable

In policy, you can assign the *string_name* from a string definition to a string variable by using the following CPL definition:

```
define string string_name
>line_of_text
>line_of_text
...
end

<Proxy>
  variable.custom_var_str_N(string.string_name)
```

For more flexibility, you can also create multiple `define string` blocks, which can be concatenated as a single string definition for use in `variable.custom_var_str_N()`.

More information:

- Content Policy Language Reference

Improvement to Packet Captures for VLAN Traffic

To improve visibility into how the appliance handles VLAN traffic, packet captures now include the VLAN interface that the packet came from.

Alerts for Event Log Processing Issues

When the event log cannot deliver its contents to the configured destinations (such as to the on-box disk, syslog hosts, email, and SNMP servers), the appliance sends you a notification. You also receive a notification when the event log is again able to process log messages. These alerts have a log level severity of informational. For more information on log level severity, see # (config event-log notifications).

When the event log cannot deliver its contents, you receive one of the following messages:

Delivery Method that is not Functioning as Expected	Message	Meaning
On-box disk	Event log failed	An error is preventing the event log from writing to the disk.
	Event log recovered	The event log is now able to write to the disk after the disk recovered from an error.
	Event log stopped	The event log has reached the maximum configured size and the option to stop logging when that size is reached has been triggered.

Delivery Method that is not Functioning as Expected	Message	Meaning
	Event log resumed	The event log has resumed writing to the disk.
Syslog	Event log to syslog [<*ip_address*> <*port*>] failed	An error is preventing the event log from writing to the syslog server, where: • <*ip_address*> is the IP address of the failing syslog server • <*port*> is the port number of the failing syslog server that receives the event log messages
	Event log to syslog [<*ip_address*> <*port*>] recovered	The event log is now able to write to the syslog server after the server recovered from an error, where: • <*ip_address*> is the IP address of the recovered syslog server • <*port*> is the port number of the recovered syslog server that receives the event log messages
Email	Event log to mail failed	An error is preventing the event log from sending notifications to the configured email address.
	Event log to mail recovered	The event log is now able to send notifications to the configured email address.
SNMP	Event log to snmp '<*sink_protocol*>:<*address*>:<*port*>' failed	An error is preventing the event log from writing to the SNMP server, where: • <*sink_protocol*> is the protocol that the SNMP server uses • <*ip_address*> is the IP address of the failing SNMP server • <*port*> is the port number of the failing SNMP server that receives the event log messages
	Event log to snmp '<*sink_protocol*>:<*address*>:<*port*>' recovered	The event log is now able to write to the SNMP server after the server recovered from an error, where: • <*sink_protocol*> is the protocol that the SNMP server uses • <*ip_address*> is the IP address of the recovered SNMP server • <*port*> is the port number of the recovered SNMP server that receives the event log messages

To ensure you receive these alerts for event log processing issues and other notifications from the event log, configure notification defaults and overrides for the event log and ensure that the log level severity is set to either informational or verbose. If you do not want to lower the default severity for all events to these levels, you can instead create an override for just these notifications using event ID `630007` .

NOTE
If you are configuring syslog hosts to receive the event log alerts, use TCP/TLS instead of UDP. If you are configuring SNMP servers to receive the event log alerts, use SNMP INFORM instead of trap PDUs. Syslog over UDP and older SNMP traps do not allow the appliance to detect when event logs are not delivered.

Fixes in SGOS 7.3.17.1

SGOS 7.3.17.1 includes the following bug fixes:

Table 80: Authentication

ID	Issue
SG-36155	Fixes an issue that occurred when determining the username fails during policy substitution authentication, where an incorrect error message was displayed in the authentication debug log.
SG-36154	Fixes an issue where the forward proxy realm had a memory leak.

Table 81: Cache Engine

ID	Issue
SG-36947	Fixes an issue where the tracking of cache blocks in the `/CE/Allocated_Cache_blocks` statistics was incorrectly calculated.
SG-36600	Fixes an issue where the cache engine statistics for RAM Only objects was not accurate.

Table 82: Cloud Platform

ID	Issue
SG-36951	Fixes an issue where ProxySG virtual appliances that were deployed on AWS with an instance type of M5 or M6i marked the boot disks as having a critical status when they were in a healthy state.

Table 83: Health Checks

ID	Issue
SG-36412	Fixes an issue in 7.3.14 and later where performing a TLS1.3 health check on a forward proxy was failing.
SG-36664	Fixes an issue where the appliance restarted because of a dead lock situation that was caused by keeping a registry lock open longer than necessary.

Table 84: HTTP Proxy

ID	Issue
SG-36209	Fixes an issue where HTTP dwell statistics were corrupted because values exceeded the buffer size.
SG-35346	Fixes an issue where an HTTP server stream error occurred when using HTTP/2 because the connection window size did not update correctly after a stream was canceled by the client.
SG-36756	Fixes an issue where the appliance restarted due to the appliance incorrectly copying the pointer of the header for the ICAP REQMOD replacement response.
SG-35659	Fixes an issue where HTTP/2 protocol errors appeared because the translation layer between HTTP/2 and HTTP 1.1 did not correctly process trailer headers.

ID	Issue
SG-36829	Fixes an issue where the client received a fatal ICAP decode error because the server returned more than one trailer section after the data.

Table 85: IPv6 Stack and IPv6 Proxies

ID	Issue
SG-35530	Fixes an issue where corrupted IPv6 packets caused HTTP performance issues.

Table 86: Java Management Console and Java VPM

ID	Issue
SG-36779	Fixes an issue where the Java Management Console and Java VPM reported security errors when you accessed the Management Console and VPM. These errors occurred because the certificate chain was updated in June 2023 and the chain referenced a root CA that was not yet included by default in the Java trust store. Releases that occurred after October 2, 2023 are now signed by a certificate chain that has a root certificate that is in the Java trust store.

SG-36965	Fixes an issue where the Java Management Console, Launcher, and Java VPM did not launch with Java 1.8u351 or later because the signature of the signed SGOS Java code did not have an SHA-256 timestamp digest in the timestamp signature. Releases before October 2, 2023 had a signature with an SHA-1 timestamp digest.
	To avoid the following errors, use the ProxySG Admin Console for accessing the ProxySG appliance.
	If you are using the loader.jnlp, you may see one of the following messages:
	• **Security Warning: "Block potentially unsafe components from being run?":** To proceed, either click Don't Block, use the mc.jnlp file, upgrade Java to 1.8u351 or later, or upgrade SGOS to a release after October 2, 2023.
	• **Error Message "Application Blocked by Java Security":** To proceed, click OK and the loader opens or use the mc.jnlp file.
	• **Application Error "Unable to launch the application":** To proceed, either upgrade SGOS to a release after October 2, 2023 or remove the SHA-1 clause from the java.security file. To remove the SHA-1 clause:
	a. Navigate to the location of java.security file (for example, [JAVA_HOME]/jre/lib/security/java.security).
	b. Locate the text:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`DSA keySize < 1024, include jdk.disabled.namedCurves, \`
	`SHA1 denyAfter 2019-01-01`
	c. Replace the text with:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`DSA keySize < 1024, include jdk.disabled.namedCurves`

Table 87: Kernel

ID	Issue
SG-36892	Fixes an issue in 7.3.15 and later where a memory leak can occur when the connection is closed while trying to send data. The appliance may run out of memory over time and cause a restart.
SG-34810	Fixes an issue where the appliance restarted because the same process was scheduled on multiple processors at the same time.

Table 88: Network Drivers

ID	Issue
SG-36304	Fixes an issue where auto-created VLAN interfaces could accidentally send and receive ARP requests, potentially causing traffic to be routed on the wrong interface.

Table 89: Policy

ID	Issue
SG-36542	Fixes an issue where the appliance experienced slowness due to a memory bottleneck during a health check process.
SG-36785	Fixes an issue where the policy to bypass scanning for HTML files was causing the proxy to not scan cached files that were replaced by an ICAP HTML exception page. This caused issues when the proxy was also directed to refresh the cached object from the server.
SG-36920	Fixes an issue in 7.3.14 and later where a policy trace was not produced after a SOCKS authentication failure.

Table 90: SNMP

ID	Issue
SG-35928	Fixes an issue where the Zabbix SNMP server interface displayed fluctuating statuses for ProxySG applications. This issue occurred after physical ProxySG devices were migrated to SG-VAs, which shared one enterprise license serial number under ISG. This fix updates the SNMPv3 default engine ID to be based on the unique appliance identifier instead of the shared serial number.
SG-36185	Fixes an issue in the DNS checks portion of a health check, where the DNS check was still performed (and a notification was sent if there was failure) when the Health Check was disabled and the default SNMP notifications were set to on.

Table 91: SSL Proxy

ID	Issue
SG-36661	Fixes an issue where the appliance restarted during a change of TLS versions due to an inconsistent forward proxy session cache state.
SG-36029	Fixes an issue in transparent deployments where trust-destination-ip was not properly honored by SSL Proxy when disabled.

Table 92: SSL/TLS and PKI

ID	Issue
SG-35140	Fixes an issue where changing the SSL device profile to TLSv1.3 without first configuring the suitable ciphers did not update the protocol.

Table 93: TCP/IP and General Networking

ID	Issue
SG-36895	Fixes two vulnerabilities in the FreeBSD network stack code that is used by the appliance. These vulnerabilities are not exploitable on any version of SGOS because the SGOS firewall rules do not use TCP options.
SG-36503	Fixes an issue where enabling the `#(config)tcp-ip tcp-fast-finwait2-recycle` setting to increase the usable TCP port range was not correctly cleaning up the TCP connections.
SG-36728	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance caused packets to show up out of order. This issue occurred when TCP packets had options or were fragmented.
SG-36278	Fixes an issue where the appliance restarted due to faulty ICMP error handling on a TCP connection.
SG-35318	Fixes an issue where the traffic on an auto-created VLAN was blocked after the security parameter of the interface (allow-intercept, reject-inbound, address-selection) was changed.
SG-36897	Fixes a vulnerability where 1 byte of system memory could be disclosed in a specific IPv6 TCP handshake packet
SG-36809	Fixes a vulnerability that is related to ICMPv6 packet processing. An attacker could potentially exploit this vulnerability to cause the appliance to restart.

Table 94: Utility Library

ID	Issue
SG-34993	Updates the PCRE Library to resolve multiple vulnerabilities.

SGOS 7.3.16.4 PR

Release Information

- Release Date: April 24, 2024
- Build Number: 295504

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.16.4

- See Fixes in SGOS 7.3.16.4.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.16.4

SGOS 7.3.16.4 includes the following bug fixes:

Table 95: Access Logging

ID	Issue
SG-37446	Fixes an issue where TCP connections from the appliance might have stalled, resulting in almost no data being transmitted. This issue only occurred for TCP connections that experienced significant packet loss in the network and that used the default New Reno congestion control algorithm. When in a stalled state, the appliance sends 1 byte of application data every 5 seconds. This issue was extremely rare and was detected for long-running connections, such as uploading access logs in continuous mode.

Table 96: HTTP Proxy

ID	Issue
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

Table 97: Kernel

ID	Issue
SG-38025	Fixes an issue where a tuning parameter for protecting storage that was introduced in version 7.3.15.1 was causing traffic to be rejected in some bursty connection workloads. The tuning parameter is now disabled by default.

Table 98: TCP/IP and General Networking

ID	Issue
SG-36728	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance caused packets to show up out of order. This issue occurred when TCP packets had options or were fragmented.
SG-38159	Fixes an issue in versions 7.3.15.1 to 7.3.18.1 using SOCKs and tunneling UDP traffic, where the appliance stopped processing traffic (GUI, proxy data, and so on) due to a lock order race condition.

SGOS 7.3.16.3 PR

Release Information

- Release Date: February 1, 2024
- Build Number: 293248

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.16.3

- See Fixes in SGOS 7.3.16.3.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.16.3

SGOS 7.3.16.3 includes the following bug fixes:

Table 99: Kernel

ID	Issue
SG-36892	Fixes an issue in 7.3.15 and later where a memory leak can occur when the connection is closed while trying to send data. The appliance may run out of memory over time and cause a restart.
SG-37772	Fixes an issue where TCP connections that were closed (either normally or by RST) while the Edge SWG appliance was sending data caused a memory leak. These connections are mostly handled by the proxy code for TCP Tunnel but they can be handled by other proxy codes, such as HTTPS.

Table 100: TCP/IP and General Networking

ID	Issue
SG-37293	Fixes an issue where the netflow timer that cleans up old connections stopped working after 49 days. This issue caused a memory leak in the appliance.
SG-37837	Fixes an issue in the Edge SWG network stack that occurred when the Edge SWG instance was deployed on SSP hardware or other virtual appliance platform. After 49 days, the Edge SWG appliance leaked connections that were in the 'last ACK wait' state. This leak prevented new TCP connections from being created.

SGOS 7.3.16.2 PR

Release Information

- Release Date: October 23, 2023
- Build Number: 290895

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8-sha256
  – tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  – Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.16.2

- See Fixes in SGOS 7.3.16.2.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.16.2

Table 101: Cloud Platform

ID	Issue
SG-36951	Fixes an issue where ProxySG virtual appliances that were deployed on AWS with an instance type of M5 or M6i marked the boot disks as having a critical status when they were in a healthy state.

Table 102: Java Management Console and Java VPM

ID	Issue
SG-36779	Fixes an issue where the Java Management Console and Java VPM reported security errors when you accessed the Management Console and VPM. These errors occurred because the certificate chain was updated in June 2023 and the chain referenced a root CA that was not yet included by default in the Java trust store. Releases that occurred after October 2, 2023 are now signed by a certificate chain that has a root certificate that is in the Java trust store.

SG-36965	Fixes an issue where the Java Management Console, Launcher, and Java VPM did not launch with Java 1.8u351 or later because the signature of the signed SGOS Java code did not have an SHA-256 timestamp digest in the timestamp signature. Releases prior to October 2, 2023 had a signature with an SHA-1 timestamp digest.
	To avoid the following errors, use the ProxySG Admin Console for accessing the ProxySG appliance.
	If you are using the loader.jnlp, you may see one of the following messages:
	• **Security Warning: "Block potentially unsafe components from being run?":** To proceed, either click Don't Block, use the mc.jnlp file, upgrade Java to 1.8u351 or later, or upgrade SGOS to a release after October 2, 2023.
	• **Error Message "Application Blocked by Java Security":** To proceed, click OK and the loader opens or use the mc.jnlp file.
	• **Application Error "Unable to launch the application":** To proceed, either upgrade SGOS to a release after October 2, 2023 or remove the SHA-1 clause from the java.security file. To remove the SHA-1 clause:
	a. Navigate to the location of java.security file (for example, [JAVA_HOME]/jre/lib/security/java.security).
	b. Locate the text:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves, \`
	`      SHA1 denyAfter 2019-01-01`
	c. Replace the text with:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves`

SGOS 7.3.16.1 GA

Release Information

- Release Date: September 25, 2023
- Build Number: 289804

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.16.1

- See Features in SGOS 7.3.16.1.

Fixes in ProxySG 7.3.16.1

- See Fixes in SGOS 7.3.16.1.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.16.1

ProxySG Admin Console 2.1.4

This release includes the ProxySG Admin Console (SGAC), which is a next-generation web interface.
The SGAC 2.1.4 release includes the contents of SGAC 2.1.3. The SGAC is the default interface that opens in the browser. The Java-based Management Console will be removed in a future release. To learn more about the SGAC, refer to the following KB article:

https://knowledge.broadcom.com/external/article/251426

- KB 251426: https://knowledge.broadcom.com/external/article/251426
- ProxySG Admin Console documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started.html
- SGAC Releases in SGOS

Web Visual Policy Manager 2.1.6

This release includes the Web Visual Policy Manager (Web VPM) 2.1.6 with the following enhancements:

- You can now search all levels of nested objects.
- Installing policy that includes the Set Effective Client IP object no longer triggers a deprecation warning.

For information on the Web VPM release, refer to the following documentation:

- Release announcement:
- Web VPM documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager.html
- Web VPM 2.1.6

Event Log Notifications for SNMP

You can now configure event log notifications for SNMP transactions by using the following command:

```
#(config event-log notifications) enable snmp [event-id]
```

To configure the default settings for SNMP notifications, use the following command:

```
#(config event-log notifications) default snmp level severe|configuration|policy|trace|informational|verbose
```

SNMP notifications are disabled by default. When you enable them, the default level is `severe` .

The new private MIB file BLUECOAT-SG-EVENTLOG-MIB includes an SNMP trap that is triggered when event log messages matching the configured criteria are generated. The existing private MIB file BLUECOAT-SG- DISK-MIB has been updated to include a new value (failed(11)) for the deviceDiskStatus variable.

IMPORTANT

Do not enable SNMP notifications for all event logs. Large numbers of notifications can cause slower performance of the appliance and make locating specific notifications difficult. To avoid receiving a large number of notifications, enable notifications for only a few event log IDs.

If you must enable notifications for all event logs, disable notifications for logs that have the event ID 430000. The event log ID 430000 indicates that the appliance cannot send an SNMP trap to the destination due to a network error. The following example is an error message with the 430000 ID:

```
SNMP error [priority 3]: snmpd: send_trap: Failure in sendto (Network is unreachable) "  0 430000:64
 sgos_logging.cpp:145
```

If you do not disable notifications for the ID 430000 when notifications are enabled for all other event logs, the appliance might enter an error cycle. In this error cycle, the appliance would attempt to send an event log trap to a destination that is unreachable. The appliance would then receive the event log notification, causing the appliance to send another event log trap to the unreachable destination, and so on.

More information:

- Command Line Interface Reference
- Private MIBs

New M5 Instance Types for ProxySG VAs on AWS

With the release of 7.3.16.1, ProxySG VAs on AWS Marketplace can now run on M5 and M6i instance types. These next-generation instance types bring with them significant increases in networking and storage performance. These instance types further enhance the ability of AWS to support ProxySG customers by granting access to a native serial console, and by increasing the regions and availability zones where the VAs can be deployed. For more information, see the AWS documentation on M5 and M6i instance types.

For ProxySG VAs, the following new models are available for AWS Marketplace deployments:

AWS Instance Type	Allowed Number of CPUs	EC2 CPU Options**	Virtual Memory (GiB)	Connection Count	Number of Virtual Disks	Storage Space Per Disk (GiB)
m5.large	2	default values	8	10000	2	100
m5.xlarge	4	default values	16	20000	2	100
m5.2xlarge	8	default values	32	50000	4	100
m5.4xlarge	16	default values	64	100000	8	100
m5.8xlarge	32	default values	128	200,000	8	100
m6i.large	2	default values	8	10000	2	100
m6i.xlarge	4	default values	16	20000	2	100
m6i.2xlarge	8	default values	32	50000	4	100
m6i.4xlarge	16	default values	64	100000	8	100
m6i.8xlarge	32	default values	128	200000	8	100

Password Lockout Changes

Previously, you could only lock out local users if they reached the maximum number of attempts to log in. Now, you can lock out the console user when they reach the maximum number of failed attempts to log in. You must use the default local user list (`local_user_database`) to lock out the console user. To set the number of attempts users can make to log in before they are locked out, use the following CLI command:

```
# (config local-user-list local_user_database) max-failed-attempts
 attempts
```

The CLI command `# (config local-user-list local_user_list)` **`password-grace`** *`number_of_days`* has changed to `# (config local-user-list local_user_list)` **`expiration-lockout`** *`number_of_days`* .

More information:

- Command Line Interface Reference

Support for Additional Format in Syslog

Previously, the ProxySG appliance sent syslog messages in RFC3164 format. In this release, support for the RFC5424 format has been added. This format includes the more detailed RFC3339 timestamp, as well as additional fields before the message (appname, procID, msgID, structureddata).

A new configuration command is available under the event-log command to allow you to select the syslog format:

```
#(config event-log) syslog format { rfc3164 | rfc5424 }
```

- The setting for the syslog format is visible in `> show event-log [configuration]` and `# show configuration`.
- The default setting is `rfc3164`.
- The event-log syslog format only affects the format sent using the syslog protocol. It does not affect the format or timestamp of event logs viewed by any other means.

More information:

- Command Line Interface Reference

Access Log Errors for Kafka Logged in the Event Log

To make debugging Kafka-related issues easier, the appliance now reports Kafka send errors in the event log.

CPU Usage Improvements

> **IMPORTANT**
> These improvements will increase the amount of memory that the appliance uses by as much as 3 GB. Ensure you monitor memory usage before and after you upgrade.

To reduce high and prolonged CPU usage, improvements have been made to the processing performance of the appliance and memory allotments have been increased for the Blue Coat content filtering databases for the following ProxySG models:

Table 103: All SG-S500 Models

Previous Normal/High Memory Allotment	New Increased Normal/High Memory Allotment
350 MB/800 MB	3 GB/6 GB

Table 104: High-Performance Virtual Appliance Models (Product Codes 59, 68, 70, and 99)

Total Virtual Appliance Memory	Previous Normal/High Memory Allotment	New Increased Normal/ High Memory Allotment
< 8 GB	800 MB/1.7 GB	350 MB/800 MB
< 16 GB	350 MB/800 MB	800 MB/1.7 GB
< 64 GB	350 MB/800 MB	1.7 GB/3 GB
>= 64 GB	350 MB/800 MB	3 GB/6 GB

OCSP Errors Now Contain Hostname Information

To make troubleshooting easier, error messages for OCSP transactions in the event log now contain information on the hostname of the OCSP responder.

Terminate ICAP Active Sessions

You can now terminate active sessions for ICAP connections by using the following CLI command:

```
# active-
sessions
  <session_type>
  terminate
  <filter>
```

where `<filter>` is:

- **`icap-method=`**{**`REQMOD`**|**`RESPMOD`**|**`any`**} : Notification method, such as request modification or response modification
- **`icap-service=`** : Unique name for the ICAP service
- **`icap-status=`**{**`completed`**|**`deferred`**|**`scanning`**|**`transferring`**|**`any`**} : Responses according to status

More information:

- Command Line Interface Reference

Timing Added to Policy Traces

To provide more information on why access logging might be slow, the policy trace now includes the timing for access log transactions. The new entry in the policy trace for the access log timing is `access-logging: precompute_fields:` *`number`* `ms, logging:` *`number`* `ms`.

Deprecation Notice for IM Policy Values

For the following CPL gestures, the IM-related values `aol-im`, `msn-im`, and `yahoo-im` are deprecated:

- `client.protocol=`
- `socks.accelerate()`
- `socks.accelerated=`

Additionally, the IM Proxy-related values `aol-im.proxy`, `msn-im.proxy`, and `yahoo-im.proxy` for the `transaction.type=` condition are deprecated.

In 7.3.x, policy that contains these values compiles with a warning message. To avoid policy errors when you upgrade to 7.4.x, ensure that you remove these values from your policy.

Fixes in SGOS 7.3.16.1

SGOS 7.3.16.1 includes the following bug fixes:

Table 105: Access Logging

ID	Issue
SG-35915	Fixes an issue where the appliance stopped responding due to an internal message corruption while under high traffic volume.
SG-35929	Fixes an issue where using CPL to exclude the Authentication log from the ProxySG main access log was not working. The CPL is described in KB165943.
SG-36203	Fixes an issue where the event log showed a timing issue with the routing table when the appliance initially started up.

Table 106: Authentication

ID	Issue
SG-34728	Fixes an issue where ProxySG was making remote procedure calls (RPC) through Netlogon using the weaker cipher RC4 by default instead of AES.
SG-35972	Fixes an issue where the appliance stopped responding due to the krb5_keytab not being in the memory list.
SG-35976	Fixes an issue where DNS lookup requests did not contain the protocol to use, which caused delays for Kerberos connections.
SG-36115	Fixes a potential memory leak when using multi-tenant policy.
SG-36183	Fixes an issue where, after configuring Common Access Card (CAC) authentication with the appliance using a personal certificate, the appliance prompted the user for a password.

Table 107: Boot

ID	Issue
SG-35738	Fixes an issue where the ProxySG VA could not boot when deployed on Hyper-V using AMD CPUs.

Table 108: Cache Engine

ID	Issue
SG-35969	Fixes an issue where the appliance stopped responding due to the cache handlers incorrectly nulling the disk.

Table 109: Diagnostic Tools

ID	Issue
SG-35816	Fixes an issue where the appliance did not recreate deleted log files for diagnostic traces that were still installed in policy due to the max probe limit being reached.

Table 110: Event Logging

ID	Issue
SG-30654	Fixes an issue where the appliance stopped responding due to a race condition where the next_index increased before the appliance could push the new message to the queue.

Table 111: Health Checks

ID	Issue
SG-36251	Fixes an issue where the expanded configuration did not show the forwarding group information when the health check for the group was set to Disabled: Healthy.

Table 112: HTTP Proxy

ID	Issue
SG-33544	Fixes an issue where the appliance stopped responding when multiple transactions in the same HTTP/2 connection were performing RDNS lookup in parallel.
SG-35778	Fixes an issue where the server.connection.parallel_connect() property closed and reconnected upstream connections for each request, which caused the appliance to make multiple unnecessary connections.
SG-35903	Fixes an issue where the appliance assumed that the addresses populated by getsockname() for HTTP transactions would always be IPv4 addresses, which caused the appliance to not properly set upstream server connections for spoofed addresses.

Table 113: Kernel

ID	Issue
SG-36025	Fixes an issue where the kernel sometimes restarted the appliance due to lock timeouts.

Table 114: Policy

ID	Issue
SG-36257	Fixes an issue where the appliance reported an incorrect number of warnings when installing an exceptions list.

Table 115: SSL Proxy

ID	Issue
SG-36175	Fixes an issue where the CLI Help for syslog format contained a typo in the RFC number.
SG-36275	Fixes an issue where the appliance stopped responding due to the appliance incorrectly reading the bytes in the client hello from the server.
SG-36468	Adds extra debug logging for the certificate forge operation.

Table 116: Storage

ID	Issue
SG-35172	Fixes an issue where downloading an upgrade image failed because the disk space was consumed by a log file that wasn't rotated.

Table 117: TCP/IP and General Networking

ID	Issue
SG-36049	Fixes an issue where the appliance added dynamic routes for IP addresses that were assigned to static routes to the routing table, even though `#(config) tcp-ip icmp-drop-redirect` was enabled.
SG-36120	Fixes an issue where you could only access the appliance by the console due to the monitoring statistic for the drive temperature.
SG-36135	Fixes an issue where the appliance incorrectly sent a TCP RST for a new connection.

SGOS 7.3.15.5 PR

Release Information

- Release Date: April 24, 2024
- Build Number: 295496

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.15.5

- See Fixes in SGOS 7.3.15.5.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.15.5

SGOS 7.3.15.5 includes the following bug fixes:

Table 118: Access Logging

ID	Issue
SG-37446	Fixes an issue where TCP connections from the appliance might have stalled, resulting in almost no data being transmitted. This issue only occurred for TCP connections that experienced significant packet loss in the network and that used the default New Reno congestion control algorithm. When in a stalled state, the appliance sends 1 byte of application data every 5 seconds. This issue was extremely rare and was detected for long-running connections, such as uploading access logs in continuous mode.

Table 119: HTTP Proxy

ID	Issue
SG-38510	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance dropped some consecutive TCP ACK packets. This issue was more likely to occur when the consecutive ACK packets that the appliance received contained no data.

Table 120: Kernel

ID	Issue
SG-38025	Fixes an issue where a tuning parameter for protecting storage that was introduced in version 7.3.15.1 was causing traffic to be rejected in some bursty connection workloads. The tuning parameter is now disabled by default.

Table 121: TCP/IP and General Networking

ID	Issue
SG-36728	Fixes an issue where the throughput of the appliance was slower than expected because the Large Receive Offload (LRO) of the appliance caused packets to show up out of order. This issue occurred when TCP packets had options or were fragmented.
SG-38159	Fixes an issue in versions 7.3.15.1 to 7.3.18.1 using SOCKs and tunneling UDP traffic, where the appliance stopped processing traffic (GUI, proxy data, and so on) due to a lock order race condition.

SGOS 7.3.15.4 PR

Release Information

- Release Date: January 29, 2024
- Build Number: 293243

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.15.4

- See Fixes in SGOS 7.3.15.4.
- To see any Security Advisories that apply to the version you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.15.4

SGOS 7.3.15.4 includes the following bug fixes:

Table 122: Kernel

ID	Issue
SG-36892	Fixes an issue in 7.3.15 and later where a memory leak can occur when the connection is closed while trying to send data. The appliance may run out of memory over time and cause a restart.
SG-37772	Fixes an issue where TCP connections that were closed (either normally or by RST) while the Edge SWG appliance was sending data caused a memory leak. These connections are mostly handled by the proxy code for TCP Tunnel but they can be handled by other proxy codes, such as HTTPS.

Table 123: TCP/IP and General Networking

ID	Issue
SG-37293	Fixes an issue where the netflow timer that cleans up old connections stopped working after 49 days. This issue caused a memory leak in the appliance.
SG-37837	Fixes an issue in the Edge SWG network stack that occurred when the Edge SWG instance was deployed on SSP hardware or other virtual appliance platform. After 49 days, the Edge SWG appliance leaked connections that were in the 'last ACK wait' state. This leak prevented new TCP connections from being created.

SGOS 7.3.15.3 PR

Release Information

- Release Date: October 23, 2023
- Build Number: 290894

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.15.3

- See Fixes in SGOS 7.3.15.3.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.15.3

SGOS 7.3.15.3 includes the following bug fixes:

Table 124: Java Management Console and Java VPM

ID	Issue
SG-36779	Fixes an issue where the Java Management Console and Java VPM reported security errors when you accessed the Management Console and VPM. These errors occurred because the certificate chain was updated in June 2023 and the chain referenced a root CA that was not yet included by default in the Java trust store. Releases that occurred after October 2, 2023 are now signed by a certificate chain that has a root certificate that is in the Java trust store.

SG-36965	Fixes an issue where the Java Management Console, Launcher, and Java VPM did not launch with Java 1.8u351 or later because the signature of the signed SGOS Java code did not have an SHA-256 timestamp digest in the timestamp signature. Releases prior to October 2, 2023 had a signature with an SHA-1 timestamp digest.
	To avoid the following errors, use the ProxySG Admin Console for accessing the ProxySG appliance.
	If you are using the loader.jnlp, you may see one of the following messages:
	• **Security Warning: "Block potentially unsafe components from being run?":** To proceed, either click Don't Block, use the mc.jnlp file, upgrade Java to 1.8u351 or later, or upgrade SGOS to a release after October 2, 2023.
	• **Error Message "Application Blocked by Java Security":** To proceed, click OK and the loader opens or use the mc.jnlp file.
	• **Application Error "Unable to launch the application":** To proceed, either upgrade SGOS to a release after October 2, 2023 or remove the SHA-1 clause from the java.security file. To remove the SHA-1 clause:
	a. Navigate to the location of java.security file (for example, [JAVA_HOME]/jre/lib/security/java.security).
	b. Locate the text:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves, \`
	`      SHA1 denyAfter 2019-01-01`
	c. Replace the text with:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves`

SGOS 7.3.15.2 PR

Release Information

- Release Date: August 25, 2023
- Build Number: 289172

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.15.2

- See Fixes in SGOS 7.3.15.2.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.15.2

SGOS 7.3.15.2 includes the following bug fixes:

Table 125: Authentication

ID	Issue
SG-36279	Fixes an issue where the appliance stopped responding when clients simultaneously authenticated to various tenants in multi-tenant policy.

Table 126: SSL Proxy

ID	Issue
SG-36275	Fixes an issue where the appliance stopped responding due to the appliance incorrectly reading the bytes in the client hello from the server.

SGOS 7.3.15.1 GA

Release Information

- Release Date: July 17, 2023
- Build Number: 287547

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.15.1

- See Features in SGOS 7.3.15.1.

Fixes in ProxySG 7.3.15.1

- See Fixes in SGOS 7.3.15.1.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.15.1

ProxySG Admin Console 2.1.4

This release includes the ProxySG Admin Console (SGAC), which is a next-generation web interface.
The SGAC 2.1.4 release includes the contents of SGAC 2.1.3. The SGAC is the default interface that opens in the browser. The Java-based Management Console will be removed in a future release. To learn more about the SGAC, refer to the following KB article:

https://knowledge.broadcom.com/external/article/251426

- Changes: Fixes in SGOS 7.3.15.1
- KB 251426: https://knowledge.broadcom.com/external/article/251426
- ProxySG Admin Console documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started.html
- SGAC Releases in SGOS

Web Visual Policy Manager 2.1.6

This release includes the Web Visual Policy Manager (Web VPM) 2.1.6 with the following enhancements:

- You can now search all levels of nested objects.
- Installing policy that includes the Set Effective Client IP object no longer triggers a deprecation warning.

For information on the Web VPM release, refer to the following documentation:

- Release announcement:
- Web VPM documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager.html
- Web VPM 2.1.6

Password Policy

New password policy options are available to ensure your local passwords on the ProxySG appliance are secure and strong. Enforce password requirements, such as:

- Minimum length
- Characters that must be used
- Whether common words or whitespaces are allowed
- Whether the password or parts of the password were used too recently

Configure password policy by using the following CLI command:

```
#(config) security password-policy
```

You can view password policy that is configured on the appliance by using the `# show security password-policy` command.

More information:

- Command Line Interface Reference

Password Grace Period

To better control user access and enforce password refreshes, you can now specify a grace period for password expiration. When you specify a grace period, users with expired passwords can log in to change their passwords for the number of days that you specify. After the grace period ends, they are locked out of their accounts. Read-only local users are able to change their passwords using the `password` command in disable mode. The `password` command is also available in enable mode and configure mode.

To set a grace period, use the following CLI command:

```
#(config local-user-list local_user_list) password-grace number_of_days
```

You can view the grace period for users by using the `# show security local-user-list` command. This command has also been updated to show more information on the account lockout details and to show the date that the password was last changed for the user.

More information:

- Command Line Interface Reference

Health Checks Now Use SSL Device Profile

Previously, when you configured your health checks for encrypted traffic, you used an SSL client profile. To offer more flexibility and security, now you specify an SSL device profile for creating new or editing existing health checks for HTTPS or SSL traffic. To set an SSL device profile for your health check, use the following CLI command:

```
#(config health-check) create https health_check URL ssl-device-profile-name
```

More information:

- Command Line Interface Reference

SMTP Enhancements

You can now authenticate with the SMTP server and use TLS for email notifications from the event log. The appliance uses TLS when you specify an SSL device profile in your SMTP settings. To specify an SSL device profile, use the following CLI command:

```
# (config smtp) ssl-device-profile ssl_device_profile_name
```

You can also configure a username and password for your SMTP server configuration by using the following CLI commands:

- `# (config smtp) username username`
- `# (config smtp) password [password]`
- `# (config smtp) encrypted-password encrypted_password`

To test your SMTP configuration, use the CLI command:

```
> test smtp
```

More information:

- Command Line Interface Reference

Set a Hostname for the Syslog

You can now set a hostname for the syslog by using the following CLI command:

```
#(config event-log) syslog hostname hostname
```

More information:

- Command Line Interface Reference

New Policy Condition ticket.reevaluation.count=

A new CPL condition has been introduced to help the appliance evaluate long-running transactions that do not require re-authentication. Use `ticket.reevaluation.count=` to allow the appliance to perform actions that are based on how many times the appliance has re-evaluated a ticket. When this condition is triggered, the appliance re-evaluates any policy changes that it might deny later in the connection.

More information:

- Content Policy Language Reference

Policy Trace Enhancements

The following enhancements for the policy trace have been made:

- The policy trace now displays MATCH ALLOW.request for users who authenticated to the Legacy Java Management Console. Previously, the trace labeled the transaction as late.
- For traces running at the level `all` , debugging enhancements have been made to include more session information for administrator transactions.
- The policy trace more accurately reports the handoff of denied TCP transactions.
- The policy trace now reports the number of bytes sent to the client and received by the server in the following format (the number of bytes provided are examples):

```
bytes received from client: 111
bytes sent to server : 133
bytes received from server: 657
bytes sent to client : 657
```

Access Log Messages Now Contain Facility Names

To make debugging a component of the access log easier, the entries for the debug log now contain their respective facility names.

Reverse Proxy Session Cache Enhancements

To help prevent latency issues that might affect the performance of applications behind reverse proxies, enhancements have been made to the session cache of the reverse proxy. These enhancements increase the size of the session cache and the speed at which the session cache can serve the applications that sit behind the reverse proxy.

HTTP/2 Server Connection Cache Enhancements

To improve the speed at which the appliance can serve HTTP/2 requests, enhancements have been made to the HTTP/2 Server Connection Cache. These enhancements include:

- Improvements to how the appliance responds when a server is unresponsive, reducing the number of connection attempts in the backlog.
- Troubleshooting improvements and statistics to help identify when streams are closed due to errors.

Dynamic License Updates from Integrated Secure Gateway (ISG)

For ProxySG applications running on the SSP platform, license changes that originate from the ISG host are now automatically updated in the ProxySG license file without requiring a restart.

Trust Package Update

The trust package is updated automatically as part of the upgrade process. Obsolete CAs have been removed.

If you are not upgrading, to download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

More information:

- Command Line Interface Reference

JAR File Update for the Java Management Console

The certificate used to sign the Management Console loader.jar has been updated. If you downloaded the Management Console loader.jar from the KB articles previously, refer to the appropriate article for the latest version of the JAR file and how to install the certificates for it:

- Launch SGOS management consoles using the Management Console Launcher https://knowledge.broadcom.com/external/article?articleId=169194
- Management Console Launcher for systems without Internet connectivity https://knowledge.broadcom.com/external/article?articleId=169208
- Support for Java 11 on ProxySG and Advanced Secure Gateway appliance https://knowledge.broadcom.com/external/article?articleId=173228
- Download and Install the New Root and Intermediate Certificates for the Java Management Console Launcher: https://knowledge.broadcom.com/external/article/270160

New preserve Option for http2.client.accept()

To prevent incompatibility issues that might occur when the appliance translates from HTTP/2 to HTTP/1.1 for websites that do not support HTTP/2, the `preserve` option has been added to the `http2.client.accept()` property. When you specify `http2.client.accept(preserve)` in policy, the appliance automatically upgrades client connections to HTTP/2 for origin content servers that support HTTP/2. When the server does not support HTTP/2, the appliance does not upgrade the client connection. The default value for `http2.client.accept()` is `preserve` . In previous releases, the default value was `yes` . This change of the default value ensures the HTTP versions for both the client and server are the same.

More information:

- Content Policy Language Reference

New transaction_type Option for Diagnostics Probe

To reduce the number of transactions in a diagnostics probe or to only display relevant transactions for your troubleshooting purposes, you can now specify what types of transactions the probe includes. To specify which transactions you want to include in the probe, use the `transaction_type=` option in the `define probe` definition.

More information:

- Content Policy Language Reference

Fixes in SGOS 7.3.15.1

SGOS 7.3.15.1 includes the following bug fixes:

Table 127: Active Sessions

ID	Issue
SG-35265	Fixes an HTTP/2 Rapid Reset DDoS vulnerability. For more information, see https://knowledge.broadcom.com/external/article/274893 and Security Advisory 22674.

Table 128: Authentication

ID	Issue
SG-35658	Fixes an issue where HTTPS transactions with IWA authentication timed out. This issue occurred several days after a reboot.
SG-35092	Fixes an issue where the appliance incorrectly authenticated users with basic credentials even though policy did not allow basic credentials for IWA direct and IWA BCAAA realms.

Table 129: CLI Consoles

ID	Issue
SG-35735	Fixed an issue where the appliance had a restart in a management worker process.

Table 130: Event Logging

ID	Issue
SG-35324	Fixes an issue where the event log recorded multiple "Warning: Unrecognized OPP PDM sample name" messages.
SG-35264	Fixes an issue where policy compilation errors were not recorded in the event log.

Table 131: FTP Proxy

ID	Issue
SG-34751	Fixes an issue where FTP upload speeds were low and packet loss occurred. This issue occurred with uploads to an Akamai FTP server.

Table 132: HTTP Proxy

ID	Issue
SG-33612	Fixes an issue where the appliance stopped responding after it had a sudden increase in traffic volume.
SG-34521	Fixes an issue where downloads failed with a 503 error. This issue occurred when the server response contained an invalid TE header field over HTTP/2.
SG-35351	Fixes an issue where the file uploads to a cloud-based server were slow in version 7.3.13.1. This issue occurred due to a limitation related to the ProxySG appliance uptime.
SG-34740	Fixes an issue where users could not connect to the Internet because they received a cached Proxy Auto-Config (PAC) file. This issue occurred because the reverse proxy did not refresh PAC files when policy included `never_serve_after_expiry(no)` .
SG-34821	Fixes an issue where, if a cached object rescan changed the Apparent Data Type (ADT) returned by the ICAP response, the ADT values were not updated correctly.
SG-34999	Fixes an issue where the appliance did not report user-defined exceptions in the /exceptions_config.html advanced URL.

Table 133: Management

ID	Issue
SG-35313	Fixes an issue where multiple appliances stopped responding. This issue occurred when a `show config` command was issued while the appliance was installing a trust package.

Table 134: Performance

ID	Issue
SG-34724	Fixes an issue on C20S ISG Proxy where Google Meet audio and video were not in sync due to bottlenecks.

Table 135: Policy

ID	Issue
SG-34864	Fixes an issue where the appliance rebooted when proxying SOCKS traffic.
SG-34553	Fixes an issue where the policy trace count at the /Policy/Diagnostics Advanced URL did not increment when the `define probe` definition contained `policy_trace=yes`.

Table 136: Proxy Forwarding

ID	Issue
SG-34578	Fixes an issue where the `host-affinity http accelerator-cookie` setting was reset to the `default` setting after an upgrade. A custom host affinity setting is now preserved after an upgrade.

Table 137: SSL Proxy

ID	Issue
SG-34300	Fixes an issue where the appliance rebooted with a 0xE (Page_Fault) in PG_SSL_HNDSHK, Process: "HTTP SW".
SG-34920	Fixes an issue where users received an expired certificate warning repeatedly after they clicked the "unsafe" link to proceed to the requested webpage.
SG-34638	Fixes an issue where the appliance did not preserve the previous TLS selections for SSL clients and SSL device profiles after an upgrade. After an upgrade, TLS 1.3 should be enabled in addition to supported pre-upgrade selections.
SG-31919	Fixes an issue where the appliance stopped responding when FTPS interception was enabled.

Table 138: SSL/TLS and PKI

ID	Issue
SG-35333	Fixes an issue where the CLI command `#show security trust-package` displayed an incorrect number for the number of CAs that were removed from the CCL.
SG-35698	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.
SG-35774	Fixes an issue where the HSM health check state was not "Unhealthy" when an HSM signing operation failed. This issue occurred for single HSM keyrings that were not part of a keylist.

Table 139: TCP/IP and General Networking

ID	Issue
SG-34796	Fixes an issue where the appliance stopped responding after an upgrade to version 7.3.12.1.
SG-35138	Fixes an issue where the Edge SWG application that manages bandwidth used a large percentage (up to 100%) of the CPU and it stopped responding to traffic. The likelihood that this issue would occur increased with the number of bandwidth management classes that were configured for the application. For more information on configuring bandwidth classes, see `#(config) bandwidth-management`.
SG-35472	Fixes an issue where the Edge SWG appliance did not terminate connections when a client sent RST packets. The proxy then sent repeated FIN-ACK requests to close the connections, which caused congestion on upstream devices.
SG-35310	Fixes an issue where a network interface could not be re-enabled from the command line interface (CLI).
SG-35210	Fixes an issue where the appliance stopped responding after an upgrade to version 7.3.13.3.
SG-35660	Fixes an issue where the appliance was slow to re-establish a gateway route after a network interface was disabled and enabled.

SGOS 7.3.14.6 PR

Release Information

- Release Date: April 16, 2024
- Build Number: 295196

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the cipher suites configuration of the HTTPS console is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.14.6

- See Fixes in SGOS 7.3.14.6.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.14.6

SGOS 7.3.14.6 includes the following bug fix:

Table 140: TCP/IP and General Networking

ID	Issue
SG-35138	Fixes an issue where the Edge SWG application that manages bandwidth used a large percentage (up to 100%) of the CPU and stopped responding to traffic. The likelihood that this issue would occur increased with the number of bandwidth management classes that were configured for the application. For more information on configuring bandwidth classes, see `#(config) bandwidth-management`.

SGOS 7.3.14.5 PR

Release Information

- Release Date: March 8, 2024
- Build Number: 294345

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Included-Component Versions

This version of SGOS includes the following versions of supporting components:

- Edge SWG Admin Console (SGAC): SGAC 2.1.4
- Web Visual Policy Manager (Web VPM): Web VPM 2.1.6

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the cipher suites configuration of the HTTPS console is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.14.5

- See Fixes in SGOS 7.3.14.5.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.14.5

SGOS 7.3.14.5 includes the following bug fixes:

Table 141: TCP/IP and General Networking

ID	Issue
SG-37446	Fixes an issue where TCP connections from the Edge SWG appliance stalled, resulting in almost no data being transmitted. When the appliance was in a stalled state, it repeatedly sent 1 byte of application data every 5 seconds. This issue only occurred for TCP connections that experienced packet loss or congestion in the network and that used the default New Reno congestion control algorithm. This issue was rare and was only easily detected for long-running connections, such as uploading access logs in continuous mode.

SGOS 7.3.14.4 PR

Release Information

- Release Date: October 26, 2023
- Build Number: 291000

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8-sha256
  – tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  – Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.14.4

- See Features in SGOS 7.3.14.4.

Fixes in ProxySG 7.3.14.4

- See Fixes in SGOS 7.3.14.4.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.14.4

HTTP/2 Server Connection Cache Enhancements

To improve the speed at which the appliance can serve HTTP/2 requests, enhancements have been made to the HTTP/2 Server Connection Cache. These enhancements include:

- Improvements to how the appliance responds when a server is unresponsive, reducing the number of connection attempts in the backlog.
- Troubleshooting improvements and statistics to help identify when streams are closed due to errors.

Fixes in SGOS 7.3.14.4

SGOS 7.3.14.4 includes the following bug fixes:

Table 142: Active Sessions

ID	Issue
SG-35265	Fixes a HTTP/2 Rapid Reset DDoS vulnerability. For more information, see https://knowledge.broadcom.com/external/article/274893 and Security Advisory 22674.

Table 143: Java Management Console and Java VPM

ID	Issue
SG-36779	Fixes an issue where the Java Management Console and Java VPM reported security errors when you accessed the Management Console and VPM. These errors occurred because the certificate chain was updated in June 2023 and the chain referenced a root CA that was not yet included by default in the Java trust store. Releases that occurred after October 2, 2023 are now signed by a certificate chain that has a root certificate that is in the Java trust store.

SG-36965	Fixes an issue where the Java Management Console, Launcher, and Java VPM did not launch with Java 1.8u351 or later because the signature of the signed SGOS Java code did not have an SHA-256 timestamp digest in the timestamp signature. Releases before October 2, 2023 had a signature with an SHA-1 timestamp digest.
	To avoid the following errors, use the ProxySG Admin Console for accessing the ProxySG appliance.
	If you are using the loader.jnlp, you may see one of the following messages:
	• **Security Warning: "Block potentially unsafe components from being run?":** To proceed, either click Don't Block, use the mc.jnlp file, upgrade Java to 1.8u351 or later, or upgrade SGOS to a release after October 2, 2023.
	• **Error Message "Application Blocked by Java Security":** To proceed, click OK and the loader opens or use the mc.jnlp file.
	• **Application Error "Unable to launch the application":** To proceed, either upgrade SGOS to a release after October 2, 2023 or remove the SHA-1 clause from the java.security file. To remove the SHA-1 clause:
	a. Navigate to the location of java.security file (for example, [JAVA_HOME]/jre/lib/security/java.security).
	b. Locate the text:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves, \`
	`      SHA1 denyAfter 2019-01-01`
	c. Replace the text with:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves`

SGOS 7.3.14.3 PR

Release Information

- Release Date: August 30, 2023
- Build Number: 289193

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.14.3

- See Features in SGOS 7.3.14.3.

Fixes in ProxySG 7.3.14.3

- See Fixes in SGOS 7.3.14.3.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.14.3

JAR File Update for the Java Management Console

The certificate used to sign the Management Console loader.jar has been updated. If you downloaded the Management Console loader.jar from KB articles previously, refer to the appropriate article for the latest version of the JAR file and how to install the certificates for it:

- Launch SGOS management consoles using the Management Console Launcher https://knowledge.broadcom.com/external/article?articleId=169194
- Management Console Launcher for systems without Internet connectivity https://knowledge.broadcom.com/external/article?articleId=169208
- Support for Java 11 on ProxySG and Advanced Secure Gateway appliance https://knowledge.broadcom.com/external/article?articleId=173228
- Download and Install the New Root and Intermediate Certificates for the Java Management Console Launcher: https://knowledge.broadcom.com/external/article/270160

Fixes in SGOS 7.3.14.3

SGOS 7.3.14.3 includes the following bug fixes:

Table 144: HTTP Proxy

ID	Issue
SG-35351	Fixes an issue where the intercepted TCP traffic was slow and the network stack experienced unexpected behavior after 49 days. This issue occurred due to a limitation related to the ProxySG appliance uptime.

SGOS 7.3.14.2 PR

Release Information

- Release Date: June 13, 2023
- Build Number: 286497

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.14.2

- See Fixes in SGOS 7.3.14.2.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.14.2

SGOS 7.3.14.2 includes the following bug fixes:

Table 145: Policy

ID	Issue
SG-35287	Fixes an issue where the appliance experienced a restart due to an out-of-memory condition during policy evaluation.

SGOS 7.3.14.1 GA

Release Information

- Release Date: May 16, 2023
- Build Number: 285017

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.14.1

- See Features in SGOS 7.3.14.1.

Fixes in ProxySG 7.3.14.1

- See Fixes in SGOS 7.3.14.1.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.14.1

ProxySG Admin Console 2.1.4

This release includes the ProxySG Admin Console (SGAC), which is a next-generation web interface. The SGAC 2.1.4 release includes all of the contents of SGAC 2.1.3. The SGAC is the default interface that opens in the browser. The Java-based Management Console will be removed in a future release. To learn more about the SGAC, refer to the following KB article:

https://knowledge.broadcom.com/external/article/251426

- Changes: Fixes in SGOS 7.3.14.1
- KB 251426: https://knowledge.broadcom.com/external/article/251426
- ProxySG Admin Console documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started.html
- SGAC Releases in SGOS

Web Visual Policy Manager 2.1.6

This release includes the Web Visual Policy Manager (Web VPM) 2.1.6 with the following enhancements:

- You can now search all levels of nested objects.
- Installing policy that includes the Set Effective Client IP object no longer triggers a deprecation warning.

For information on the Web VPM release, refer to the following documentation:

- Release announcement: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/22180
- Web VPM documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager.html
- Web VPM 2.1.6

Single Data Disk Deployments of ProxySG VAs Removed

New deployments of ProxySG virtual appliances (VAs) no longer support single data disk configurations. Existing single data disk configurations continue to work. To ensure redundancy and prevent data loss, migrate your single data disk configurations to multi-disk configurations.

More information:

- The specific VA deployment guide for your environment on the Tech Docs Portal
- Knowledge Base article: 262935

Configure Short and Long LACP Timeouts

To allow the appliance to interface with a variety of switches, a new CLI command is available to configure the LACP timeout for switches with slow (30 seconds) or fast (1 second) timeouts. To configure the appliance to interface with your switch, use the following command:

```
# (config interface aggr:number) lacp-timeout
fast|slow
```

More information:

- Command Line Interface Reference

New ALLOW (isolated) Verdict in Policy Traces

In earlier versions of SGOS that used Web Isolation, policy traces did not indicate that the appliance had isolated transactions. In 7.3.14.1, policy traces now label isolated transactions as `ALLOW (isolated)` .

Authentication Groups Now Reported in Policy Trace

When you perform a policy trace, information on which authentication groups users belong to is now reported in the trace.

ICAP Setup and Queuing Time Statistics Added

To track timing delays more explicitly, the time spent waiting due to ICAP setup and queuing has been added to the policy trace, access log, and HTTP statistics. Two new timestamps have been added to capture the elapsed time when the ICAP action is created, and when it is successfully queued up.

The following access log fields were added to support this feature:

- `x-bluecoat-icap-reqmod-setup-time`
- `x-bluecoat-icap-reqmod-queuing-time`
- `x-bluecoat-icap-respmod-setup-time`
- `x-bluecoat-icap-respmod-queuing-time`

The related statistics were added to the `/HTTP/Statistics` Advanced URL:

- Total MS ICAP REQMOD setup time
- Total MS ICAP REQMOD queuing time
- Total MS ICAP RESPMOD setup time
- Total MS ICAP RESPMOD queuing time

Customizable Variables for Special Use Cases

To support special use cases in your policy, the following custom Boolean, integer, and string variables have been added:

- `variable.custom_var_bool_`*`N`*
- `variable.custom_var_int_`*`N`*
- `variable.custom_var_str_`*`N`*

You can specify up to five custom variables of each type. All of the custom variables can be used in policy substitutions. In addition, the string variable supports base64 encoding.

More information:

- Content Policy Language Reference

Fixes in SGOS 7.3.14.1

SGOS 7.3.14.1 includes the following bug fixes:

Table 146: Access Logging

ID	Issue
SG-34512	Fixes an issue where the appliance experienced a restart due to the appliance not preserving keyring information for the session.
SG-34562	Fixes an issue where the appliance experienced a restart due to it concurrently initializing static objects in the access log.
SG-33009	Fixes an issue where performance decreased when the appliance was uploading the access log to Kafka servers in continuous mode.

Table 147: Admin Console

ID	Issue
SWGMGT-8827	Fixes an issue where the character limit on interface names on the Network Adapters page was incorrectly set and caused a Bad Configuration error. The character limit maximum is now 120 characters.
SWGMGT-8928	Fixes an issue where the minimum value for the 'Save First' field in the 'Start Packet Capture' dialog was too low. Now the allowed range is 128–65535 bytes.
SWGMGT-8941	Fixes an issue where the Forwarding Hosts page stop responding when loading many entries.

Table 148: Authentication

ID	Issue
SG-34059	Fixes an issue where users received the error message `The IWA direct realm encountered an unmapped error code` due to the appliance not challenging an invalid token that the Firefox browser supplied.
SG-34406	Fixes an issue where users received the error message `The call to Kerberos 5 failed` due to the appliance not supporting certain encryption types.
SG-34557	Fixes an issue where group authorization sometimes did not work for groups that had the same group name in policy and were realm qualified in multiple realms.
SWGMGT-8936 SWGMGT-8890 SG-34702	Fixes an issue where, if you launched the SG Admin Console (SGAC) or Web VPM from the ProxySG appliance, these UIs did not log users out when the session reached the web-timeout threshold. This issue did not affect the Java-based management console.
SG-34830	Fixes an issue where the appliance experienced a memory leak in the IWA direct realm under a heavy Kerberos authentication load.
SG-34973	Fixes an issue where the appliance experienced a memory leak during a heavy load for IWA direct Kerberos authentication.

Table 149: Boot

ID	Issue
SG-34019	Fixes an issue where the appliance stopped responding when executing the build image during an upgrade.
SG-34659	Fixes an issue where the appliance experienced a restart due to it leaking ICAP objects.

Table 150: CLI Consoles

ID	Issue
SG-32594	Fixes an issue where the appliance experienced a restart due to faulty condition handling in **Proxy Management Console** > **Maintenance** > **Send Service Information**.
SG-34063	Fixes an issue where the appliance reported the max-log-size in megabytes instead of mebibytes.
SG-34146	Fixes an issue where the appliance experienced a restart due to non-ascii character code sequences in a policy.

Table 151: Event Logging

ID	Issue
SG-30856	Introduces a method to better track syslog messages in case the appliance stops responding due to corrupted memory.
SG-34753	Fixes an issue where the appliance stopped responding when the length of the syslog message exceeded the maximum allocated size. The maximum allocated size has been increased to 64000 bytes.

Table 152: HTTP Proxy

ID	Issue
SG-28450	Fixes an issue where the appliance experienced a restart when offloading SSL traffic for HTTP/2 connections.
SG-33938	Fixes an issue where users could not access certain websites when HTTP/2 intercept was enabled due to the appliance incorrectly encoding the request path, resulting in a 404 response.
SG-34355	The Zlib library has been updated to resolve multiple vulnerabilities.
SG-34530	Fixes an issue where ETAP did not work for HTTP/2 client connections if client-encrypted tap policy (`client.connection.encrypted_ tap()`) contained the conditions `http.connect.host. category=`, `url.domain=`, or `url.category=`.

Table 153: Kernel

ID	Issue
SG-33290	Fixes an issue where the appliance experienced a restart due to memory not being used efficiently for HTTP/2 traffic.
SG-33826	Fixes an issue where the appliance experienced a restart due to the kernel reporting a false error when creating a process that had been completed quickly.

Table 154: Licensing

ID	Issue
SG-34145	Fixes an issue where the `show license enterprise` CLI command and /license/enterprise advanced URL displayed an incorrect aggregate CPU count for Enterprise or WPS licenses. Since this data is based on a deprecated license model, this command and URL have now been deprecated.

Table 155: Network Drivers

ID	Issue
SG-31708	Fixes an issue where the appliance experienced a restart due to malformed packets.

Table 156: Policy

ID	Issue
SG-34404	Fixes an issue in policy creation where there were no customizable variables available in CPL that could be base64 encoded. In this release, five placeholder string variables and five placeholder integer variables have been added.
SG-34491	Fixes an issue where policy definitions did not display in the output for the `#(config)show policy executable` command.

Table 157: SSL/TLS and PKI

ID	Issue
SG-34534	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.

Table 158: TCP/IP and General Networking

ID	Issue
SG-32527	Fixes an issue where the appliance stopped working after running out of cache buffers.
SG-34735	Fixes an issue where starting a packet capture that had already been started would stop the packet capture process.

SGOS 7.3.13.5 PR

Release Information

- Release Date: October 18, 2023
- Build Number: 290888

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.13.5

- See Features in SGOS 7.3.13.5.

Fixes in ProxySG 7.3.13.5

- See Fixes in SGOS 7.3.13.5.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.13.5

HTTP/2 Server Connection Cache Enhancements

To improve the speed at which the appliance can serve HTTP/2 requests, enhancements have been made to the HTTP/2 Server Connection Cache. These enhancements include:

- Improvements to how the appliance responds when a server is unresponsive, reducing the number of connection attempts in the backlog.
- Troubleshooting improvements and statistics to help identify when streams are closed due to errors.

Fixes in SGOS 7.3.13.5

Table 159: Active Sessions

ID	Issue
SG-35265	Fixes an HTTP/2 Rapid Reset DDoS vulnerability. For more information, see https://knowledge.broadcom.com/external/article/274893 and Security Advisory 22674.

Table 160: Java Management Console and Java VPM

ID	Issue
SG-36779	Fixes an issue where the Java Management Console and Java VPM reported security errors when you accessed the Management Console and VPM. These errors occurred because the certificate chain was updated in June 2023 and the chain referenced a root CA that was not yet included by default in the Java trust store. Releases that occurred after October 2, 2023 are now signed by a certificate chain that has a root certificate that is in the Java trust store.

SG-36965	Fixes an issue where the Java Management Console, Launcher, and Java VPM did not launch with Java 1.8u351 or later because the signature of the signed SGOS Java code did not have an SHA-256 timestamp digest in the timestamp signature. Releases prior to October 2, 2023 had a signature with an SHA-1 timestamp digest.
	To avoid the following errors, use the ProxySG Admin Console for accessing the ProxySG appliance.
	If you are using the loader.jnlp, you may see one of the following messages:
	• **Security Warning: "Block potentially unsafe components from being run?":** To proceed, either click Don't Block, use the mc.jnlp file, upgrade Java to 1.8u351 or later, or upgrade SGOS to a release after October 2, 2023.
	• **Error Message "Application Blocked by Java Security":** To proceed, click OK and the loader opens or use the mc.jnlp file.
	• **Application Error "Unable to launch the application":** To proceed, either upgrade SGOS to a release after October 2, 2023 or remove the SHA-1 clause from the java.security file. To remove the SHA-1 clause:
	a. Navigate to the location of java.security file (for example, [JAVA_HOME]/jre/lib/security/java.security).
	b. Locate the text:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves, \`
	`      SHA1 denyAfter 2019-01-01`
	c. Replace the text with:
	`jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024, \`
	`      DSA keySize < 1024, include jdk.disabled.namedCurves`

SGOS 7.3.13.4 PR

Release Information

- Release Date: September 22, 2023
- Build Number: 290000

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and Edge SWG (ProxySG) Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis : 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.5.x and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.13.4

- See Features in SGOS 7.3.13.4.

Fixes in ProxySG 7.3.13.4

- See Fixes in SGOS 7.3.13.4.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.13.4

JAR File Update for the Java Management Console

The certificate used to sign the Management Console loader.jar has been updated. If you downloaded the Management Console loader.jar from KB articles previously, refer to the appropriate article for the latest version of the JAR file and how to install the certificates for it:

- Launch SGOS management consoles using the Management Console Launcher https://knowledge.broadcom.com/external/article?articleId=169194
- Management Console Launcher for systems without Internet connectivity https://knowledge.broadcom.com/external/article?articleId=169208
- Support for Java 11 on ProxySG and Advanced Secure Gateway appliance https://knowledge.broadcom.com/external/article?articleId=173228
- Download and Install the New Root and Intermediate Certificates for the Java Management Console Launcher: https://knowledge.broadcom.com/external/article/270160

Fixes in SGOS 7.3.13.4

SGOS 7.3.13.3 includes the following bug fixes:

Table 161: Authentication

ID	Issue
SG-34758	Fixes an issue where the appliance did not respond when booting up after an upgrade.

Table 162: Boot

ID	Issue
SG-34019	Fixes an issue where the appliance stopped responding when executing the build image during an upgrade.

SGOS 7.3.13.3 PR

Release Information

- Release Date: April 19, 2023
- Build Number: 283837

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
```

```
   client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
 <ssl>
   server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.13.3

- See Fixes in SGOS 7.3.13.3.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.13.3

SGOS 7.3.13.3 includes the following bug fix:

Table 163: Event Logging

ID	Issue
SG-34753	Fixes an issue where the appliance stopped responding when the length of the syslog message exceeded the maximum allocated size. The maximum allocated size has been increased to 65536 bytes.

SGOS 7.3.13.2 PR

Release Information

- Release Date: March 29, 2023
- Build Number: 283458

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
```

```
   client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
 <ssl>
   server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.13.2

- See Fixes in SGOS 7.3.13.2.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.13.2

SGOS 7.3.13.2 includes the following bug fixes:

Table 164: Authentication

ID	Issue
SG-34557	Fixes an issue where group authorization sometimes did not work for groups that had the same group name in policy and were realm qualified in multiple realms.

SGOS 7.3.13.1 GA

Release Information

- Release Date: March 9, 2023
- Build Number: 282539

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
```

```
   client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
 <ssl>
   server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.13.1

- See Features in SGOS 7.3.13.1.

Fixes in ProxySG 7.3.13.1

- See Fixes in SGOS 7.3.13.1.
- To see any Security Advisories that apply to the version of you are running, go to:
  New advisories are published as security vulnerabilities are discovered and fixed.

Limitations

- See Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.13.1

Optimization for server.certificate.hostname=

For the `server.certificate.hostname=` condition, domain suffixes that begin with a '.' have been optimized for faster policy evaluation.

More information:

- Content Policy Language Reference

Configure ICAP Resource Overload Behavior

In 7.3.12.1, the CLI command `#(config icap <icap_service>)` **`resource-overload-time`** was introduced to bypass ICAP scanning to avoid latency and outage issues that can occur when the resources of the ICAP service are overloaded. For this feature to work, configure the following policy properties to fail_open:

- `request.icap_service()`
- `response.icap_service()`

In 7.3.13.1, the following access log fields have been added for troubleshooting and monitoring purposes:

- `cs-icap-failure-mode` : Displays how the failure_mode for the REQMOD transaction was configured. The possible values are `fail_closed` , `fail_open` , or `fail_open_unavailable` .
- `rs-icap-failure-mode` : Displays how the RESPMOD transaction was configured. The possible values are `fail_closed` , `fail_open` , or `fail_open_unavailable` .

Also, when ICAP resources are overloaded, the existing log fields `cs-icap-status` and `rs-icap-status` now display the value `ICAP_RESOURCE_OVERLOAD` .

The existing https://<*IP_address*>:<*port*>/ http/info Advanced URL has also been updated to identify whether HTTP cached objects hit this fail-open case during ICAP queuing. When the objects do hit this case, the information block for the HTTP object displays the message `ICAP response type: ICAP_RESOURCE_OVERLOAD` .

More information:

- Command Line Interface Reference
- Content Policy Language Reference
- Log Fields and Substitutions

Added HSTS Support for Virtual Authentication URLs

Appliances now support HTTP Strict Transport Security (HSTS) functionality for virtual authentication URLs.

Log Reduction for Common HTTP/2 Events

To make the event log clearer, the number of common HTTP/2 events that the appliance logs has been reduced.

Egress IP Address Selection

To reduce port exhaustion, you can now configure the appliance to set the egress IP address using a hash of the client IP address. Assign IP addresses that belong to the same subset of addresses to the same interface. The exception to this rule is if the interfaces you want to assign the addresses to belong to the same LAG or bridge. This feature is currently only available for IPv4 addresses.

To configure the egress IP address to use a hash of the client IP address for a physical interface, use the following CLI command:

```
# (config interface interface) address-selection ipv4-source-hash
```

You can also set the egress IP address for VLAN to use a hash of the client IP address or to inherit the configuration of the physical interface with the following command:

```
# (config interface interface.vlan) address-selection
 {ipv4-source-hash | inherit}
```

More information:

- Command Line Interface Reference

Empty r-supplier-country Entries in the Access Log Are Not Reported as Invalid

In previous releases, when the `r-supplier-ip` was not set to an IPv4 or IPv6 address, the appliance reported the `r-supplier-country` as `Invalid` in the access log. In 7.3.13.1, the appliance reports an empty `r-supplier-ip` with a - instead.

Delete the DNS Cache for a URL

You can now specify a *`hostname`* to clear the DNS cache for a specific URL with the following CLI command:

```
#clear-cache dns-cache [hostname]
```

More information:

- Command Line Interface Reference

New Cache Engine Statistics in the Heartbeat Data

To help track disk space usage, the following statistics have been added to the heartbeat data for the cache engine:

- Under Disks: DiskCEUsage
- Under Cache Engine Statistics:
  - LargeObjectsDeletedSinceRestart
  - LargeObjectsTerminatedSinceRestart

Enhancement for Troubleshooting Access Logging

To enable administrators to set and reset the debug level, reset the access-log debug log, and see the debug log related to the access-log, the following using Advanced URLs are added:

- /Accesslog/debug
- /Accesslog/debug/enable
- /Accesslog/debug/disable
- /Accesslog/debug/logaddmask
- /Accesslog/debug/logreset

Fixes in SGOS 7.3.13.1

SGOS 7.3.13.1 includes the following bug fixes:

Table 165: Authentication

ID	Issue
SG-33350	Fixes an issue where the appliance experienced a restart caused by insufficient stack space.
SG-33709	Fixes an issue where the syslog did not report when the WSS Agent was used to access the appliance and administrators could not perform Agent actions such as Reconnect, Block, and Disable.
SG-33854	Fixes an issue where the appliance experienced a restart when an Active Directory rejoin was done during a call to look up the user's email address.
SG-34045	Fixes an issue where the appliance assigned users to invalid groups of interests when they logged in to the appliance.

Table 166: Cache Engine

ID	Issue
SG-33713	Fixes an issue where the appliance lost all of its configuration due to the cache engine attempting to reinitialize the last valid disk on the appliance and destroying the contents of that disk.

Table 167: HTTP Proxy

ID	Issue
SG-28759	Fixes an issue where the appliance stopped responding when policy contained a section on policy substitution and CFS lookup.
SG-33950	Fixes an issue where users could not access some websites when DLP scanning was enabled on the appliance.

Table 168: ICAP

ID	Issue
SG-33253	Fixes an issue where the disks of the appliance filled up due to issues related to RAM-only objects, causing the appliance to stop responding.
SG-33599	Fixes an issue where the access log fields `cs-icap-failure-mode` or `rs-icap-failure-mode` were empty when ICAP scanning was bypassed due to the ICAP service being overloaded. Now when the service is overloaded, these fields contain the message `ICAP_RESOURCE_OVERLOAD`.
SG-33877	Fixes an issue where the users could not access the Internet and the CPU of the appliance experienced a high amount of usage.
SG-33953	Fixes an issue that occurred when the appliance used service groups in a sequence. If a service group contained any sick members, requests would fail open when the appliance exhausted the service group instead of the appliance sending to the next service group in the sequence.

Table 169: Java Management Console

ID	Issue
SG-34006	Fixes an issue where the appliance displayed a 404 error when users launched the Admin Console from Management Center, navigated to the PCAP/statistics screen, and clicked the Download PCAP button.

Table 170: Network Drivers

ID	Issue
SG-32963	Fixes an issue where the ProxySG application lost data on e-tap traffic due to it sending raw packets out of order to the ISG host.

Table 171: Policy

ID	Issue

SG-32518	Fixes an issue where the appliance did not deny access to the Admin Console when policy contained a DENY rule for a specific subnet. Now, policy denies access when you include the `deny.connection()` property. For example, the following rule denies access:
	`<admin>`
	`client.address=`*`ip-address`*` deny.connection`

SG-33614	Fixes an issue where the appliance stopped responding due to the appliance not decrypting a password.
SG-33817	Fixes issues where policy traces did not have evaluation results for hashed sections that were a MISS in policy and policy traces that did not display guard conditions that were a MATCH in policy.
SG-33959	Fixes an issue where the appliance did not protect tenant transitions in multi-threaded environments.

Table 172: SNMP

ID	Issue
SG-26639	Fixes an issue where the appliance experienced a restart because of an exception when trying to free cache.

Table 173: SSL/TLS

ID	Issue
SG-31247	Fixes an issue where removing a CA Certificate List (CCL) from the Trust Package did not remove it from the appliance.
SG-31528	Fixes an issue where the appliance experienced a memory leak during an HSM re-sign operation.
SG-32900	Fixes an issue where TCP termination errors were occurring in some configurations because the appliance was not sending the close_notify alert at the end of the TLS transaction.
SG-33613	Fixes an issue where the appliance stopped responding when closing an HTTP/2 session due to a race condition.

Table 174: Storage

ID	Issue
SG-33516	Fixes an issue where the virtual appliance stopped responding when it attempted to check the temperature of its disks and could not complete the check because virtual appliances do not have physical disks.

Table 175: TCP/IP and General Networking

ID	Issue
SG-33344	Fixes an issue where the appliance did not respond to ARP requests for interfaces that were part of a bridge and were not the common interface of the bridge.
SG-33952	Fixes an issue where the boot time was incorrectly reset on the software reboot and caused the expiry times in the route table to be incorrect.
SG-34021	Fixes an issue where the appliance removed the LAG configuration after rebooting if the LAG contained an interface that was also in the hardware bridge.

SGOS 7.3.12.1 GA

Release Information

- Release Date: January 30, 2023
- Build Number: 281125

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
```

```
   client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
 <ssl>
   server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console's cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.12.1

- See Features in SGOS 7.3.12.1.

Fixes in ProxySG 7.3.12.1

- See Fixes in SGOS 7.3.12.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.12.1

SGOS 7.3.12.1 introduces the following new features

ProxySG Rebrand as Edge SWG

Starting in version 7.4.x, the ProxySG will be known as Edge Secure Web Gateway (Edge SWG). Areas in the SGAC and the Web VPM, and some documentation, display the new product name.

ProxySG Admin Console 2.1.2

This release includes the ProxySG Admin Console (SGAC), which is a next-generation web interface. The SGAC is the default interface that opens in the browser. The Java-based Management Console will be removed in a future release. To learn more about the SGAC, refer to the following KB article:

https://knowledge.broadcom.com/external/article/251426

Previously, SGAC was available in Management Center only.

SGAC 2.1.2 release includes SGAC 2.1.1, which was released on November 21, 2022. For information on the SGAC release, refer to the following documentation:

- 2.1.1 features and changes: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/21104
- KB 251426: https://knowledge.broadcom.com/external/article/251426
- ProxySG Admin Console documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started.html
- SGAC Releases in SGOS

Web Visual Policy Manager 2.1.5.1

This release includes the Web Visual Policy Manager (Web VPM) 2.1.5.1, which was released on December 5, 2022. For information on the Web VPM release, refer to the following documentation:

- Release announcement: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/21107
- Web VPM documentation: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager.html
- Fixes in SGOS 7.3.12.1

Trust Package Update

The trust package has been updated. For an overview of the changes, refer to KB article 185058:

https://knowledge.broadcom.com/external/article/185058

To download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

Updated TLS Defaults and Support

For better security, TLSv1.2 and TLSv1.3 are the default selections in the following areas:

ProxySG Area	TLS Versions Support	Upgrade Behavior
HTTPS Management Console	TLSv1.1 cannot be enabled.	If you upgrade from version 6.7.x with TLSv1.1 enabled, it is disabled after the upgrade.
HTTPS Reverse Proxy service	TLSv1.1, TLSv1, and SSLv3 can be enabled.	If the older TLS/SSL versions were enabled before upgrading, they are still enabled after the upgrade.
SSL Client	TLSv1.1, TLSv1, and SSLv3 can be enabled.	If the older TLS/SSL versions were enabled before upgrading, they are still enabled after the upgrade.

ProxySG Area	TLS Versions Support	Upgrade Behavior
SSL Device Profile	TLSv1.1 and TLSv1 can be enabled. TLSv1.1 and TLSv1 cannot be enabled on read-only device profiles.	If the older TLS/SSL versions were enabled before upgrading, they are still enabled after the upgrade.

If you upgrade from version 6.7.x where only the default versions were selected, the current defaults apply and only TLSv1.2 and TLSv1.3 are selected.

Apparent Data Type Allow/Deny Policy Enhancement

This release adds the ability to allow or block Apparent Data Types in policies based on authentication conditions. Use the existing `http.request.apparent_data_type.allow()` and `http.request.apparent_data_type.deny()` properties. See the following example:

```
<Proxy "block file uploads from user">
  user=<authenticated_username> http.request.apparent_data_type.deny(<file_type>)
```

NOTE
Use these properties for Apparent Data Type detection of multipart data. The **Apparent Data Type** source object and its associated `http.request.apprarent_data_type=` condition do not support multipart data detection.

Policy Diagnostics Advanced URL Shows Status for Probe Definitions

The https://<*IP_address*>:<*port*>/Policy/Diagnostics Advanced URL now displays an appropriate status for probe definitions:

- `satisfied` : The condition specified in the `define probe` is met and diagnostics have been collected.
- `expired` : The `define probe` is expired.
  If the probe is neither satisfied nor expired, the Advanced URL displays the expiry date and time.

Configure ICAP Queueing Fail-Open Behavior

This release includes a CLI command to specify the time of the oldest queued request before a new request is failed-open, ICAP scanning is bypassed, and content is returned to the client:

```
#(config icap <icap_service>)resource-overload-time <0_to_300_seconds>
```

The existing https://<*IP_address*>:<*port*>/ OPP/statistics Advanced URL has also been updated with an OPP1.2 "Fail open due to resource overload" statistic. This statistic is incremented when a failed-open ICAP service or service group is overloaded.

NOTE
This feature is not fully functional yet. It will be available in a future release.

Improved Partial Object Handling

Previously, when the appliance detected a partial file, it treated it as a standard file when it was sent to Content Analysis. This process caused some slowness and unnecessary resource usage for Content Analysis, which was not always able to decode the file without reporting errors, or scan it. In this release, partial files are handled better when scanning is enabled. When a partial file is detected, these ICAP transactions are abandoned. On the client side, the appliance sends the partial file and resets the connections if the ICAP service is configured to **fail_open**. When ICAP is configured to **fail_closed**, the appliance sends an exception page or trickles the initial data and resets the connection.

When detecting partial objects and abandoning the ICAP transaction, the appliance:

- Closes the connection to Content Analysis while the request is being sent to Content Analysis, or
- If the ICAP service has the **Sense Settings** option applied and Content Analysis supports abandoning without closing the connection, the appliance finishes the transaction with a special chunk indicating that it is abandoning the request.

About Sense Settings

The Sense Settings change some ICAP settings based on the Content Analysis response. If Content Analysis supports abandoning the transaction without closing the connection, the appliance sends a dummy response from Content Analysis.

> **NOTE**
> Because this command can override some ProxySG ICAP settings (such as max-connect, preview, and defer-threshold based on the Content Analysis response to Sense Settings), the appropriate settings must be applied after the Sense Settings.

Policy

You can test for the `partial_object` error in the `request.icap.error_code=` and `response.icap.error_code=` conditions.

Access Logging

The following access log field values are added:

- `rs-icap-error-code` : Displays "partial_object" when a partial object is detected in the transaction.
- `rs-icap-error-details` : Displays "Abandoning ICAP request due to partial object" when the transaction is abandoned due to a partial object.

Monitoring

This release adds statistics to help monitor connectivity and improve troubleshooting during partial file transactions. To enable monitoring these statistics using SNMP, the BLUECOAT-SG-PROXY-MIB and BLUECOAT-SG-ICAP-MIB files have been updated.

Table 176: HTTP Miscellaneous Statistics (Advanced URL /HTTP/Statistics)

Statistic	Description
Total server connections with response timeouts	Total number of HTTP server connections on which a timeout occurred.
Total server connections with response errors	Total number of HTTP server connections on which a socket error occurred.
Total server connections with premature EOF	Total number of HTTP server connections on which a premature EOF was received. Server fin with (content-length or chunked-encoding) Closing the server socket normally is not considered an error if neither content-length or chunked-encoding headers are provided in the response. (The appliance can determine if the content is received fully or not when the server closes the socket.
Total transactions where object was truncated	Total number of HTTP server connections on which a premature EOF is set due to truncation failures.
Total transactions where object exceeded max cacheable size	Total number of HTTP server connections on which a premature EOF is set due to exceeding max cache size.
Total transactions abandoned by client	Total number of HTTP server connections on which a premature EOF occurs due to the client abandoning the connection
Total transactions where ICAP replacement was incomplete	Total number of HTTP server connections on which a premature EOF is set while handling ICAP response.

Previously, the Advanced URL counted only the total number of abandoned transactions. This release adds counters for the number of transactions aborted by the client and for transactions aborted by the server due to detecting partial objects or connectivity errors.

Table 177: OPP Statistics for an OPP-Entity: <icap_server_alias> (Advanced URL /OPP/Statistics)

Statistic	Description
Total aborted transactions by client	Total number of transactions that are aborted due to the client abandoning the request.
Total aborted transactions by server	Total number of transactions that are aborted due to the partial server response.

More information:

- Content Policy Language Reference
- SGOS Upgrade/Downgrade
- Log Fields and Substitutions

Updated Private MIB Files

The following objects were added to BLUECOAT-SG-PROXY-MIB:

- sgProxyHttpTotalServerConnectionWithResponseTimeouts
- sgProxyHttpTotalServerConnectionWithResponseErrors
- sgProxyHttpTotalServerConnectionWithPrematureEOF

The following objects were added to BLUECOAT-SG-ICAP-MIB:

- icapServiceStatsClientAbortedTrans
- icapServiceStatsServerAbortedTrans

More information:

- SNMP

Java Visual Policy Manager Help System Update

The look and feel of the Java VPM help system in this release is updated to be consistent with the Broadcom Tech Docs site.

Fixes in SGOS 7.3.12.1

SGOS 7.3.12.1 includes the following bug fixes. This release:

Table 178: Authentication

ID	Issue
SG-33471	Fixes an issue where the appliance experienced a hardware restart in Process group: "PG_CFG_PROPRIETOR", Process: "cfg.proprietor".
SG-33035	Fixes an issue where the appliance experienced a software restart in Process group: "PG_HEALTH_CHECKS", Process: "HC Worker".
SG-32051	Fixes an issue where the appliance stopped responding during an Integrated Windows Authentication (IWA) health check process.

Table 179: Boot

ID	Issue
SG-33552	Fixes an issue where upgrading from version 7.3.8.2 to version 7.3.10.11 or 7.3.11.1 caused the appliance to experience a page fault in Process group: "PG_CFSSL", Process: "Authenticate stack extender".

Table 180: CIFS Proxy

ID	Issue
SG-32854	Fixes an issue where the appliance performed consecutive restarts due to a race condition on the CIFS Admin queue.

Table 181: CLI Consoles

ID	Issue
SG-33195	Fixes an issue where the appliance stopped responding when the remote syslog server became unavailable and SSH was unable to transmit an error message.

Table 182: HTTP Proxy

ID	Issue
SG-30304	Fixes an issue where the policy trace incorrectly displayed `http2.client.accept() action will not apply` warnings for transactions where a tenant change reset the HTTP/2 upgrade decision.
SG-32975	Fixes an issue where requests to sites that used Akamai Bot Manager were blocked.

Table 183: ICAP

ID	Issue
SG-32014	Fixes an issue where the appliance experienced a restart after an ICAP service was removed.
SG-33017	Fixes an issue where incomplete transactions were slowing down ICAP transactions, causing clients to time out and reset.
SG-33291	Fixes an issue where a stale ICAP action was kept in the active queue while abandoning the ICAP requests.

Table 184: IPv6 Stack and IPv6 Proxies

ID	Issue
SG-32141	Fixes an issue where internet browsing was slow when IPV6 and `#(config)tcp-ip tcp-tso` were enabled.

Table 185: Management

ID	Issue
SG-33354	Fixes an issue where you could not download files (such as PCAPs) or change some settings (such as debug levels) on some Advanced URL pages.

Table 186: Policy

ID	Issue
SG-33214	Fixes an issue where the appliance experienced a page fault in Process group: "PG_POLICY_HTTP", Process: "PDW t=91494 for=A580031A".
SG-33200	Fixes an issue where the appliance experienced a page fault in Process group: "PG_CFG_PROPRIETOR, "Process: "cfg.proprietor".
SG-32945	Fixes an issue where the https://<*IP_address*>:<*port*>/Policy/Diagnostics Advanced URL incorrectly counted transactions that did not match a `define probe` condition.
SG-32689	Fixes an issue where policy rules to block some file uploads using the **Apparent Data Type** source object did not match. Blocking multiform data by Apparent Data Types is unsupported; see the "Apparent Data Type Allow/Deny Policy Enhancement" in Features in SGOS 7.3.12.1 for more information.

Table 187: SSL/TLS and PKI

ID	Issue
SG-33742	Fixes an issue where the appliance experienced an unexpected restart when performing SSLV Offload.

Table 188: SSL Proxy

ID	Issue
SG-32103	Fixes an issue where TLS selections for the HTTPS reverse proxy service were not maintained after an upgrade from version 6.7.x to 7.3.x.
SG-33341	Fixes an issue where the appliance served exception pages with expired certificates when Outlook autodiscover requests did not receive immediate responses.
SG-31502	Fixes an issue where rules including `client.protocol=` testing SSL or STunnel sometimes produced incorrect behavior, such as erroneously blocked sites. This issue occurred when policy included `ssl.forward_proxy(stunnel)` , or `ssl.forward_proxy(yes)` with protocol detection enabled. Refer to the SGOS 7.3.x Upgrade/Downgrade Behavior Changes for more information.

Table 189: System Statistics

ID	Issue
SG-33357	Fixes an issue where some SysInfo statistics shared the same obfuscated name.

Table 190: TCP/IP and General Networking

ID	Issue
SG-33192	Fixes an issue where the appliance did not apply GRE encapsulation on the SYN-ACK that it used to respond to the SYN sent from the WCCP router. This issue occurred when the appliance incorrectly applied RTS on the SYN-ACK.
SG-32744	Fixes an issue where the appliance experienced a page fault in Process group: "PG_TCPIP", Process: "stack-bnd-0:0-rxq-0".
SG-33331	Fixes a potential performance bottleneck that could occur when most of the appliance's traffic was HTTPS-tunneled.
SG-33782	Fixes an issue where the appliance stopped routing traffic because the gateway route expired (even though the route is healthy). This issue can be triggered from packet loss upstream of the appliance.

Table 191: Threshold Monitor

ID	Issue
SG-32856	Fixes an issue where the appliance experienced a restart after a sudden spike in traffic that pushed memory above the threshold.

Table 192: URL Filtering

ID	Issue
SG-30992	Fixes an issue where the appliance experienced a page fault in Process group: "PG_POLICY", Process: "PDW t=406795454 for=674839D1".

Table 193: Web VPM

ID	Issue
SWGMGT-2505	Fixes an issue where Web VPM performance decreased when compiling large policy.
SWGMGT-4923	Fixes an issue where the Web VPM could not modify combined objects that had spaces in the object name.
SWGMGT-8438	Fixes an issue where IP6 subnets of /40 and higher were stripped.
SWGMGT-8459	Fixes an issue where nested combined objects were removed when edited.
SWGMGT-8492	Fixes an issue where the Web VPM incorrectly displayed slow load confirmation in certain situations.
SWGMGT-8368	Provides enhancements for usability.
SWGMGT-8676	Fixes an issue where updating a nested combined object and then installing policy removed the object.

SGOS 7.3.11.3 PR

Release Information

- Release Date: January 20, 2023
- Build Number: 281125

IMPORTANT
This patch release (PR) includes a critical fix and replaces SGOS 7.3.11.1. If you are running an earlier 7.3.11.x release, upgrade to version 7.3.11.3 to apply the fix. See Fixes in SGOS 7.3.11.3 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.11.3

- See Fixes in SGOS 7.3.11.3.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.11.3

SGOS 7.3.11.3 includes the following bug fixes. This release:

Table 194: TCP/IP and General Networking

ID	Issue
SG-33768 SG-33871	Fixes an issue where the appliance stopped routing traffic because the gateway route expired (even though the route is healthy). This issue can be triggered from packet loss upstream of the appliance.

SGOS 7.3.11.1 GA

Release Information

- Release Date: November 16, 2022
- Build Number: 279474

IMPORTANT
This release is no longer available for download. To apply the changes and fixes from this release, upgrade to SGOS 7.3.11.3, which includes a critical fix. See Fixes in SGOS 7.3.11.3 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in ProxySG 7.3.11.1

- See Features in SGOS 7.3.11.1.

Fixes in ProxySG 7.3.11.1

- See Fixes in SGOS 7.3.11.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.11.1

SGOS 7.3.11.1 introduces the following new features:

Policy Condition to Test Appliance Name

You can test the configured name of an appliance in policy. Depending on the name of the current appliance, the condition evaluates to either true or false. In both cases, at least some of the affected rules or layers are removed from the compiled policy to optimize policy evaluation.

Use the following CPL condition:

```
appliance.name[.string_modifier][.case_sensitive|.case_insensitive]=<appliance_name1>[,<appliance_name2>, ...]
```

where *string_modifier* is [.exact|.prefix|.suffix|.regex]

For example, the following policy always evaluates to true on an appliance named SGOS_1:

```
<Proxy>
 url.domain=cnn.com appliance.name="SGOS_1" allow
```

The current policy file removes the condition from the rule:

```
<Proxy>   [layer 21] [vpm-cpl:3235]
  ALLOW url.domain=//cnn.com/
```

More information:

- appliance.name=

Policy Trace Enhancements

This release includes the following policy enhancements:

- Policy trace includes HTTP versions used on the client-side request and server-side response for HTTP/S transactions.
- Policy trace includes warnings when web isolation overrides forwarding and when isolation CONNECT header modifications are used for the transaction.

Web Isolation Enhancement

If the proxy forwards headers to the isolation service, the CLI warns you if the service is not using an SSL tunnel to the isolation server. For example, if you specified the service using `non-secure` and issue `#(config isolation)send authenticated-user`, the CLI displays `Warning: Sending sensitive information on non-secure isolation service!`

The same warning appears in the Admin Console (**Administration > Data & Cloud Services > Isolation**) if you select any options for **Include Headers** without selecting **Enable Secure Connection**.

For best security, enable Web Isolation in **secure** mode when sending headers

More information:

- Configure the web isolation feature on the ProxySG appliance (KB 201609)
- #(config isolation)

HTTP Enhancements

This release includes the following HTTP enhancements:

- The appliance now passes through some HTTP/2 error codes (such as HTTP_1_1_REQUIRED) back to the client when authentication required HTTP/1.1.
- The following access log fields now include more information for subsequent HTTP/2 transactions:
  – x-rs-certificate-validate-status
  – x-sc-connection-issuer-keyring
  – x-cs-connection-encrypted-tap
  – x-rs-connection-encrypted-tap
  – x-cs-ocsp-error
  – x-rs-ocsp-error
  – x-sc-connection-issuer-keyring-alias
  – x-sr-connection-client-keyring
  – x-cs-offload-session-log-id
  – x-rs-offload-session-log-id

FTP Upload Client Enhancements

You can now control FTP connection timeouts when uploading access logs. Use the following CLI commands:

```
#(config log <log_name>)ftp-client keep-alive-idle {<number_of_seconds> | default}
```

Specify the keep-alive timeout for idle sessions in seconds, or specify `default` to restore the default value of 10 seconds.

```
#(config log <log_name>)ftp-client keep-alive-interval {<number_of_seconds> | default}
```

Specify the keep-alive interval in seconds, or specify `default` to restore the default value of 5 seconds.

```
#(config log <log_name>)ftp-client timeout {<number_of_seconds> | default}
```

Specify how long the proxy should wait for a response from the log server in seconds, or specify `default` to restore the default value of 180 seconds.

In addition, the event log displays more details when the socket times out, closes, or has an error in the FTP upload client.

More information:

- #(config log *log_name*)

Health Check Status Advanced URL Enhancement

SGOS 7.3.10.1 introduced the ability to monitor the appliance health check status from an external service. In this release, the health check status URL (https://<*IP_address*>:<*port*>/healthcheck/status) returns details when the target is partially healthy.

More information:

- Monitor ProxySG health check status from an external service (KB248315)

Management Console Help System Update

The look and feel of the on-box Management Console help system in this release is updated to be consistent with the Broadcom Tech Docs site.

Fixes in SGOS 7.3.11.1

SGOS 7.3.11.1 includes the following bug fixes. This release:

Table 195: Access Logging

ID	Issue
SG-31411	Fixes an issue where Reporter rejected an access log that used the bcreporterwarp_v1 format due to parsing errors. This issue occurred when the access log contained WAF constraint violation entries.
SG-31536	Fixes an issue where uploading access logs with `continuous-upload` enabled reset TCP connections.
SG-32623	Fixes an issue where the `cs-auth-groups` access log field contained group information for transactions matching `authenticate(no)` policy. The `cs-auth-groups` field now shows `"-"` for these transactions.

Table 196: Authentication

ID	Issue
SG-32584	Fixes an issue where a ProxySG application running on the Integrated Secure Gateway rebooted after an upgrade from version 6.7.5.12 to version 7.3.9.2.
SG-30652	Fixes an issue where the appliance experienced a hardware restart in process "likewise Lsass_ADSyncMachinePassword" in liblikewise.exe.so.
SG-32220	Fixes an issue where the appliance experienced a hardware restart in process "Authenticate stack extender" in libicuuc.exe.so
SG-32805	Fixes an issue where Kerberos authentication failed with an error "Cannot decrypt ticket". This issue occurred when the load balancer user's userPrincipalName (UPN) attribute in Active Directory was set to a UPN suffix other than the suffix used in the user's DNS domain name.
SG-32109	Fixes an issue where the appliance experienced a page fault in Process group: "PG_HTTP", Process: "HTTP CW 106F30D1A40".

Table 197: Boot

ID	Issue
SG-32627	Fixes an issue where a potential race condition at startup could cause a crash in IPFW initialization. This issue occurred due to an underlying Kernel problem.

Table 198: CLI Consoles

ID	Issue
SG-32399	Fixes an issue where the `secure` flag was not set on the JSESSIONID cookie for HTTPS sessions.

Table 199: DNS Proxy

ID	Issue
SG-32789	Fixes an issue where the appliance stopped responding to DNS queries and initiating outbound connections to DNS servers.

Table 200: HTTP Proxy

ID	Issue
SG-32951	Fixes an issue where HTTP/2 Client Error Statistics and HTTP/2 Server Error Statistics on the "Show HTTP Statistics" Advanced URL page were duplicates.

Table 201: Policy

ID	Issue
SG-32939	Fixes an issue where the "Show policy diagnostics" Advanced URL page showed an incorrect number of transactions for configured diagnostics probes (`define probe`).
SG-32938	Fixes an issue where an uninitialized variable caused a hardware restart when referencing the appliance name.

Table 202: SSL/TLS and PKI

ID	Issue
SG-32029	Fixes an issue where SSL client certificate validation failed and access logs included errors such as `Client certificate (CN=<common_name>) validation failed: (null) (ssl_client_cert_ocsp_check_failed).`

Table 203: Tap

ID	Issue
SG-30756	Fixes an issue where encrypted tap shows a destination address of 0.0.0.0:0 when using HTTP/2 with an HTTP/1.1 server.

Table 204: TCP/IP and General Networking

ID	Issue
SG-32968	Fixes an issue where the appliance experienced a restart a crash during the closing of a TCP connection that had client spoofing enabled. This issue occurred in a WCCP setup with GRE as the forwarding protocol.
SG-32263	Fixes an issue where using Management Center to push policy with a large number of tenants caused a memory leak in TCP/IP.
SG-32241	Fixes an issue on S400 and S500 platforms with a bridge card, where a disabled bridge became enabled during boot and caused switches with STP to disable ports.
SG-32506	Fixes an issue where existing default routes on the appliance stopped working after an upgrade from version 6.7.5.12 to version 7.3.8.2.
SG-32708	Fixes an issue where the appliance experienced a hardware exception in Process group: "PG_UNKNOWN", Process: "registry" upon bootup. This issue occurred after downgrading SGOS.

SGOS 7.3.10.1 GA

Release Information

- Release Date: September 28, 2022
- Build Number: 278442

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

> **NOTE**
> The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.10.1

- SGOS 7.3.10.1 includes features and enhancements. See Features in SGOS 7.3.10.1.

Fixes in ProxySG 7.3.10.1

- This release includes fixes. See Fixes in SGOS 7.3.10.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.10.1

SGOS 7.3.10.1 introduces the following new features and changes.

Monitor ProxySG Health Check Status from an External Service

This release introduces the ability to associate system-defined, user-defined, or composite health checks with an external monitoring service. You can enable this feature on the ProxySG appliance and you can specify the health check target status URL (an Advanced URL on the appliance) in an external service. Then, you can take corrective actions as needed, based on the HTTP response associated with the Advanced URL status.

To support this feature, the following CLI command has been added:

```
#(config health-check) [no] status-check-target <alias>
```

where `<alias>` is the name of a configured user-defined composite health check. Enter the name in the format `user.<alias>`.

More information:

- Command Line Interface Reference
- KB248315 - "Monitor ProxySG health check status from an external service"

New response.header.<*header-name*>.exists= Policy Condition

You can now test if a specified HTTP header exists in a response. Use the following CPL:

```
response.header.<header_name>.exists={yes|no}
```

where `<header_name>` is a recognized HTTP header.

More information:

- Content Policy Language Reference

Cache Layer Supports ICAP Response Feedback Properties

You can now use the following ICAP response feedback properties in the `<Cache>` layer:

- `response.icap_feedback()`
- `response.icap_feedback.force_interactive()`
- `response.icap_feedback.interactive()`
- `response.icap_feedback.non_interactive()`

More information:

- Content Policy Language Reference

WebPulse Supports IPv6 Address

The WebPulse service supports using an IPv6 address, and hostnames that return IPv6 addresses.

Improved Performance in Threat Protection Database Traffic

This release includes optimizations that improve performance when the appliance processes content filtering, Threat Risk, and Application Protection database traffic (such as categorization requests and lookups).

WAF Subscription Updates

Web Application Firewall subscription updates are available. Download the latest WAF database to get the updated content.

More information:

- 2022 Content Updates

Remove Novell SSO, CA eTrust SiteMinder, and Oracle COREid Authentication Realms

Remove any existing Novell SSO, SiteMinder, and COREid realms that are still configured on the appliance. Support for these realms was deprecated in version 7.3.2.1, where you could still configure existing realms but not create new ones. In this release, you cannot configure existing realms.

To remove these realms, use the command to display existing realms. Then, remove the realms from the ProxySG configuration:

Table 205: Commands for removing deprecated realms

Authentication Realm	View Existing Realms	Remove Realms

Novell SSO	`#(config)`**`security novell-sso view`**	`#(config)`**`security novell-sso delete`**
		`<`*`realm_name`*`>`

CA eTrust SiteMinder	`#(config)`**`security siteminder view`**	`#(config)`**`security siteminder delete`**
		`<`*`realm_name`*`>`

Oracle COREid	`#(config)`**`security coreid view`**	`#(config)`**`security coreid delete`**
		`<`*`realm_name`*`>`

Fixes in SGOS 7.3.10.1

SGOS 7.3.10.1 includes the following bug fixes. This release:

Table 206: Access Logging

ID	Issue
SG-32245	Fixes an issue where the access log field `x-cs-client-effective-ip` incorrectly showed values between quotation marks (" ").

Table 207: Authentication

ID	Issue
SG-32284	Fixes an issue where an IWA Direct realm became unmapped after the system was rebooted.
SG-26119	Fixes an issue where the event log displayed "unable to connect to DC" errors even though the domain controller did respond.
SG-31006	Fixes an issue where the appliance experienced a restart in LDAP authentication code.

Table 208: Boot

ID	Issue
SG-31648	Fixes an issue where the appliance experienced a page fault in PG_DNS, Process: "libboot_console.exe.so" in "kernel.exe" at .text+0x12fe9a6.

Table 209: Cloud Platform

ID	Issue
SG-32304	Fixes an issue where the ProxySG application on ISG stopped responding when bridging was enabled.

Table 210: HTTP Proxy

ID	Issue
SG-31403	Fixes an issue where some origin content servers returned CAPTCHA prompts when HTTP/2 iwas enabled on the appliance.
SG-32173	Fixes an issue where a memory leak occurred in HTTP due to an issue with the H2 connection timers.
SG-28756	Fixes an issue where the appliance experienced a hardware exception in process "HTTP SW 10F72C46A40 for 20E95DABA40" in "libpolicy_enforcement.so" at .text+0x42f490.

Table 211: Initial Configuration

ID	Issue
SG-32117	Fixes an issue where the booting the ProxySG application on ISG did not display the prompt to activate the serial console. This issue occurred when booting a VM with bridge support and a ZTP payload.

Table 212: Kernel

ID	Issue
SG-32741	Fixes an issue where the appliance experienced a restart in process: "H2 SCH-2" in "kernel.exe" at .text +0x123f4c1.

Table 213: Licensing

ID	Issue
SG-31460	Fixes an issue where the booting the ProxySG application on ISG displayed memory configuration warnings for supported configurations.

Table 214: MAPI Proxy

ID	Issue
SG-31865	Fixes an issue where the appliance stopped responding during specific types of Outlook sessions (fast transfer messages) because memory was not allocated correctly.

Table 215: Performance

ID	Issue
SG-31917	Fixes an issue where the appliance stopped responding because resources were locked up while monitoring a faulty disk.
SG-31718	Fixes an issue where the ProxySG appliance on AWS stopped responding due to a race condition occurring during bootup.

Table 216: Policy

ID	Issue
SG-32189	Fixes an issue where policy did not match when a response Content-Length header value was large.
SG-32301	Fixes an issue where the `client.address=` and `client.effective_address` conditions did not use the value in the X-FORWARDED-FOR or CLIENT-IP headers. This issue occurred when the client address was previously tested during SSL interception from the forwarding proxy.

Table 217: Security

ID	Issue
SG-27826	Updates the open-source library Brotli to resolve multiple security vulnerabilities. The Brotli library is used to implement the Brotli data compression algorithm.
SG-29953	Updates the open-source library Newlib to resolve multiple security vulnerabilities. The Newlib library implements the C standard library.

Table 218: SSL/TLS and PKI

ID	Issue
SG-31808	Fixes an issue where the appliance experienced a page fault when an HSM was configured and **Enable CRL on emulated certificates** was set in the SSL proxy configuration.

Table 219: TCP/IP and General Networking

ID	Issue
SG-32162	Fixes an issue where the appliance stopped responding because packets arriving after the file handle closed were not ignored.
SG-31858	Fixes an issue where the appliance experienced a page fault in Process group: "PG_TCPIP"Process: "cookie-monster" in "libstack.exe.so" at .text+0x3e5cea.
SG-31623	Fixes an issue where bandwidth management failed due to a rounding error when calculating the processor frequency.
SG-31521	Fixes an issue where a memory leak occurred in DNS.
SG-32149	Fixes an issue where the appliance opened and closed the web filtering database every time it performed a web categorization.

Table 220: URL Filtering

ID	Issue
SG-32600	Fixes an issue where the appliance experienced a restart in Process: "HTTP CW 30E93122A40" in "liburl_filter.exe.so", Process group: "PG_POLICY_HTTP".
SG-31859	Fixes an issue where database downloads from an IPv6 address failed.
SG-32485	Fixes an issue where the appliance experienced a restart in Process: "HTTP CW 30E93122A40" in "liburl_filter.exe.so", Process group: "PG_POLICY_HTTP".

SGOS 7.3.9.2 PR

Release Information

- Release Date: August 4, 2022
- Build Number: 276793

> **IMPORTANT**
> This patch release (PR) includes a critical fix and replaces SGOS 7.3.9.1, which released on July 13, 2022. If you are running version 7.3.9.1, upgrade to version 7.3.9.2 to apply the fix. See Fixes in SGOS 7.3.9.2 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

> **NOTE**
> The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.9.2

- This release includes fixes. See Fixes in SGOS 7.3.9.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.9.2

SGOS 7.3.9.2 includes the following bug fixes. This release:

Table 221: TCP/IP and General Networking

ID	Issue
SG-32026	Fixes an issue where the appliance experienced a hardware exception in Process group: "PG_TCPIP" Process: "libopenldap.exe.so" in "libstack.exe.so" at .text+0x313a2a.

SGOS 7.3.9.1 GA

Release Information

- Release Date: July 13, 2022
- Build Number: 275996

> **IMPORTANT**
> This release is no longer available for download. To apply the changes and fixes from this release, upgrade to SGOS 7.3.9.2, which includes a critical fix. See Fixes in SGOS 7.3.9.2 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

> **NOTE**
> The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.9.1

- SGOS 7.3.9.1 includes features and enhancements. See Features in SGOS 7.3.9.1.

Fixes in ProxySG 7.3.9.1

- This release includes fixes. See Fixes in SGOS 7.3.9.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.9.1

SGOS 7.3.9.1 introduces the following new features and changes.

Deploy ProxySG VAs on VMware with ZTP

You can now deploy a ProxySG VA on VMware using ZTP.

More information:

- ZTP Deployment Guide

New Integrated Secure Gateway ProxySG Virtual Appliance Package for Microsoft Hyper-V

A new ProxySG virtual appliance package for the Integrated Secure Gateway (ISG) license is available to download from the Broadcom Support Portal and to deploy on Microsoft Hyper-V.

More information:

- ISG ProxySG VA on Hyper-V Deployment Guide

New Integrated Secure Gateway ProxySG Virtual Appliance Package for KVM

A new ProxySG virtual appliance package for the Integrated Secure Gateway (ISG) license is available to download from the Broadcom Support Portal and to deploy on Linux Kernel-based Virtual Machine (KVM).

More information:

- ISG ProxySG VA on KVM Deployment Guide

Layer 2 Transparent Support on Integrated Secure Gateway

The ProxySG appliance now supports Layer 2 (L2) transparent deployment when running as an application on Integrated Secure Gateway (ISG). To enable bridging, the ISG must be running 2.4.3.1 or later, and the ProxySG application must be running 7.3.9.1 or later.

L2 bridging support includes the following behavior changes or new behaviors:

Behavior on ProxySG appliances	Behavior when running ProxySG 7.3.9.1+ applications on ISG 2.4.3.1+ (if applicable)
The ProxySG appliance supports hardware and software bridges.	Hardware bridging support is new in this release. Enable hardware bridges on the ISG. The bridges are populated automatically in the ProxySG application. Software bridges are not supported. Any existing software bridges created in previous versions of the ProxySG application on ISG are automatically removed upon upgrade.
Hardware bridges have default labels of WAN/LAN.	Bridges are not labeled by default.

Configure a bridge's failover mode and link failure propagation settings on the ProxySG appliance:
`# (config bridge bridge_name) failover mode {parallel | serial}`
`#(config bridge bridge_name) propagate-failure {enable | disable}`
	Change a bridge's failure mode or link failure propagation settings on the ISG.

Behavior on ProxySG appliances	Behavior when running ProxySG 7.3.9.1+ applications on ISG 2.4.3.1+ (if applicable)
Reject inbound is enabled by default on WAN/LAN interfaces.	Reject inbound is disabled by default. Enable reject inbound on the externally-facing interface: `# (config interface interface) reject-inbound enable`

NOTE
To configure bridging on the ISG, refer to ISG documentation:

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/integrated-secure-gateway/2-4.html

License and Usage Telemetry Reporting

This release allows you to collect and send telemetry data to Broadcom. This feature is enabled by default. If you cannot send usage data automatically, you can enter the data manually at the Broadcom Support Portal. For more information, refer to Usage Data (Telemetry).

To support this feature, new `#(config telemetry)` commands have been added.

More information:

- Usage Data (Telemetry)
- Command Line Interface Reference

Web Visual Policy Manager Warns of Duplicate User Objects in Migrated Policy

The legacy VPM allows case-sensitive **User** object names, such as Bkent, bkent, and bKent. The Web VPM does not allow case-sensitive User object names; for example, if a **User** object named BKent already exists, you cannot create a **User** object named bKent. As a result, when you use the Web VPM to edit policy that was created in the legacy VPM, the Web VPM considers any existing **User** objects whose names differ only in letter case to be duplicates.

Starting in this release, the Web VPM displays a warning when you click **Edit** to change an existing **User** object to another object that has a duplicate.

To support this feature, the Web VPM allows you to filter the objects in the following areas:

- The All Objects dialog (**Operations > View All Objects**).
- The **Set** <*object_type*> **Object** dialog.

To filter objects, select **Filter By** and select one of the following options:

- **None**: (Default) No filter; the dialog displays all applicable objects.
- **Duplicates**: The dialog displays duplicate objects.
- **Unused**: The dialog displays objects that are configured but not included in any policy rules or objects.

NOTE
In a future release, the Web VPM will facilitate resolving duplicate objects without affecting policy operation. To receive updates about this feature, subscribe to KB244059 and refer to the *SGOS Release Notes* for future releases.

More information:

- Web VPM warns "User already exists" but I can't edit the user (KB244059)
- Web Visual Policy Manager documentation

Health Check Policy Enhancement

The health_check= condition now supports pattern matches and case sensitivity to test more selectively for health check names:

```
health_check[.string_modifier][.case_sensitive|.case_insensitive]=[user.]health_check_name
```

Supported modifiers are exact , prefix , regex , substring , and suffix . Refer to the CPL documentation for more information on the modifiers and how to use them in policy.

You can still test whether the current transaction is for any health check, or for a specific health check, using health_check={yes|no} .

More information:

- Content Policy Language Reference

'Service Request' Updated to 'Case Number' in User Interfaces

The ProxySG Management Console, Admin Console, and command line interface (CLI) now use the current term for support cases.

Previous term	Current term
service request (SR)	case
SR number	case number

For example, the command # (config service-info) **periodic sr-number** *sr_number* is now changed to # (config service-info) **periodic case-number** *case_number*.

More information:

- ProxySG Administration
- ProxySG Admin Console
- Command Line Interface Reference

Fixes in SGOS 7.3.9.1

SGOS 7.3.9.1 includes the following bug fixes. This release:

Table 222: Access Logging

ID	Issue
SG-29738	Fixes an issue where Kafka access logging had high memory usage.

Table 223: Authentication

ID	Issue
SG-26327	Fixes an issue where authenticating from a SAML realm without client redirects to a SAML realm with client redirects failed with a configuration error.
SG-31652	Fixes an issue where an error incorrectly indicated that SAML assertions were not encrypted. This issue occurred only when **Require encryption** was enabled in SAML realm configuration.
SG-31984	Fixes an issue where SAML stopped working with Chromium-based browsers (Chrome, Edge, Chromium, etc.) due to blank (space) characters between the cookie parameters.

ID	Issue
SG-31405	Fixes an issue where changing a member realm within a sequence realm after installing authentication policy resulted in an authentication error.
SG-31809	Fixes an issue where a page fault occurred in PG_CFG_PROPRIETOR in process: "IWA Onbox Domain Trust Refresher".
SG-32045	Fixes realm configuration issues that occurred after deleting policy that referenced a sequence realm with a Windows SSO member realm.

Table 224: DNS Proxy

ID	Issue
SG-30851	Fixes an issue where, when the appliance replied to DNS queries with the correct IP address and TTL=0.

Table 225: HTTP Proxy

ID	Issue
SG-31525	Fixes an issue where the appliance stopped responding when the appliance processed an ICAP RESPMOD with a header value greater than 8kB.

Table 226: IPv6 Stack and IPv6 Proxies

ID	Issue
SG-31698	Fixes an issue where the appliance experienced a restart in process "stack-bnd-2:0-rxq-0" in "libstack.exe.so".

Table 227: Legacy Visual Policy Manager

ID	Issue
SG-30905	Fixes an issue where policy could not be installed using the legacy VPM when policy included **Notify User** objects.

Table 228: MAPI Proxy

ID	Issue
SG-30723	Fixes an issue where ROP_GET_PER_USER_LONG_TERM_IDS request parsing failed due to the GUID value being read incorrectly.

Table 229: Reverse Proxy

ID	Issue
SG-31076	Fixes an issue where reverse proxy traffic had latency of 5-15 seconds. This issue occurred with `session-cache-clientmap` enabled and HTTP configuration set to `http no persistent server`. The issue was caused by unnecessary checks during cache insertion and removal that degraded performance under heavy load.

Table 230: SNMP

ID	Issue
SG-30952	Fixes an issue where event logs showed SNMP errors "Getting ipV4 vlan information for <*interface*> failed".

Table 231: SSH Proxy

ID	Issue
SG-31624	Fixes an issue where the appliance experienced a page fault in PG-SSH and process "admin@ssh".

Table 232: TCP/IP and General Networking

ID	Issue
SG-31420	Fixes an issue where enabling IP forwarding (IPv4/IPv6) disabled the stack's LRO (Large Receive Offload) for all flows (whether they were forwarded or not), preventing some performance gains provided by LRO.
SG-20236	Fixes an issue where the appliance experienced a restart due to a socket allocation failure.
SG-31640	Fixes an issue where the appliance experienced a restart because a cached packet was for a terminated connection (in TIME_WAIT), causing the appliance to lose track of the listening socket to which a SYN needed to be sent.
SG-31670	Fixes an issue where the appliance experienced a restart and prompted you to select an image to load after the reboot.
SG-31513	Fixes an issue where network drivers used a shared heap without proper locking.
SG-31175	Fixes an issue where the appliance experienced non-atomic route manipulation.
SG-31804	Fixes an issue where the passthru interface was configured for spanning tree participation (STP) even though the interface was disabled.
SG-29829	Fixes an issue where the appliance experienced a page fault in PG_TCPIP in process: "cookie-monster" in "libstack.exe.so".

SGOS 7.3.8.2 PR

Release Information

- Release Date: June 7, 2022
- Build Number: 274167

> **IMPORTANT**
> This patch release (PR) includes a critical fix and replaces SGOS 7.3.8.1, which released on May 11, 2022. If you are running version 7.3.8.1, upgrade to version 7.3.8.2 to apply the fix. See Fixes in SGOS 7.3.8.2 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.6.x and later, and 11.x and later
- Management Center: 2.2.2.3 and later

> **NOTE**
> The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.8.2

- SGOS 7.3.8.2 includes the features and enhancements that are introduced in version 7.3.8.1. See Features in SGOS 7.3.8.1.

Fixes in ProxySG 7.3.8.2

- This release includes the fixes that are introduced in version 7.3.8.1 and a critical fix. See Fixes in SGOS 7.3.8.1 and Fixes in SGOS 7.3.8.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.8.2

SGOS 7.3.8.2 includes the following bug fix, as well as the fixes included in version 7.3.8.1.

Table 233: Kernel

ID	Issue
SG-31689	Fixes an issue where kernel lock changes caused the appliance stop responding.

SGOS 7.3.8.1 GA

Release Information

- Release Date: May 11, 2022
- Build Number: 273000

IMPORTANT
This release is no longer available for download. To apply the changes and fixes from this release, upgrade to SGOS 7.3.8.2, which includes a critical fix. See Fixes in SGOS 7.3.8.2 for information.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 ProxySG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

NOTE
The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- Upon upgrading to 7.3.x, malware scanning is replaced with Symantec Access Security Policy and Content Security Policy. For information, see Using Policy Services in the ProxySG administration documentation.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

NOTE
If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.8.1

- SGOS 7.3.8.1 introduces new features and enhancements. See Features in SGOS 7.3.8.1.

Fixes in ProxySG 7.3.8.1

- This release includes various fixes. See Fixes in SGOS 7.3.8.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of the limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.8.1

SGOS 7.3.8.1 introduces the following new features and changes.

ProxySG Admin Console 1.2.4

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

SSL/TLS Version Controls for SSL Forward Proxy

Alternatively, use the CLI. Use the CLI to set the minimum version and maximum version of the SSL/TLS protocol to use for client connections:

```
# (config ssl) proxy client-ssl-version-range <minimum_version> <maximum_version>
```

Set the minimum version and maximum version of the SSL/TLS protocol to use for server connections:

```
# (config ssl) proxy server-ssl-version-range <minimum_version> <maximum_version>
```

To control the SSL/TLS versions used for specific transactions instead of using the global command, add the following Action VPM objects to policy:

- **Set Client Min Max SSL Version**
- **Set Server Min Max SSL Version**

Alternatively, use the CPL properties associated with these VPM objects:

- `client.connection.min_ssl_version()`
- `client.connection.max_ssl_version()`
- `server.connection.min_ssl_version()`
- `server.connection.max_ssl_version()`

Prior to this release, the SSL/TLS version used for intercepted SSL connections was the highest version supported by the appliance, the client, and the server. This behavior is the same as using the `preserve` option, which is the default setting.

More information:

- Command Line Interface Reference
- Web Visual Policy Manager Reference
- Content Policy Language Reference
- Security Best Practices

X.509v3 Enhancements for Self-Signed Certificates and Certificate Signing Requests

When creating self-signed certificates and certificate signing requests (CSRs), you can specify values for the following extensions:

- Subject Alternative Name
- Basic Constraints
- Key Usage
- Extended Key Usage

Refer to the following CLI example for usage:

```
#(config ssl)create signing-request ssl_proxy_issuer_keyring c US cn "My SSL Proxy" bc CA:TRUE ku
 digitalSignature,keyCertSign eku serverAuth,clientAuth
```

You can also set a "critical" flag for these attributes to indicate that OpenSSL must enforce using the attribute for your security needs. Refer to the *Command Line Interface* for more information.

More information:

- Command Line Interface Reference

Separate Event Logging Configuration for Email and Syslog

Previous SGOS releases allowed you to select event logging levels that applied to all events for Syslog and email. Now, you can select different event logging levels for Syslog and email, as well as use event IDs to specify overrides to the default logging level.

To support this feature, the following commands are deprecated:

```
# (config event-log) level <level>
```

```
# (config event-log) syslog {enable | disable}
```

Use the following new commands to configure and view event log notification settings:

```
# (config event-log notifications) <subcommands>
```

```
# show event-log notifications
```

You can also use the ProxySG Admin Console (**Administration > Logging > Event Logging**) to configure the logging behavior.

More information:

- ProxySG Admin Console
- Command Line Interface Reference

Recognition of Specific CAB Data Types in HTTP Responses

The `http.response.apparent_data_type=<data_type>` condition now supports matching for specific CAB file types:

- `MSCAB` : MS Cab archive
- `ISCAB` : InstallShield archive

The existing`CAB` type previously matched for MS Cab only; now you can use it to match for both MSCAB and ISCAB.

More information:

- Content Policy Language Reference
- SGOS 7.3.x Upgrade/Downgrade

Threat Detection Notification VPM Objects

SGOS 7.3.4.1 introduced CPL to trigger ICAP notifications based on content in ICAP-scanned requests and responses. For more information, see "ProxySG ICAP Enhancements" in Features in SGOS 7.3.4.1. Version 7.3.8.1 adds the following new Service VPM objects for the gestures:

- **Request Threat Detected**: (Static object) Specifies whether threat scanning detected a threat in the request.
  CPL condition: `request.icap.threat_detected=`
- **Response Threat Detected**: (Static object) Specifies whether threat scanning detected a threat in the response.

CPL condition: `response.icap.threat_detected=`

- **Request Threat Info**: Specifies whether threat scanning detected a specific type of threat in the request.

  CPL conditions: `request.icap.threat_id=` , `request.icap.threat_id.exists=` , `request.icap.threat_details=` , `request.icap.threat_details.exists=` , `request.icap.threat_source=` , and `request.icap.threat_source.exists=`
- **Response Threat Info**: Specifies whether threat scanning detected a specific type of threat in the response.

  CPL conditions: `response.icap.threat_id=` , `response.icap.threat_id.exists=` , `response.icap.threat_details=` , `response.icap.threat_details.exists=` , `response.icap.threat_source=` , and `response.icap.threat_source.exists=`

These objects are available in the Web Access Layer and Web Request Layer.

More information:

- Web Visual Policy Manager Reference

Deploy ProxySG Virtual Appliance to ESX Environments using VMware Tools

For secured ESX environments that do not permit mounting an ISO file, you can provide the ZTP payload as a parameter to VMware tools so that you can use ZTP to programmatically deploy Virtual Appliances.

More information:

- ZTP Deployment

Microsoft Outlook Email Protocol (MAPI) Improvements

- REQMOD and RESPMOD statistics are now reported separately under MAPI over HTTP proxy statistics (available at advanced URL /mapihttp/statistics).
- Email attachment upload in Outlook 2021 is significantly improved. Previously, sometimes uploaded email attachments were truncated, jumbled, or both. Email attachment upload is now fully supported in Outlook 2021.
- Email attachment upload performance is improved.

Specify an Interface for Reflect Client IP

When initiating upstream connections, use the specified interface for the outbound source IP address.

```
reflect_ip(interface.<label>)
```

More information:

- Content Policy Language Reference

Removed Hardware Registration Commands

The following CLI commands have been removed:

```
#licensing register-hardware
#licensing mark-registered
```

These commands are no longer required for licensing an appliance.

Fixes in SGOS 7.3.8.1

SGOS 7.3.8.1 includes the following bug fixes.

Table 234: Access Logging

ID	Issue
SG-23434	Fixes an issue where the appliance stopped responding when running an access logging script from Management Center.
SG-30186	Fixes an issue where the s-action access log field returned "-" instead of information from the transaction.
SG-30522	Fixes an issue where the appliance stopped responding in process "cfg.proprietor" in "libtransactions.exe.so" at .text+0x3135c0.
SG-29190	Fixes an issue where the appliance stopped responding when access logs included `*-supplier-country` fields or policy included references to supplier country.

Table 235: Active Sessions

ID	Issue
SG-31084, SG-29401	Fixes an issue where terminating active sessions (using `#active-sessions proxied-sessions terminate`) caused the appliance to stop responding.

Table 236: Authentication

ID	Issue
SG-29479	Fixes an issue where CPU utilization was 100% under heavy LDAP load.
SG-31219	Fixes an issue where changing policy that included a sequence realm caused the appliance to stop responding.
SG-30269	Fixes an issue where the "Access Denied" exception page did not display information about the transaction when users clicked the **more** link.
SG-31171	Fixes an issue where policy failed to install after a sequence realm had an authorization error.
SG-30293	Fixes an issue where changing the SAML IDP caused an "invalid certificate" error and required an appliance reboot to refresh the certificate cache.
SG-30783	Fixes an issue where the appliance rebooted when attempting to apply policy changes. This issue occurred after an IWA realm was removed.
SG-30844	Fixes an issue where attempting to upgrade version 7.2.5.1 to 7.3.7.1 failed. When this issue occurred, the appliance rebooted with version 7.2.5.1 running.
SG-31292	Fixes an issue where the appliance stopped responding after deleting realms after attempting to install policy with bad syntax.

Table 237: CLI Consoles

ID	Issue
SG-30692	Fixes an issue where the show config CLI output did not indicate whether automatic refresh bandwidth for caching was enabled (for example, using `#(config caching)refresh bandwidth automatic`).
SG-30948	Fixes an issue where the appliance stopped responding in process group PG_ACCESS_LOG, process: "sshc.worker" in "" at .text+0x0.
SG-30917	Fixes an issue where `#show output` displayed some archive-config settings incorrectly, without quotation marks.

Table 238: Cloud Platform

ID	Issue
SG-30953	Fixes an issue where an appliance with a ZTP payload could not be registered to a device group in Management Center.
SG-23203	Fixes an issue where the appliance stopped responding due to a hardware exception in process "STORVSC" in "storvsc.exe".

Table 239: DNS Proxy

ID	Issue
SG-31007	Fixes an issue where the appliance stopped responding with a hardware exception in process group "PG_DNS"Process: "DNS Proxy Administrator" in "libdnsproxy.exe.so".

Table 240: Hardware Drivers

ID	Issue
SG-30813	Fixes an issue where PCAPs with filters captured traffic only in one direction. This issue occurred on ProxySG applications on the SSP platform.

Table 241: HTTP Proxy

ID	Issue
SG-26322	Fixes an issue where the appliance stopped responding with a software exception in process group "PG_HTTP" process: "HTTP SW 20B1CD01A40 for 30C2D661A40" in "".
SG-29480	Fixes an issue where the appliance did not send an "HTTP/1.1" ALPN extension in the server hello message back to the client when the server used HTTP/2.
SG-29969	Fixes an issue where the appliance stopped responding when trying to allocate memory when mapping HTTP/2 to HTTP/1 headers.

Table 242: Licensing

ID	Issue
SG-29643	Fixes an issue where a SWG VA that could not communicate with the license validation server had a grace period of 3.5 days instead of 7 days.

Table 243: Management

ID	Issue
SG-30997	Fixes an issue where the https://<*IP_address*>:8082/Secure/Local/console/MCApplet.html page had a potential XSS exploit.

Table 244: MAPI Proxy

ID	Issue
SG-30307	Fixes an issue where some users intermittently could not send messages with attachments from Outlook 2021.
SG-30245	Fixes an issue where messages from which the proxy blocked and removed attachments were not sent.
SG-30807, SG-31250	Fixes an issue where dragging and dropping a file from email to a delegate calendar sometimes resulted in file corruption.

Table 245: Management Console

ID	Issue
SG-31038	Fixes an issue where the Management Console could not be accessed after Chrome was updated to version 10.

Table 246: Policy

ID	Issue
SG-30288	Fixes an issue where the appliance performed DNS queries even when policy included a `restrict dns` rule.
SG-30564	Fixes an issue where logs did not indicate that a local database containing an error was downloaded. When this issue occurred, the download status did not reflect the latest download status immediately, and the Local Database communication status metric was Critical.
SG-30206	Fixes an issue where the appliance experienced a hardware exception in process group "PG_POLICY"Process: "SSLW 10D7510DC00" in "libc.so".
SG-30360	Fixes an issue where the default value of a variable was not used when the variable was used in a substitution.

Table 247: SSL/TLS and PKI

ID	Issue
SG-30816	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.
SG-30416	Fixes an issue where the appliance had a hardware exception in process group: "PG_SSL_HNDSHK" process: "Hybrid_Administrator" in "kernel.exe".
SG-30565	Fixes an issue where multiple TCP sessions used the same TCP connection, causing some requests not to match.

Table 248: SSL Proxy

ID	Issue
SG-30706	Fixes an issue where high memory caused TCP connections to drop.
SG-29909	Fixes an issue where SSL connections requiring server certificate emulation timed out when the server certificate cache was full.
SG-26714	Fixes an issue where `client.certificate.requested=` lookups failed.

Table 249: TCP/IP and General Networking

ID	Issue
SG-30509	Fixes an issue where upgrading the appliance from version 7.2.x to a later 7.2.x or 7.3.x failed while performing #restart upgrade.
SG-30896	Fixes an issue where the appliance stopped responding when adding default gateways.
SG-29589	Fixes an issue where the appliance stopped responding in process: "cookie-monster" in "libstack.exe.so" at .text +0x42d3e1.

Table 250: Legacy VPM

ID	Issue
SG-30750	Fixes an issue where a line break in the Comment cell creates an unknown tag that fails to install.

Table 251: Web VPM

ID	Issue
SG-28356	Fixes an issue where the web VPM page did not load. When this issue occurred, policy loaded in the legacy VPM.
SG-28393	Fixes an issue where the **Comment** cell and tooltips did not display long comments correctly.
SG-28590	Fixes an issue where saving policy changes after saving previous changes did not automatically refresh the **Generated CPL**. This issue occurred when launching the VPM from Management Center.
SG-28100	Fixes an issue where Excel files could not be previewed on Dropbox when policy included a **Notify User** object.

SGOS 7.3.7.1 GA

Release Information

- Release Date: February 24, 2022
- Build Number: 271019

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- Gen3 Proxy SG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200
- Integrated Secure Gateway hardware appliances: SSP-S210, SSP-S410

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- You may potentially experience performance issues after upgrading to this release. See SG-30438 in Known Issues in SGOS 7.x for more information.
- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.7.1

- SGOS 7.3.7.1 introduces new features and enhancements. See Features in SGOS 7.3.7.1.

Fixes in ProxySG 7.3.7.1

- This release includes various fixes. See Fixes in SGOS 7.3.7.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.7.1

SGOS 7.3.7.1 introduces the following new features and changes.

Session Correlation with SSL Visibility Appliance

When session correlation is enabled, the SSL Visibility (SSLV) appliance sends its client-side and server-side session log IDs to the ProxySG appliance. To review the SSLV session log IDs from the ProxySG appliance, add the following fields to the access log.

1. In the SSL Visibility Management Console, enable the **Session Correlation with ProxySG** option.
2. In the ProxySG Admin Console or Management Console, add the following access log fields to the `ssl` log:
   - `x-cs-offload-session-log-id` : SSLV client-side session log ID when SSLV is performing SSL offload.
   - `x-rs-offload-session-log-id` : SSLV server-side session log ID when SSLV is performing SSL offload.
   - `cs(X-Forwarded-For)` : Value of request header X-Forwarded-For.

   This feature requires SSLV appliance version 5.4.1.1 or later. SSLV version 4.5.9.1 will also support this feature.

   > **NOTE**
   > These options only apply to traffic that is not destined for ProxySG appliances, and the ProxySG segment needs at least one copy port in place to have SSLV inspect non-proxy flows.

More information:

- SSLV documentation (available when version 5.4.1.1 is released)
- ProxySG Log Fields and Substitutions

Drop ICMP Redirect Packets

This release addresses a potential vulnerability where an attacker could send ICMP redirect packets to the appliance. This can result in the redirection of traffic to an attacker-controlled device, potentially compromising the integrity of any redirected unencrypted traffic, or lead to a denial-of-service if the attacker blocks redirected traffic. This release includes a new CLI command to enable dropping ICMP redirects:

```
#(config)tcp-ip icmp-drop-redirect {disable|enable}
```

The setting is disabled by default. For best security, enable it.

More information:

- Command Line Interface Reference

Access Log Fields for ICAP Failure Mode

The following access log fields have been added to track the ICAP failure mode (fail open or fail closed):

- `cs-icap-failure-mode` : REQMOD ICAP service failure mode
- `rs-icap-failure-mode` : RESPMOD ICAP service failure mode

More information:

- ProxySG Log Fields and Substitutions

Trust Package Update

The trust package has been updated to match the Microsoft July 2021 update level. Obsolete CAs have been removed. To download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

Timezone Database Update

The timezone database has been updated to reflect changes in Release 2021e of the IANA timezone database.

CSRF Protection for Advanced URLs

This release includes additional cross-site request forgery (CSRF) attack protection for ProxySG advanced URLs.

Removed Web-Based Initial Configuration Wizard

The browser-based ProxySG Initial Configuration Wizard (available through https://proxysg.bluecoat.com:8083 or https://*IP_address*:8083) has been removed. Starting in this release, you can perform initial configuration through the serial console only.

Fixes in SGOS 7.3.7.1

SGOS 7.3.7.1 includes the following bug fixes.

Table 252: Access Logging

ID	Issue
SG-28439	Fixes an issue where the appliance experienced a restart following disk re-initialization due to an error in the access log copying process.
SG-29685	Fixes an issue where access logging used more memory than required.

Table 253: Authentication

ID	Issue
SG-26170	Fixes an issue where RADIUS authentication stopped working after upgrading to version 7.3.2.1.
SG-29329	Fixes an issue where SNMP walk failed because the appliance attempted to retrieve authentication statistics from a server that was unavailable, instead of retrieving them from a cache.
SG-25285	Fixes an issue where SAML authentication stopped working with Chromium-based browsers (such as Chrome, Edge, and Chromium) in versions after SGOS 6.7.5.6 due to blank characters (spaces) between the cookie parameters.

Table 254: Boot

ID	Issue
SG-30541	Fixes an issue where a ProxySG virtual appliance running on Google Cloud Platform experienced a restart loop.

Table 255: CLI Consoles

ID	Issue
SG-29744	Fixes an issue where the appliance experienced a page fault due to insufficient Syslog worker stack size.

Table 256: CPLE

ID	Issue
SG-29957	Fixes an issue where `server.certificate.hostname=` matched only the first entry under the `subjectAlternativeName` of the certificate. Now, all available server certificate hostnames are checked and matched.

Table 257: DNS Proxy

ID	Issue
SG-28533	Fixes an issue where the appliance experienced restarts when EDNS was enabled and DNS lookup was performed for an IP address.
SG-28266	Fixes an issue where the appliance did not honor the configured DNS server preference after a primary or alternate server went offline and then came back online.
SG-32131	Fixes an issue where performing `# test dns` resulted in an "Unknown error response(203)" when EDNS was enabled.

Table 258: HTTP Proxy

ID	Issue
SG-28504	Fixes an issue in reverse proxy during the processing of HTTP requests to prevent HTTP request smuggling / HTTP desync attacks.
SG-29322	Fixes an issue where Firefox showed an alert on the Host Affinity cookie because the appliance did not set up all of the required cookie attributes.
SG-28248	Fixes an issue where the appliance experienced a restart when policy included a `log_message()` action referring to an HTTP header substitution string.
SG-29187	Fixes an issue where the appliance experienced a restart when multiple H2 workers tried to use the same socket during an HTTP/2 upgrade.
SG-30148	Fixes an issue where the downstream SNI header was not applied on an upstream connection when the HTTP Connect message contained a dotted IP address. This issue occurred when a transparent downstream Squid proxy connected upstream to an explicit ProxySG appliance.

Table 259: Kernel

ID	Issue
SG-29402	Fixes an issue where the appliance experienced a restart due to an insufficient front panel worker stack size.

Table 260: MAPI Proxy

ID	Issue
SG-30196	Fixes an issue where Outlook 2012 file attachments were not sent to Content Analysis.
SG-28606	Fixes an issue where the MAPI debug log displayed the error: `Rop response parser failed to parse RopId = ROP_QUERY_ROWS with value ERROR_CODE_PARSE_ERROR.` This issue occurred in Outlook 2016 with caching disabled.

Table 261: Policy

ID	Issue
SG-27100	Fixes an issue where Excel files on Dropbox could not be previewed when policy included the **Notify User** action.
SG-30085	Fixes an issue where the link to Symantec Site Review on exception pages was broken in some cases.
SG-29657	Fixes an issue where installing policy that contained many categories resulted in multiple "Unknown category" warnings.
SG-28593	Fixes an issue where long lines in exceptions files were parsed incorrectly, preventing some elements from displaying in exception pages.
SG-28416	Fixes an issue where installing policy fails with a warning "Unreachable rule, conditions will be matched by a preceding rule" when policy contains different IP addresses in a category definition.

Table 262: Security

ID	Issue
SG-28694	Fixes an issue where the `load trust-package` command output showed an incorrect creation time, suggesting that the trust package was not the latest version.
SG-29650	Fixes an issue where the `show configuration` command output did not display the `trust-package auto-update` or `auto-update-interval` configuration settings.

Table 263: Serviceability

ID	Issue
SG-29688	Fixes an issue where PDM statistics were inaccurate because the PG process memory usage reported on linear memory instead of physical memory.

Table 264: SSL/TLS and PKI

ID	Issue
SG-28734	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.
SG-29503	Fixes an issue where a memory leak occurred when a certificate was re-signed for an intercepted TLS connection and OCSP was enabled.

Table 265: SSL Proxy

ID	Issue
SG-29358	Fixes an issue where the appliance experienced a restart when attempting to complete an SSL handshake using a closed socket.
SG-28624	Fixes an issue where the browser returned an exception because the latest Chrome and Firefox extensions were not included in the known extensions list.
SG-28622	Fixes an issue where server certificates were not validated as specified in policy when the appliance encountered unrecognized extensions.

Table 266: Storage

ID	Issue
SG-29406	Fixes an issue where disk space issues caused the appliance to stop responding. This issue occurred when ICAP scanned large objects.

Table 267: TCP/IP and General Networking

ID	Issue
SG-28822	Fixes an issue where the connection pair of a transparent IPv6 session by SSLV reused the same TCP source port if the **Reflect Client IP** option was enabled, resulting in session timeouts.
SG-29607	Fixes an issue where download failures occurred due to an insufficient number of TCP re-assembly objects for the number of connections.
SG-28561	Fixes an issue where the user could not filter active sessions with an IPv6 address.
SG-28638	Fixes an issue where the appliance experienced a restart due to asynchronous requests in progress during a SOCKS timeout.
SG-28909	Fixes a rare race condition when a TCP connection was cleaning up that could lead to a restart.
SG-28841	Fixes an issue where the appliance experienced a restart due to invalid memory pointers.
SG-28994	Fixes an issue where port reuse caused latency and dropped Internet connections. This issue occurred in a transparent proxy environment with `reflect-client-ip` enabled.
SG-29217	Fixes an issue where the appliance experienced a restart because the limit on the number of canceled timers was reached.
SG-29824	Fixes an issue where running the `pcap start coreimage` *`bytes`* command caused the appliance to stop responding.
SG-29051	Fixes an issue where the appliance experienced high memory consumption in TCP/IP, causing Internet sessions to stop until the appliance restarted. This issue occurred with bandwidth management enabled.
SG-28444	Fixes a timer issue that caused the appliance to experience high CPU usage and a restart.
SG-30132	Fixes an issue where some TCP connections were incorrectly kept open instead of closing or being reused.
SG-29737	Fixes a potential race condition where TCP persistence timer reuse led to a restart.

Table 268: URL Filtering

ID	Issue
SG-29178	Fixes an issue where every URL lookup returned an 'unavailable; unlicensed' status after clearing category mappings and synonyms and reloading the Blue Coat content filtering database.
SG-28860	Fixes an issue where the Threat Risk Levels database was stuck in a 'loading' status even after an appliance restart.
SG-28565	Fixes an issue where the appliance sent too many SNMP messages for content filtering database changes.

Table 269: Utility Libraries

ID	Issue
SG-28924	Updates the open-source library libxml to resolve multiple security vulnerabilities. This open-source library is used to parse XML in WAF deployments and for XML/SAML authentication realms.
SG-28926	Fixes an issue where the third-party ICU (International Components for Unicode) library required updating to resolve critical vulnerabilities. This open-source component consists of C/C++ and Java libraries for Unicode support, software internationalization, and software globalization.

Table 270: Web Application Firewall

ID	Issue
SG-28299	Updates the open-source library libxml to resolve multiple security vulnerabilities. This open-source library is used to parse XML in WAF deployments and for XML/SAML authentication realms.

Table 271: Web VPM

ID	Issue
SG-28521	Fixes an issue where attempting to install web VPM policy that included multiple objects of the same type did not save all instances of the object. This issue occurred if the object names were not changed from their defaults.

SGOS 7.3.6.4 PR

Release Information

- Release Date: December 15, 2021
- Build Number: 269365

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- 3 Gen Proxy SG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After upgrading, reconfigure your malware scanning. For information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.6.4

- This release includes a fix for a connection issue for configurations transparently intercepting traffic with `reflect-client-IP` enabled. See Fixes in SGOS 7.3.6.4.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.6.4

SGOS 7.3.6.4 includes the following bug fix.

Table 272: Health Checks, TCP/IP and General Networking

ID	Issue
SG-29088	Fixes an issue where ProxySG 7.3.6.1 and higher configurations transparently intercepting traffic with `reflect-client-IP` enabled stopped initiating or responding to new connections. These configurations consequently required a scheduled SG reboot before the maximum number of available connections was reached.

SGOS 7.3.6.3 PR

Release Information

- Release Date: December 13, 2021
- Build Number: 268974

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- 3 Gen Proxy SG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

> **NOTE**
> The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After upgrading, reconfigure your malware scanning. For information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.6.3

- This release includes a performance fix. See Fixes in SGOS 7.3.6.3.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.6.3

SGOS 7.3.6.3 includes the following bug fix.

Table 273: Performance

ID	Issue
SG-29292	Fixes an issue where SSL performance dropped. This issue occurred when SSL interception policy was installed.

SGOS 7.3.6.1 GA

Release Information

- Release Date: October 7, 2021
- Build Number: 266990

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA
- 3 Gen Proxy SG virtual appliances for GCP and ISG Enterprise VA deployments: ISG-Proxy-VA-100, ISG-Proxy-VA-200

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.

- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.6.1

- This release includes various fixes. See Fixes in SGOS 7.3.6.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.6.1

SGOS 7.3.6.1 introduces the following new features and changes.

ProxySG Admin Console 1.2.3

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

PM Object to Enable/Disable Parallel Connectivity

The content policy language (CPL) to enable or disable parallel connectivity using RFC8305 (Happy Eyeballs algorithm) was added in version 7.3.4. This release adds new **Enable Parallel Connect** and **Disable Parallel Connect** static Action objects to the Web Visual Policy Manager (VPM). The algorithm can improve user experience when requesting specified URL domains by allowing parallel connections, which avert delays that might occur with serial connection attempts. To enable or disable parallel connections globally, use the `#(config)`**`parallel-connect`** `{`**`enable`** `|` **`disable`**`}` CLI command, introduced in version 7.3.4.1.

More information:

- Web Visual Policy Manager Reference

New Default Port for Web Isolation Service

Starting in this release, the default port for the Web Isolation Service is 443 instead of 8080. If you currently use the default web isolation service hostname and port, upgrading will change the port from 8080 to 443. If you then downgrade to version 7.3.5 or earlier, the configuration retains the port 443 setting. If you configured a custom web isolation service, issuing the `# (config isolation)` **`service cloud`** command in version 7.3.6 reverts the service to default settings, including the new default port.

More information:

- Command Line Interface Reference
- KB article 201609

Review and Terminate Active Sessions and Connections

To help with troubleshooting, a new `#` **`active-sessions`** CLI command allows you to display a list of active inbound ADN connections, bypassed connections, or proxied sessions. You can also terminate multiple connections or long-running sessions, which may be faster than terminating sessions from the Management Console.

In addition, a new `#` **`show active-sessions`** command displays overall session statistics including active, terminating, and errored sessions.

More information:

- Command Line Interface Reference

Determine Host ISG for ProxySG Applications

A new `#` **`show isg-host`** CLI command allows you to determine if the current appliance is running as an application on Integrated Secure Gateway (ISG). If it is an application running on ISG, the command displays ISG host information. Otherwise, the CLI indicates that the system is not running on ISG.

More information:

- Command Line Interface Reference

Detect Protocol in <Proxy> Layers

The `<SSL-Intercept>` layer no longer supports `detect_protocol()` . Use this property in `<Proxy>` layers.

Fixes in SGOS 7.3.6.1

SGOS 7.3.6.1 includes the following bug fixes.

Table 274: Abstract Management Interface

ID	Issue
SG-28486	Fixes an issue where the upgrade process had an uncaught exception because an invalid hostname was saved in the registry.

Table 275: Authentication

ID	Issue
SG-25971	Fixes an issue where the whoami response header (X-WSS-CLIENT-INFO-2-RESPONSE) was not being returned from the proxy unless SAML authentication was used. This caused WSSA to use a cached username when switching to/from SAML authentication.
SG-28600	Fixes an issue where the appliance restarted when an object representing the authentication state was sometimes NULL and it was handled incorrectly.

Table 276: DNS Proxy

ID	Issue
SG-17287	Fixes an issue where the ProxySG appliance was restarting because DNS/Stack allocations that were close to a multiple of the page size were causing a page fault.

Table 277: Initial Configuration

ID	Issue
SG-28355	Fixes an issue where new ProxySG appliances that were not yet licensed could not be added to Management Center using ZTP.

Table 278: HTTP Proxy

ID	Issue
SG-28013	Fixes an issue where the appliance stopped responding with a hardware exception in process group: "PG_ POLICY" and process "HTTP CW 10F37D70A40" in "libcfssl.exe.so" at .text+0x2af117.
SG-28181	Fixes an issue where proxy exception pages were not loading when SSLv offload and HTTP/2 were enabled.
SG-28553	Fixes an issue where setting `http2.client.max_concurrent_streams(1)` did not allow any streams through because the concurrent stream count was incremented too early.
SG-28708	Fixes an issue where `ip_country_uid_map` was not initialized properly if parallel connections are enabled.
SG-28290	Fixes an issue where the appliance experienced high memory usage due to some HTTP/2 processes.

Table 279: Kernel

ID	Issue
SG-28065	Fixes an issue where the central policy file download interval constantly increased.

Table 280: Management Console

ID	Issue
SG-28324	Fixes an issue where the certificate in a keying could not be changed through the Management Console if the keyring was referenced elsewhere. Now, the **Import** button in a keyring is always available.

Table 281: MAPI

ID	Issue
SG-25958	Fixes an issue where sending Outlook mail did not work unless MAPI handoff was disabled on the appliance (or HTTPS interception of office 365 servers were not enabled). This issue occurred after an upgrade to Outlook 2016.

Table 282: Policy

ID	Issue
SG-28376	Fixes an issue where larger base64-encoded images using `<style>` tags did not display in exception pages.
SG-28353	Fixes an issue where, after authenticating and getting the group policy site location, refreshing the browser caused the location ID to change to the default of `0` .

Table 283: SNMP

ID	Issue
SG-28264	Fixes an issue where the SNMP OID `tcpCurrEstab` reported a larger number than the number in `/TCP/Connections`.

Table 284: SSL Proxy

ID	Issue
SG-27138	Fixes an issue where specifying the CCL using the `client.certificate.validate.ccl()` property did not work in reverse proxy mode.

Table 285: SSL/TLS and PKI

ID	Issue
SG-28279	Fixes an issue where an ADN deployment had a potential memory leak in SSL and Cryptography.

Table 286: TCP/IP and General Networking

ID	Issue
SG-26282	Fixes an issue where high memory usage in TCP/IP led to general connectivity issues and event log errors. This issue occurred with IPv6 traffic and when bandwidth management was enabled.
SG-28111	Fixes an issue where extra interfaces defined in the ARM template for ProxySG on Azure were not displayed when issuing the `>show interface all` command output on the VM.
SG-28434	Fixes an issue where there was a memory leak when Jumbo frames were enabled, which were not accounted for when cleaning up reference count objects.
SG-28528, SG-28723	Fixes an issue where the appliance experienced frequent unforced restarts in the PG_TCPIP process.

SGOS 7.3.5.2 PR

Release Information

- Release Date: September 7, 2021
- Build Number: 265904

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
```

```
    server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8-sha256
  – tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  – Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.5.2

- This release includes a single fix. See Fixes in SGOS 7.3.5.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.5.2

Deprecations and Removals

This release removes the HTTP/2 Server Connection handling improvements made in SGOS 7.3.5.1. These improvements will be available in a future release.

Fixes in SGOS 7.3.5.2

SGOS 7.3.5.2 includes the following bug fixes.

Table 287: HTTP Proxy

ID	Issue
SG-28388	Fixes an issue where the appliance experienced a restart when upgrading server connections to HTTP/2.

SGOS 7.3.5.1 GA

Release Information

- Release Date: August 25, 2021
- Build Number: 265431

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
```

```
    server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suite configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.5.1

- This release includes various fixes. See Fixes in SGOS 7.3.5.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.5.1

SGOS 7.3.5.1 introduces the following new features and changes.

New Models for Virtual Appliances

For ProxySG virtual appliances, the following new models are available for GCP and ISG Enterprise VA deployments:

Virtual CPUs	Virtual Memory (GB)	ISG-Proxy-VA-100 Storage (GB)	ISG-Proxy-VA-200 Storage (GB)	Connection Count
6	24	2x100	1x200	37,500
6	40	4x100	2x200	62,500
6	48	4x100	2x200	75,000

Virtual CPUs	Virtual Memory (GB)	ISG-Proxy-VA-100 Storage (GB)	ISG-Proxy-VA-200 Storage (GB)	Connection Count
10	40	4x100	2x200	62,500
10	80	4x100	2x200	125,000
10	96	4x100	2x200	150,000
12	48	4x100	2x200	75,000
12	96	4x100	2x200	150,000
12	128	4x100	2x200	200,000
14	64	4x100	2x200	100,000
14	112	4x100	2x200	175,000
14	144	8x100	4x200	225,000
20	96	4x100	2x200	150,000
20	144	N/A	4x200	225,000
20	192	N/A	6x200	300,000
24	112	4x100	2x200	175,000
28	128	8x100	4x200	200,000
28	192	N/A	6x200	300,000
28	288	N/A	8x200	450,000
32	80	8x100	2x200	125,000
32	160	N/A	4x200	250,000
32	256	N/A	8x200	400,000
32	320	N/A	8x200	500,000

More information:

- *SGOS on GCP Configuration Guide*
- *ISG Enterprise VA Guide*

Set IP Version Preferences for DNS Resolution

You can now configure preferences for which IP version to use for DNS queries by using the following command (default is `unspecified`):

```
#(config)dns ip-version {ipv4-only|ipv6-only|prefer-ipv4|prefer-ipv6|unspecified}
```

More Information:

- *Command Line Interface Reference*

Configure Local Categories for Web Filtering

You can disable or enable whether local categories for Web Filtering are included in the configuration for the proxy client with the following command:

```
#(config clients web-filtering)include-local-categories {disable | enable}
```

More Information:

- *Command Line Interface Reference*

New `incorrect_content_length` Option for `response.raw_headers.tolerate`

Previously, the appliance would forward responses that exceeded the length specified in the response header to the ICAP server or client. Now the appliance drops additional bytes before sending a response. If you do want the appliance to forward responses that exceed the specified length, use the property `response.raw_headers.tolerate(incorrect_content_length)`.

More information:

- *Content Policy Language Reference*

Updated Application Protection Database

SGOS 7.3.5.1 enables the appliance to use the new version of the fingerprint database when the next Application Protection subscription is released.

More information:

- *Web Applications Firewall Solutions Guide*

New CLI Command for ARP Strict Matching

The following CLI command is available for enabling and disabling ARP strict matching (default `enable`):

```
#(config)tcp-ip arp-strict-matching {enable|disable}
```

More information:

- *Command Line Interface Reference*

Event Log Trace Level Enhancement

The `#(config event-log)`**`level trace`** CLI command was added in version 7.3.2.1. In this release, the `trace` level also writes long-running ICAP REQMOD transactions, and deferred and resumed ICAP RESPMOD transactions to the event log.

More Information:

- *Command Line Interface Reference*
- *SGOS Upgrade/Downgrade*, "Behavior Changes in SGOS 7.3.x"

Timezone Database URL HTTPS by Default

The timezone database download is now performed over HTTPS by default.

New HTTP Headers for `delete()` Action

You can now delete the following custom request headers by using the `delete()` policy action:

- X-BlueCoat-Authorization
- X-WSS-Client-Info
- X-WSS-Client-Info-2
- X-WSS-Client-Info-SSO-Request
- X-WSS-SAML

More Information:

- *Content Policy Language Reference*

HTTP/2 Hardening

Improvements to HTTP/2 connections have been made to increase security and efficiency of HTTP/2 connections by reducing additional upstream connections.

Fixes in SGOS 7.3.5.1

SGOS 7.3.5.1 includes the following bug fixes.

Table 288: Authentication

ID	Issue
SG-27258	Fixes an issue with the help text for the `# (config local-user-list` *`local_user_list user_name`*`)` **`password-grace ?`** command. Now the help text prompts for the number of days to be supplied.
SG-27378	Fixes an issue where users could not join or rejoin a domain if the username contained a dollar sign ($) character.
SG-27405	Fixes an issue where details for group-async were not available for the `#show configuration` and `#(config windows-domains)view` commands.
SG-27851	Fixes an issue where users that belonged to a user group of a parent domain were not able to authenticate.

Table 289: DNS Proxy

ID	Issue
SG-27367	Fixes an issue where the appliance experienced a restart when the DNS proxy incorrectly copied from or to a null pointer.

Table 290: HTTP Proxy

ID	Issue
SG-25111	Fixes an issue where `supplier.country` policy did not match for tunneled HTTPS connections when protocol detection was disabled.
SG-26987	Fixes an issue where content-length headers had incorrect values when server-side HTTP requests were translated to HTTP/2.
SG-27922	Fixes an issue where connections would break for some WebFTP clients.

Table 291: Initial Configuration

ID	Issue
SG-27919	Fixes an issue where appliances that could not download the application database on the first attempt would wait until the next scheduled download time, which might not have been for several hours. Now the appliance re-attempts the download more frequently until a connection is established and then returns to the usual frequency for downloading.

Table 292: Kernel

ID	Issue
SG-27772	Fixes an issue where after 49 days, appliances running any version including and between SGOS 7.3.1.1 to 7.3.4.1 experienced high CPU utilization, and traffic being refused and hung up.

Table 293: Policy

ID	Issue
SG-26626	Fixes an issue where the appliance experienced a restart when the hostname was assigned "null" during address resolution.
SG-27924	Fixes an issue where HTTP connections that were terminated by a timed termination caused a delay in exception pages from displaying. Now the fields for the timed termination are copied to the SSL proxy to prevent delays.
SG-28067	Fixes an issue where the appliance experienced a restart when the EDNS handler did not recognize the end of the source buffer.

Table 294: SSL/TLS and PKI

ID	Issue
SG-27616	Fixes an issue where policy that contained `server.connection.client_issuer_keyring()` did not work as expected in a reverse proxy deployment.
SG-28105	Fixes an issue where the appliance experienced a restart during an SSL session.

Table 295: SSL Proxy

ID	Issue
SG-23268	Fixes an issue where a memory leak occurred when SSLV offloading was enabled.
SG-26999	Fixes an issue where the appliance experienced high memory usage during SSL handshakes.

Table 296: TCP/IP and General Networking

ID	Issue
SG-25055	Fixes an issue where the appliance experienced a restart due to outstanding TCP timers.
SG-27025	Fixes an issue where ARP strict matching was not functioning as expected.
SG-27375	Fixes an issue where the appliance experienced a restart when the database was updated.
SG-27677	Fixes an issue where the appliance returned the error "DNS Resolver Response: Unknown error response(202)" for a DNS-forwarding group that was associated with the default routing domain.
SG-27681	Fixes an issue where entries in the ARP table were incorrectly shown as expired when accessed through the CLI or Management console.
SG-27756	Fixes an issue where the statistics counter for ARP strict matching continued to increase when Management Console URLs were accessed in a bridge configuration.
SG-27807	Fixes an issue where DNS flags were not set correctly for AAAA requests, causing the appliance to not retry with A requests after receiving invalid AAAA responses.
SG-27947	Fixes an issue where appliances that were configured in a bridge could not be pinged after a restart.

ID	Issue
SG-28005	Fixes an issue where default gateways or static routes in routing domains were pointing to the incorrect interface.
SG-28102	Fixes an issue where the appliance experienced a crash when a high number of HTTP connections were established.

Table 297: Web VPM

ID	Issue
SG-27169	Fixes an issue where the policy enforcement was not correctly applied due to the Application Group incorrectly referencing an object.

SGOS 7.3.4.1 GA

Release Information

- Release Date: July 14, 2021
- Build Number: 264353

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- Content Analysis: 2.4.x, 3.0.x, and 3.1.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
```

```
    server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8-sha256
  – tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  – Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.4.1

- SGOS 7.3.4.1 introduces new features and enhancements. See Features in SGOS 7.3.4.1.

Fixes in ProxySG 7.3.4.1

- This release includes various fixes. See Fixes in SGOS 7.3.4.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.4.1

SGOS 7.3.4.1 introduces the following new features and changes.

ProxySG Admin Console version 1.2.2

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

Support for Java 16 on ProxySG Appliances

The Management Console Launcher is now supported for Java 16. For more information, refer to https://knowledge.broadcom.com/external/article/173228/.

UDP Proxy Enhancements

SGOS 7.3.2 introduced a UDP-Tunnel proxy service and provided basic visibility into UDP flows through the appliance. This release allows you to intercept and further manage UDP flows.

UDP proxy services

Starting in this release, the appliance's **Default** service listener which matched all TCP traffic not intercepted by other services is renamed to **Default TCP**. A new **Default UDP** service listener has been added, which is used for all UDP traffic not intercepted by other services.

This release also introduces the following new CLI commands:

- `# (config udp_proxy_service) intercept <subcommands>`
  Set the behavior of the UDP service listener to intercept.
- `# (config) udp-tunnel <subcommands>`
  Configure UDP tunnel connections.

In the ProxySG Admin Console, you can configure a UDP Tunnel proxy service in **Configuration > Services > UDP Tunnel Proxy Settings**.

New Microsoft Teams proxy service

This release includes a new built-in proxy service for Microsoft Teams. This proxy service uses the UDP Tunnel proxy and is set to Bypass by default. To edit the Microsoft Teams service, use the following commands:

```
#(config proxy-services)edit "MS Teams"
```

This changes the prompt to `#(config MS Teams)` . Refer to the`#(config udp_proxy_service)` command in the *Command Line Interface* documentation for supported subcommands.

New policy URL scheme

The `url=` and related `url` conditions now support UDP as follows:

```
server_url=udp-tunnel://<ip_address>
```

Statistics and monitoring

Statistics about UDP traffic are now available in various areas of the Management Console:

- Active Sessions
- Advanced URLs:
  - Show UDP proxy debug log - Displays information such as internal settings and error messages
  - Show UDP proxy statistics - Displays basic statistics about memory, flow, and transferred bytes
- SysInfo

In addition, the ProxySG Admin Console shows UDP Tunnel service information in **Reports > Traffic Details**.

More Information:

- *Command Line Interface Reference*
- *SGOS Administration Guide*
- *SGOS Administration Guide (Admin Console Edition)*

Support for Parallel DNS Lookups (Happy Eyeballs)

You can enable or disable parallel DNS lookups using RFC8305 (Happy Eyeballs algorithm). The algorithm allows parallel connections, which avert delays that might occur with serial connection attempts. To support this feature, the following CLI command was added:

```
# (config general) parallel-connect {attempt-delay [<10-10000> | default] | enable |
disable}
```

Use this command to enable parallel connections and configure its settings globally. By default, parallel connections are disabled.

To override the global enable/disable setting, use the following property:

```
server.connection.parallel_connect(yes|no)
```

More Information:

- *Command Line Interface Reference*
- *Web Visual Policy Manager Reference*
- *Content Policy Language Reference*

New http.response Policy Gesture

The following property has been added to force the appliance to stop waiting for HTTP response data from the client:

```
 http.response.response_data.prevent_inspection_delay(yes|no)
```

More Information:

- *Content Policy Language Reference*

New Policy Action for SOCKS Requests

To ensure that SOCKS requests use cached surrogate credentials for authentication, a new `socks.authenticate.mode()` policy action has been added. Use this policy instead of `authenticate.mode()` for SOCKS requests. The policy supports the `proxy` and `proxy-ip` challenge type and surrogate credential.

For example:

```
 <proxy> client.protocol=socks
   socks.authenticate(testrealm) socks.authenticate.mode(proxy-ip)
```

More information:

- *Content Policy Language Reference*
- KB Article 166657

ProxySG ICAP Enhancements

ProxySG and DLP integration is improved. You can configure the ICAP service to send additional request headers to the ICAP server, and add more ICAP server and service information to access logs.

Information in ICAP requests from the ProxySG appliance to the ICAP server

You can now send the following header information in ICAP requests from the ProxySG appliance:

```
#(config icap service_name)send server-country
#(config icap service_name)send threat-risk-level
#(config icap service_name)send url-categories
```

Additional headers are sent in ICAP requests with the existing commands:

- `#(config icap service_name)send authenticated-groups` includes the `X-SYMC-Groups` header.
- `#(config icap service_name)send authenticated-users` includes the `X-SYMC-Users` and `X-SYMC-User-Email-Address` headers.

ICAP server and ICAP service information in access logs

The following access log fields have been added to help identify ICAP servers and services:

- `cs-icap-host`
- `cs-icap-ip`
- `cs-icap-service`
- `rs-icap-host`
- `rs-icap-ip`
- `rs-icap-service`

More Information:

- *Command Line Interface Reference*
- *ProxySG Log Fields and Substitutions*

This release introduces new policy conditions that you can use in CPL to trigger ICAP notifications based on content in ICAP-scanned requests and responses.

Use the conditions to specify the service that identified the threat in the scanned request or response:

- `request.icap.threat_source=`
- `request.icap.threat_source.exists=`
- `response.icap.threat_source=`
- `response.icap.threat_source.exists=`

Use the conditions to specify an identifier of the threat detected in the scanned request or response:

- `request.icap.threat_id=`
- `request.icap.threat_id.exists=`
- `response.icap.threat_id=`
- `response.icap.threat_id.exists=`

Use the conditions to specify details detected in the scanned request or response:

- `request.icap.threat_details=`
- `request.icap.threat_details.exists=`
- `response.icap.threat_details=`
- `response.icap.threat_details.exists=`

Use the conditions to specify whether or not a threat was detected in the scanned request or response:

- `request.icap.threat_detected=`
- `response.icap.threat_detected=`

Use these conditions instead of `virus_detected=` , which is now deprecated.

Deprecations

Refer to the Upgrade/Downgrade Guide for a list of all policy, log fields, and substitutions that are deprecated with the introduction of this new policy.

HTTP Enhancements

This release includes the following HTTP enhancements:

Cached HTTP/1.1 Session Timeout for HTTP/2 Client Sessions

For an HTTP/2 client session, the cached server-side HTTP/1.1 connections expire and are removed from cache if they exceed the threshold specified in the existing `# (config) http persistent-timeout client seconds` setting. Connections that are closed on the server side are removed from cache regardless of the timeout setting..

New HTTP/2 Connection and Stream Counts in the Heartbeat Report

New counters have been added to the heartbeat report for HTTP/2 connections and streams.

Explicit Congestion Notification (ECN) Support

The following commands were added to support ECN:

```
#(config)tcp-ip ecn {disable | receive-only | send-receive}
```

You can specify `receive-only` to respond to inbound ECN notifications, or `send-receive` to request outbound and receive inbound ECN notifications. By default, ECN is disabled.

More Information:

- *Command Line Interface Reference*

Web Isolation Enhancement

The Web Isolation service is enabled by default. If you have configured your custom web isolation service with forwarding hosts, you can now disable the Web Isolation service to allow forwarding-based isolation to work as intended. Use the following CLI:

```
#(config isolation)disable
```

CAUTION
Before disabling the Web Isolation service, you must first uninstall any existing Web Isolation policy. Disabling the service before removing the policy will return exception pages for traffic matching the isolation policy rules.

To re-enable the service, use the CLI:

```
#(config isolation)enable
```

Make sure that the Web Isolation service is enabled before configuring Web Isolation policy; otherwise, policy compilation warnings occur, such as "Warning: 'isolate' Isolation service is disabled; it must be enabled in order to use the isolate action using the CLI isolation->enable command".

The output of the `#show isolation` and `#(config)isolation view` commands display the status of the service.

More Information:

- KB 201609

Improved Security for Local User Passwords

New commands have been added to improve security of local user passwords:

```
# (config local-user-list local_user_list) inactivity-lockout
```

```
number_of_days
```

Specify how long an account can be inactive before it is locked out. Accepted values are between 0 and 365. The default is 0, which disables the setting (there is no inactivity period).

You can use the existing `# (config local-user-list local_user_list user_name)` **`enable`** command to reset the inactivity-lockout period for an expired password.

```
# (config local-user-list local_user_list) max-password-age
number_of_days
```

Specify the maximum age of a password. Accepted values are between 0 and 365. The default is 0, which disables the setting (there is no maximum age).

```
# (config local-user-list local_user_list user_name) password-grace
number_of_days
```

Provide the user with a grace period in which they can change their expired password. Accepted values are from 1 to 5.

More Information:

- *Command Line Interface Reference*

TLS 1.3 Offload Support

TLS 1.3 offload support for SSLV was disabled in version 7.2.2.1. The feature is restored in this release.

Removal of Custom Diffie-Hellman Groups

For better security, custom Diffie-Hellman groups have been removed from TLS cipher suites.

Timezone Database Update

The timezone database has been updated to reflect changes in Release 2021a of the IANA timezone database.

Support for New Network Interface Card

The Silicom bypass driver has been updated to support the PE310G4BPI40-T Quad port Copper 10 Gigabit Ethernet PCI Express Bypass Server Intel® x540 Based card.

New Maximum High Memory Threshold for Cloud Deployments

For ProxySG virtual appliances deployed in the cloud with Enterprise and Node-Locked licenses, the thresholds for high memory pools have been increased to 1600 MB.

Increased Maximum Number of NICs on Virtual Appliances

The following types of ProxySG virtual appliances now support more virtual interfaces:

Platform	Maximum NICs
AWS	8
Azure	8
GCP	8
Hyper-V	8
KVM	16

Platform	Maximum NICs
VMware	10
Xen	8

Fixes in SGOS 7.3.4.1

SGOS 7.3.4.1 includes the following bug fixes.

Table 298: Access Logging

ID	Issue
SG-26885	Fixes an issue where Kafka uploads failed if a cluster had many nodes.

Table 299: Admin Console

ID	Issue
SGAC-2841	Fixes an issue where selections for sending service information (**Administration > Service Information > Send Information**) were not displayed.
SGAC-2764	Fixes an issue where the Instant Save function did not work when entering Kerberos credentials in an IWA realm configuration.
SGAC-2763	Fixes an issue where updated values in the **Timeout request after** field were not saved in an IWA realm configuration.
SGAC-2702	Fixes an issue where disabling the **Prefix IDP cookies** setting in a SAML realm did not take effect after saving the configuration.
SGAC-2702	Fixes an issue where showing **Advanced Settings** in an IWA realm displayed console errors.
SGAC-2693	Fixes an issue where the console erroneously reported conflicting proxy service listeners on the appliance.

Table 300: Authentication

ID	Issue
SG-26727	Fixes an issue where the appliance stopped responding during LDAP realm destruction while attempting to clean up a cached network socket used for LDAP searches.
SG-26994	Fixes an issue where the appliance was unresponsive due to incorrectly prioritizing certain processes.

Table 301: CLI Consoles

ID	Issue
SG-25897	Fixes an issue where sometimes a kex protocol error would occur when running CLI commands.

Table 302: Cloud Platform

ID	Issue
SG-26843	Fixes an issue where ZTP did not successfully set up an appliance.

Table 303: DNS Proxy

ID	Issue
SG-25261	Fixes an issue where the appliance experienced a restart when attempting to free a pointer it had already freed.

Table 304: Health Monitoring

ID	Issue
SG-25858	Fixes an issue where the Policy Services Communication Status was in a critical state after upgrading an appliance with the MACH5 license to version 7.3.x. Previously, Policy Services was disabled by default for some license types; now, it is enabled and available for all license types.

Table 305: HTTP Proxy

ID	Issue
SG-26832	Fixes an issue where web isolation forwarding did not work if the appliance was upgraded from version 6.7.x to 7.3.2.
SG-25593	Fixes an issue where protocol detection did not detect HTTP/2 when a server response was received before the client connection. When this issue occurred, the log displayed "Cannot detect server speakfirst protocol".

Table 306: Kernel

ID	Issue
SG-25602	Fixes an issue where Secure Web Gateway virtual appliances running on Microsoft Azure platforms stopped responding.

Table 307: Policy

ID	Issue
SG-26413	Fixes an issue where policy coverage reports showed inaccurate 'true' counts for unconditional rules in scheduled layers (such as time denials and access logging).
SG-25137	Fixes an issue where the appliance could not rewrite URLs that had empty HTML comments preceding them.

Table 308: Security

ID	Issue
SG-25886 SG-25487	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.

Table 309: SOCKS Proxy

ID	Issue
SG-25580	Fixes an issue where SOCKS requests failed due to not being matched to the IP surrogate credential. This fix requires using the new `socks.authenticate.mode()` , policy action, as described in Features in SGOS 7.3.4.1.

Table 310: SSL Proxy

ID	Issue
SG-23430	Fixes an issue where the appliance experienced high memory usage. This issue occurred in reverse proxy mode with `#(config service_name)attribute forward-client-cert` enabled and Certificate Policies extensions in use.

Table 311: SSL/TLS and PLI

ID	Issue
SG-25640	Fixes an issue where the appliance became unresponsive when loading a trust package.
SG-25818	Fixes an issue where the appliance experienced a restart when attempting to install HSM configuration.

Table 312: TCP/IP and General Networking

ID	Issue
SG-26111	Fixes an issue where users experienced slow loading pages or pages not loading due to high memory utilization in TCP/IP.
SG-10571	Fixes an issue where the appliance dropped fragmented IPv6 NDP packets.
SG-26509	Fixes an issue where the ProxySG applications restarted frequently due to encrypted tap sessions not closing correctly.
SG-25552	Fixes an issue where IPv6 UDP did not track destination addresses correctly.
SG-27101	Fixes an issue where the appliance stopped responding due to a bypassed connection with fragmented packets, which had no TCP header.
SG-27115	Fixes an issue where adding NICs to a virtual appliance running on VMware ESXi changed the order of NICs.
SG-25955	Fixes an issue where the appliance experienced a restart due to the appliance marking the mbuf with a weak INP.
SG-26308	Fixes an issue where a DHCP vulnerability could allow an attacker to cause the appliance to restart.
SG-25947	Fixes an issue where the appliance experienced a restart when the appliance had many items in the queue for the stack-ip-forward worker.

Table 313: URL Filtering

ID	Issue
SG-25492	Fixes an issue where purging the databases of Intelligence Service subscription services changes the previously configured download method.

Table 314: Web Application Firewall

ID	Issue
SG-25723	Fixes an issue where interactions between `http.request.log.mask_by_name()` and `http.request.detection.bypass_cache_hit()` policy properties sometimes resulted in the appliance not decoding the URLs of payloads during internal analysis.
SG-26127	Fixes an issue where the SQL injection engine incorrectly blocked some Chrome headers.

SGOS 7.3.3.3 PR

Release Information

- Release Date: June 28, 2021
- Build Number: 263824

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION
  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.3.3

- This release includes various fixes. See Fixes in SGOS 7.3.3.3.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.3.3

Table 315: Security

ID	Issue
SG-27187	Fixes a security vulnerability. For more information, see SYMSA18331.

SGOS 7.3.3.2 PR

Release Information

- Release Date: May 20, 2021
- Build Number: 262454

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION
  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable

FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After upgrading, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.3.3.2

- This release includes various fixes. See Fixes in SGOS 7.3.3.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.3.3.2

SGOS 7.3.3.2 includes the following bug fix.

Table 316: SSL/TLS and PKI

ID	Issue
SG-25328	Fixes an issue where the appliance would experience a restart when the appliance parsed all PSK extensions regardless of the maximum TLS version for the client.

SGOS 7.3.3.1 GA

Release Information

- Release Date: April 28, 2021
- Build Number: 261578

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION

  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2 and later, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.3.1

- SGOS 7.3.3.1 introduces new features and enhancements. See Features in SGOS 7.3.3.1.

Fixes in ProxySG 7.3.3.1

- This release includes various fixes. See Fixes in SGOS 7.3.3.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.3.1

SGOS 7.3.3.1 introduces the following new features:

Integrated Secure Gateway Enterprise Secure Web Gateway Virtual Appliance

A new Integrated Secure Gateway (ISG) Enterprise Secure Web Gateway Virtual Appliance (SWG VA) license is supported for ProxySG VAs running on VMware's vSphere Hypervisor. The ISG Enterprise SWG VA facilitates server consolidation by co-existing with other virtual machines on a single hardware platform, including Symantec Content Analysis. With the ISG SWG VA providing security, the other virtual machines can provide branch office services (such as Domain Controller, print, DNS, and DHCP), as well as any VMware-certified software applications.

For more information, refer to the *Integrated Secure Gateway Enterprise Secure Web Gateway Virtual Appliance Deployment Guide*.

New HTTP/2 Connection and Stream Counts in the Heartbeat Report

New counters have been added to the heartbeat report for HTTP/2 connections and streams.

Policy Optimizations

Hashed Conditions in Executable Policy

A new command has been added to enable or disable policy hash optimizations:

```
# (config) policy optimize-hash
```

The command applies to the`url.domain=` and `server_url.domain=` conditions. When enabled, lists of `url.domain=` , and `server_url.domain=` conditions, and various subnet and substitution conditions are transformed into a hashed condition in executable policy.

The following command was introduced in version 7.3.1:

```
# (config) policy optimize-tautology
```

When enabled, conditions that are determined to be constantly true or constantly false at compilation time are not evaluated (they still appear in executable policy).

Policy Compilation Improvement

Compilation of policy that includes many `user=` conditions is improved. The policy compiler now optimizes `user=` conditions into groups of case-sensitive and case-insensitive realms. A minimum of five qualifying conditions is required for optimization into a group.

> **NOTE**
> Conditions that have variable criteria, such as substitutions rather than strings, are not optimized.

For more information, refer to the *Command Line Interface Reference* documentation.

Web Visual Policy Manager Enhancements

This release includes the following web VPM enhancements:

Management Center Roles and Permissions

Management Center administrators can assign permissions to users, which determine whether users can:

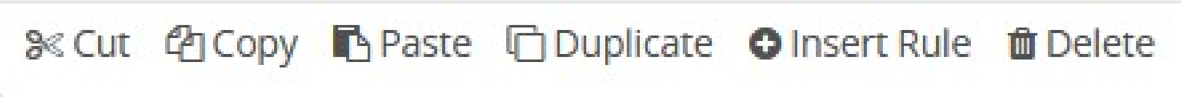
- View, add, edit, and delete policy layers.
- View, add, edit, and delete policy layer guards.
- View, add, edit, and delete policy rules.
- View, add, edit, and delete specific VPM objects.
- View and use the following options in the Operations menu: **Change Enforcement Domains**, **View All Objects**, **View Generated CPL**.

Improved Look and Feel

- The **Update policy** menu option to refresh generated CPL has been replaced with a 'refresh' icon:

  🔄

  . When you use the icon to refresh the CPL, the VPM notifies you of the change with a message, "Successfully refreshed generated CPL."
- All policy rule menu options now have icons:



Fixes in SGOS 7.3.3.1

SGOS 7.3.3.1 includes the following bug fixes.

Table 317: Access Logging

ID	Issue
SG-25675	Fixes an issue where an existing access log facility could not be deleted.

Table 318: Authentication

ID	Issue
SG-25138	Fixes an issue where the appliance stopped responding after writing some `<admin>` layer policy.
SG-25860	Fixes an issue where the appliance had a hardware exception when the XML authentication realm contained a parsing issue.

Table 319: Cache Engine

ID	Issue
SG-25363	Addresses potential denial of service attacks when there was a high number of simultaneous URL-based searches in /CE/Listing_Form.

Table 320: CLI Consoles

ID	Issue
SG-25564	Fixes an issue where attempting to view Advanced URLs results in an "Encrypted token has expired" message. This issue occurred when logging in to the console with a non-local admin user.

Table 321: Health Monitoring

ID	Issue
SG-23967	Fixes an issue where the appliance stopped responding when starting up in standalone mode.

Table 322: HTTP Proxy

ID	Issue
SG-22988	Fixes an issue where requests including both the Content-Length and Transfer-Encoding headers were forwarded to the OCS. Now, the Transfer-Encoding: identity header is removed from such requests before being forwarded.
SG-25957	Fixes an issue where users cannot access alldata.com after an upgrade to version 7.3.
SG-25953	Fixes an issue where the appliance had a software exception when policy included `ssl.forward_proxy(yes)` and a deferred transaction was denied.
SG-25612	Fixes an issue where protocol detection failed to detect HTTPS with TLS 1.3 post handshake messages, and the HTTP logs contained "Cannot detect server speakfirst protocol" messages.

Table 323: ICAP

ID	Issue
SG-19774	Fixes an issue where "Request timed out" errors were incorrectly reported when ICAP connections were closed on the server side. Now, the ICAP error states "Failed due to dropped connection".

Table 324: Kernel

ID	Issue
SG-19721	Fixes an issue where the appliance stopped responding when there was a high number of HTTP/S connections on the appliance.

Table 325: Management Console

ID	Issue
SG-25199	Fixes an issue where the Management Console exited with an error message, "SSL protocol negotiation failed. Logging out from Management Console".

Table 326: Policy

ID	Issue
SG-25255	Fixes an issue where the Management Console exited with an error message, "SSL protocol negotiation failed. Logging out from Management Console".
SG-25472	Fixes an issue where a `define condition` did not match if it included more than four `user=` conditions.

Table 327: Reverse Proxy

ID	Issue
SG-25442	Fixes an issue where existing forwarding host names could not be edited to exceed 64 characters.

Table 328: SSL/TLS and PKI

ID	Issue
SG-25924	Fixes an issue where the appliance stopped responding after deleting an SSL keyring.

Table 329: SSL Proxy

ID	Issue
SG-13361	Fixes an issue where authentication sessions persisted across browser sessions. Now, users are prompted to authenticate each new browser session.
SG-25006	Fixes an issue where users received an "EXCEPTION(tcp_error): Request could not be handled" message when a site required a client certificate.
SG-25594	Fixes an issue where some SSL tunnel transactions are allowed although they are denied in policy. This issue occurred if protocol detection for SIPS was enabled and policy included deny actions based on response.

Table 330: TCP/IP and General Networking

ID	Issue
SG-24139	Fixes an issue where outgoing connections intermittently went to an incorrect interface.
SG-23835	Fixes an issue where users experienced slow browsing due to a large number of failed DNS lookups on the appliance.
SG-26046	Fixes an issue where the serial console showed error message "Apply__DNS_fwd() ERRO DNS fibnum = 0" when the appliance booted up. The issue occurred because DNS forwarding group names were truncated if they were 16 characters or more in length.

Table 331: URL Filtering

ID	Issue
SG-25892	Fixes an issue where user requests were denied due to a content_filter_denied exception that matched in error. This issue occurred after an upgrade from version 7.2.3.
SG-25752	Fixes an issue where application attributes policy was not enforced. This occurred when application classification or access logging was disabled.

Table 332: Web VPM

ID	Issue
SG-25201	Fixes an issue where the **Combined Time Object** could not be added.
SG-24881, SG-23553	Fixes an issue where adding a **User** source object resulted in a "Cannot read property 'getAttribute' of undefined Retrieving base DN" error. The issue occurred if the LDAP realm was configured without a Base DN.
SG-20718	Fixes an issue where editing an IP address list in an object (such as **Send DNS Response**) immediately returned an inaccurate "IP address already exists" error.
SG-23981	Fixes an issue where authenticated users were allowed to access the HTTPS-Console service even though the Management Console login banner (Notice and Consent Banner) policy was configured in the web VPM. This occurred if CPL policy layers were not ordered correctly.

ID	Issue
SG-21338	Fixes an issue where comparing generated CPL with deployed CPL incorrectly indicated differences between the two policies.
SG-23229	Fixes an issue where configured HSM keyrings were not available in the web VPM.
SG-21638	Fixes an issue where the **Allow user to override read-only** option in the **Web Isolation** object was not indented. It is now indented to indicate that it requires the preceding **Read-only, prevent user from entering data** option to be selected.

SGOS 7.3.2.1 GA

Release Information

- Release Date: March 3, 2021
- Build Number: 259959

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION
  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.x might cause unexpected behavior with configured HSMs. See SG-23171 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.x. If you begin upgrading to 7.3.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.x without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.3.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- When upgrading to version 7.3.2, the HTTPS console cipher suites configuration is preserved. In addition, the following TLS 1.3 high-strength cipher suites are enabled by default:
  - tls_aes_256_gcm_sha384
  - tls_chacha20_poly1305_sha256
  - tls_aes_128_gcm_sha256
  - tls_aes_128_ccm_8-sha256
  - tls_aes_128_ccm_sha256
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.3.x from an earlier version 7.x or from version 6.7.4.4 or later. If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.
  - Downgrade from 7.3.x to an earlier version 7.x or to version 6.7.4.4 or later.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.2.1

- SGOS 7.3.2.1 introduces new features and enhancements. See Features in SGOS 7.3.2.1.

Fixes in ProxySG 7.3.2.1

- This release includes various fixes. See Fixes in SGOS 7.3.2.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.2.1

SGOS 7.3.2.1 introduces the following new features:

Zero Touch Provisioning for ProxySG Deployments

Zero Touch Provisioning (ZTP) allows you to easily deploy ProxySG appliances or virtual appliances without using the terminal to configure the deployment. Instead, you prepare a ZTP payload containing the configuration and environment details, and provide the payload to the appliance. Additionally, if you are using Management Center to manage your appliances, ZTP can automatically register the appliance with Management Center.

> **NOTE**
> ZTP can only be performed on an appliance that is in a factory-reset state.

ZTP is available for all physical ProxySG S-series appliances and the following virtual platforms:

- AWS
- Azure
- Cisco Cloud Services Platform
- ESXi
- KVM
- Microsoft Hyper-V

> **NOTE**
> ZTP is not currently available for ProxySG applications running on Integrated Secure Gateway.

ProxySG Admin Console 1.2.1

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

Proxy Protocol Support

The DNS, HTTP, HTTPS, RTSP, SOCKS, SSL, TCP, and Telnet services now include an **Expect Proxy Protocol** option.

When enabled, the appliance looks for the originating IPv4 or IPv6 addresses in the Proxy Protocol request header. If Proxy Protocol is supported on the OCS and available, the proxy then includes the originating address in the request.

The IP address is used for the effective client IP address in policy; refer to the *Visual Policy Manager Reference* or *Content Policy Language Reference* for more information.

When **Expect Proxy Protocol** option is enabled and Proxy Protocol is not supported on the OCS or is unavailable, the request header is unchanged.

In the CLI, configure Expect Proxy Protocol with the following command:

```
# (config proxy_service_name) attribute expect-proxy-protocol {disable | enable}S
```

To learn about the Proxy Protocol, refer to https://www.haproxy.org/download/1.8/doc/proxy-protocol.txt.

Full information:

- *SGOS Administration Guide*
- *Command Line Interface Reference*

Proxy Service Drop and Reject Actions

- Proxy service listeners now support two more default actions:

- `# (config proxy_service) drop [all|<source_ip>|<source_ip/subnet_mask>] transparent|explicit|all|<destination_ip>|<destination_ip/subnet_mask> <port>|<first_port>-<last_port>`
  Silently drop matching incoming packets.
- `# (config telnet_proxy_service) reject [all|<source_ip>|<source_ip/subnet_mask>] transparent|explicit|all|<destination_ip>|<destination_ip/subnet_mask> <port>|<first_port>-<last_port>`
  Respond to the sender indicating that the packet was rejected.

These actions are added to the DNS, FTP, FTPS, HTTP, HTTPS reverse proxy, MMS, SOCKS, SSL, TCP Tunnel, and UDP Tunnel proxy services.

Full information:

- *Command Line Interface Reference*

UDP Proxy Enhancements

This release supports a UDP-Tunnel proxy service, which allows basic visibility and control of UDP flows through the appliance.

Use the following CLI:

```
# (config proxy-services)
# (config proxy-services) create udp-tunnel
udp_proxy_service [service_group]
# (config proxy-services) edit
udp_proxy_service
```

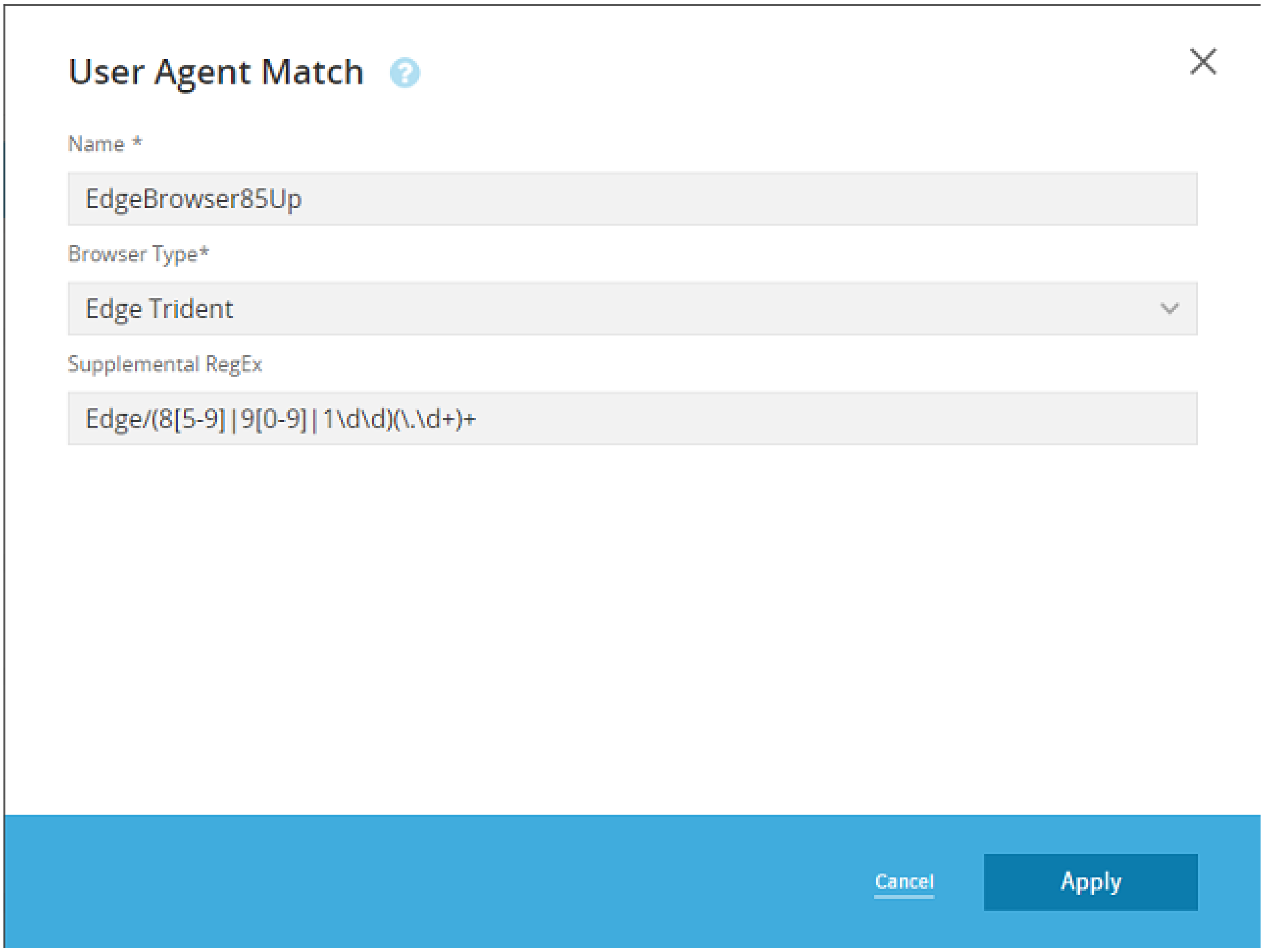
You can add listeners to the UDP proxy service and set listener actions to bypass, drop, or reject.

Full information:

- *Command Line Interface Reference*

User Agent Match Object for Web VPM

A new **User Agent Match** Web Visual Policy Manager (VPM) object has been added for the existing `request.header.User-Agent=` CPL condition. Use the object to test the User-Agent request header: select a browser from a list and optionally specify a regular expression for the type and version.



User Agent Match

Name *

EdgeBrowser85Up

Browser Type*

Edge Trident

Supplemental RegEx

Edge/(8[5-9]|9[0-9]|1\d\d)(\.\d+)+

Full information:

- *Web Visual Policy Manager Reference*

Diagnostic Probe Enhancements

The define probe definition has the following enhancements:

- The existing `limit` attribute is now tenant-specific when the probe definition is included in the tenant policy file.
- The new `limit.reset` attribute resets the diagnostic probe limit after the specified number of seconds. If unspecified, the diagnostic probe does not reset.

Refer to the following example of usage:

```
define probe case123
  condition=my_traffic_selection
  scope=session
  target=http:debug,ssl:all
  policy_trace=yes
  limit=10
  limit.reset=10
  expiry=20220101:2350
end
```

New Trace Logging Level

A new trace logging level has been added:

```
#(config event-log)level trace
```

Full information:

- *Command Line Interface Reference*

Absolute Management Console Session Timeout

A new command allows you to enable or disable an absolute timeout for all Management Console sessions:

```
#(config)security management [no] absolute-web-timeout <minutes>
```

where *minutes* is a value from 15 to 43200.

The appliance terminates all Management Console sessions after the specified timeout period. For best security, use this command to require users to re-authenticate to the Management Console after the timeout.

Full information:

- *Command Line Interface Reference*

Clear the Serial Number When Restoring Factory Defaults

You now have the option to clear virtual appliance serial numbers when restoring factory defaults:

```
# restore-defaults factory-defaults [clear-va-serial]
```

HTTP/2 Enhancements and Changes

This release includes the following HTTP/2 enhancements and changes:

- HTTP/2 response headers up to 1 MB are supported.
- HTTP/2 responses with large headers no longer cause an error.
- The default value of `http2.client_max_concurrent_streams()` is changed to 0. The previous default was 100 (according to bug) or 15 (according to CLI guide)
- The `http2.client.accept()` property does not apply when it is guarded with `client.connection.ssl_server_name=` for HTTPS reverse proxy transactions.

TCP/IP Enhancements and Changes

This release includes the following TCP/IP enhancements and changes:

- You can use the following command to specify the algorithm to use for TCP congestion avoidance:
  ```
  # (config) tcp-ip congestion-algorithm {cubic | htcp | newreno}
  ```
- IPv4 Path MTU Discovery support has been updated to reflect latest standards.
- The appliance has improved detection of out-of-order packets, allowing throughput to remain high.
- The appliance supports RFC2883, which extends TCP SACK support.

DNS Transaction Access Log Fields

The following access log fields were added to help track HTTP transaction times:

- `x-client-dnslookup-time` : Total time taken (in ms) to perform the client DNS lookup.
- `x-server-dnslookup-time` : Total time taken (in ms) to perform the server DNS lookup.

New HTTP Dwell Time Statistics

The following counters have been added for dwell time statistics:

- Transactions performing static and dynamic categorization
- Transactions performing authentication and authorization, and server authentication
- Transactions performing various upstream, downstream, and reverse proxy handshakes
- Transactions determining object disposition
- Transactions performing DNS lookup for clients and servers

Troubleshooting Improvements

- HTTP/2 connection and stream counters have been added to the heartbeat report.
- Port numbers are now available in the policy trace output.
- Kerberos 5 replay attack error messages in the event log now include the client IP address.

Other Enhancements and Changes

- You can now view your entitlements via the Management Console. Select **Maintenance > Licensing > Install** and click **View Entitlements**. The console opens the MyBroadcom portal, where you can log in with your MyBroadcom credentials. **View Entitlements** replaces the previous **Register/Manage** option.
- For best security, CBC cipher suites are now disabled by default for the HTTPS management console.
- Performance is improved when bridging packets on machines with more than 8 cores.
- Performance of dynamic bypass and asymmetric bypass are improved when higher maximum entries are configured.
- Protocol detection is now enabled by default when:
  - Creating a new HTTP/S proxy service and on new installations
  - Performing a `restore-defaults`

  The protocol detection setting on existing built-in and user-defined HTTP/S proxy services persists after an upgrade.

Deprecations and Removals

- This release removes support for Space Communications Protocol Specification (SCPS). The `# (config)` **`tcp-ip scps`** commands are no longer available.
- The following commands were removed:

  ```
  # (config) tcp-ip tcp-loss-recovery-mode {aggressive | enhanced | normal}
  # (config) tcp-ip tcp-newreno {disable | enable}
  ```

  These commands are replaced by `# (config)` **`tcp-ip congestion-algorithm`** ; see **TCP/IP Enhancements and Changes** for information.
- Support for Novell SSO, CA eTrust SiteMinder, and Oracle COREid authentication realms is deprecated. You can no longer configure new or existing realms through the Management Console; you can configure existing realms through the CLI.

Fixes in SGOS 7.3.2.1

SGOS 7.3.2.1 includes the following bug fixes.

Table 333: Access Logging

ID	Issue
SG-22694	Fixes an issue where the appliance restarted due to multiple log upload threads attempting to simultaneously initialize the SSL cryptographic parameters.
SG-18288	Fixes an issue where access logs using a custom log format could not be uploaded using the Kafka client to the broker.
SG-24708	Fixes an issue where the HTTP transaction timing fields (x-cs-rp-https-handshake-time, x-cs-https-handshaketime, and x-sr-https-handshake-time) in the access log generated a "-" or a "0" in log output regardless of the latency from the client or server.

Table 334: Admin Console

ID	Issue
SGAC-2591	Fixes an issue where the console did not reflect changes to the **User Overflow Action** option in General Proxy Settings.
SGAC-2577	Fixes an issue where offline download could not be configured for the geolocation database.
SGAC-2574	Fixes an issue where `net 10.10.10.10/24` could not be saved as a packet capture filter expression.
SGAC-2446	Fixes an issue where disabled fields in the Admin Console did not appear to be disabled. Disabled fields now look disabled, consistent with behavior in the Management Console.
SGAC-2306	Fixes issues with Windows Domain configuration: • The console no longer incorrectly indicates that there are no changes to be saved. • When joining a domain, the console now shows that the operation is in progress.

Table 335: Authentication

ID	Issue
SG-17630	Updates the Kerberos open-source library to resolve multiple security vulnerabilities.
SG-23878	Addresses an issue where authenticated users were allowed to access the HTTPS-Console service even though the Management Console login banner (Notice and Consent Banner) policy was configured in the VPM. This issue occurred if CPL policy layers were not ordered correctly.
SG-23208	Fixes an issue where the appliance experienced high memory usage in HTTP policy evaluation.
SG-22754	Fixes an issue where users received "Appliance Error (configuration_error). Your request could not be processed because of a configuration error. 'User has been logged out.'" This issue occurred when surrogate credentials expired with SAML authentication.
SG-21796	Addresses an issue where the appliance experienced a page fault (error code 0x4) within process "libauthenticator.exe.so" (0x40015).
SG-23983	Fixes an issue where the appliance experience high CPU and memory consumption due to fragmentation in bget heap.
SG-23880	Addresses an issue where the appliance restarted after memory was released for an invalid memory pointer.
SG-23666	Fixes an issue where the web VPM session persisted without user re-authentication after the Management Console session expired according to the `#(config) security management absolute-web-timeout` setting.
SG-23644	Fixes an issue by adding the IP address of the client to the event log message when the appliance receives a Krb5 replay error.

Table 336: Cache Engine

ID	Issue
SG-23589	Fixes an issue where the appliance restarted due to the appliance not re-evaluating entries in the hash table.

Table 337: FTP Proxy

ID	Issue
SG-4624	Fixes an issue where the `s-action` access log field was sometimes not populated.

Table 338: Health Checks

ID	Issue
SG-22815	Fixes a timing issue where the appliance stopped responding when modifying an access log facility.
SG-23269	Fixes an issue where a restart occurred in a forward proxy deployment that included HSMs.

Table 339: HTTP Proxy

ID	Issue
SG-18817	Fixes an issue where the browser did not display full exception details when the default policy was set to deny and the TCP Tunnel service had protocol detection enabled.
SG-20969	Addresses an issue where the appliance experienced a restart in the HTTP process when reading a response from ICAP.
SG-23441	Fixes an issue where some webpages would not render correctly when an SSL Visibility appliance was decrypting traffic.
SG-14408	Fixes an issue where Websocket tunnels inflated some HTTP transaction time statistics.
SG-22779	Addresses an issue where the appliance experienced a restart after receiving an invalid request when using HTTP/2 and SSLV offload.
SG-23197	Addresses an issue where the appliance experienced a restart when there were multiple concurrent HTTP/2 requests and the web server closed the connection.
SG-23178	Fixes an issue where the limit set in `http2.client.max_concurrent_streams()` did not apply immediately to new HTTP/2 connections.
SG-20158	Fixes an issue where certain ICAP threads were not terminated and caused memory leaks.
SG-24969	Fixes an issue where browsing to facebook.com returned error 502: Content Encoding Error.
SG-22988	Fixes an issue where requests including both the Content-Length and Transfer-Encoding headers were forwarded to the OCS. Now, the Transfer-Encoding: identity header is removed from such requests before being forwarded.

Table 340: ICAP

ID	Issue
SG-23811	Fixes an issue where the response time for health checks was longer than expected when the appliance was sending Content Analysis traffic to the ICAP broker.

Table 341: Management

ID	Issue
SG-24442	Fixes an issue where upgrading from version 6.7.4 to 7.2 did not preserve the previous non-default HTTPS console ciphers configuration or enable TLS 1.3 by default. This issue occurred if non-default SSL protocols were selected for the HTTPS console. If the appliance was never upgraded to 7.2.x or 7.3.x previously, upgrading to this release preserves the previous ciphers selection and enable TLS 1.3 by default. To apply the fix if the appliance was previously upgraded to 7.2.x or 7.3.x, you must remove the existing SGOS 7.x configuration before upgrading. Issue the #**`remove-sgos7-config`** command, restart the appliance, and then install this release.

Table 342: Performance

ID	Issue
SG-21976	Fixes an issue where ProxySG instances running on Hyper-V and Azure experienced a 20% reduction in traffic throughput. The issue occurred after changes were made to the Hyper-V paravirtual network driver in version 7.2.2.

Table 343: Policy

ID	Issue
SG-21244	Fixes an issue where exception pages rendered incorrectly when they were larger than 8000 bytes.
SG-24326	Fixes an issue where accessing the /dme/configuration advanced URL caused the license key auto-update feature to be enabled when it was originally set to disabled.
SG-24288	Fixes an issue where authenticating traffic using NTLM with BCAAA did not work.

Table 344: Proxy Forwarding

ID	Issue
SG-23369	Fixes an issue where forwarding groups did not balance the load equally when members of the group were in a failure state.

Table 345: Security

ID	Issue
SG-24232	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.

Table 346: SSL/TLS and PKI

ID	Issue
SG-24065	Fixes an issue where the appliance incorrectly listed the DHE-DSS-DES-CBC3-SHA cipher strength as High instead of Medium.
SG-24931	Fixes an issue where revoked intermediate certificates were added to the cached intermediate certificate list.
SG-24947	Addresses an issue where the appliance experienced a restart when multiple SSL connections are opened. The issue occurred due to changes made for SSL session ticket support in version 7.3.1.

Table 347: SSL Proxy

ID	Issue
SG-22312	Fixes an issue where a memory leak occurred when MS-TURN traffic was detected.
SG-23828	Fixes an issue where the appliance experienced a memory leak when handling HTTPS reverse proxy traffic with forward-client-cert enabled.
SG-2311	Fixes an issue where cached intermediate CA certificates caused certificate expiration errors even when the certificate expiration date was updated. Now, the certificate with an updated expiration date replaces the certificate in the cache.
SG-23380	Fixes an issue where `server.certificate.validate.ccl()` did not apply to SSL tunnel transactions.
SG-23117	Fixes an issue where handshake failure occurred when using Java applications. This issue occurred if TSL 1.3 was enabled and protocol detection was disabled on the appliance.

Table 348: TCP/IP and General Networking

ID	Issue
SG-24546	Addresses an issue where a restart occurred when Routing Information Protocol (RIP) was in use.
SG-24706	Addresses an issue here a restart occurred when a packet capture was initiated from the ProxySG Admin Console that included a large filter expression.
SG-24034	Fixes an issue where the appliance did not indicate that WCCP did not start after a reboot. Now, when WCCP does not start after a reboot, error messages are logged in the debug log.
SG-24810	Fixes an issue where the appliance experienced a restart when an HTTP/2 transaction could not be completed due to a null socket.
SG-24291	Fixes several implementation issues in dynamic bypass and asymmetric bypass that might have led to a restart.

Table 349: URL Filtering

ID	Issue
SG-24231	Fixes an issue where the appliance experienced a restart when testing a URL category in the format of an email address (for example, "/ContentFilter/TestUrl/testuser@broadcom.com").
SG-23245	Fixes an issue where a requested URL matched policy for "None" category even though the URL was categorized in the local database.
SG-20587	Fixes an issue where categorization timing information was not displayed correctly in the access log.

Table 350: Web VPM

ID	Issue
SG-15678	Fixes an issue where checkboxes in VPM objects such as **Combined Source** were editable in read-only mode.
SG-21623	Fixes an issue where the **Operations** menu option incorrectly read **Enable Enforcement Domains** when enforcement domains were enabled. The menu option now says **Disable Enforcement Domains** when the feature is enabled.
SG-20679	Fixes an issue where adding a **DNS Request Threat Risk Level** object resulted in an error, "Please ensure that you have enabled Threat Risk Levels" even though the Threat Risk Levels service was enabled.
SG-21942	Fixes an issue where adding a User object with an LDAP realm selected prepended "cn=" to the Full Name field.
SG-15678	Fixes an issue where checkboxes in VPM objects such as **Combined Source** were editable in read-only mode.

ID	Issue
SG-20679	Fixes an issue where adding a **DNS Request Threat Risk Level** object resulted in an error, "Please ensure that you have enabled Threat Risk Levels" even though the Threat Risk Levels service was enabled.
SG-15678	Fixes an issue where checkboxes in VPM objects such as **Combined Source** were editable in read-only mode.
SG-21326	Fixes an issue where the UI incorrectly displayed "Enable Enforcement Domains" when the enforcement domains were already enabled.
SG-21942	Fixes an issue where adding a **User** object with an LDAP realm selected prepended "cn=" to the Full Name field.

SGOS 7.3.1.1 GA

Release Information

- Release Date: November 12, 2020
- Build Number: 256495

NOTE

SGOS is cumulative. SGOS 7.3.1.1 is based on the SGOS 7.2.3.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.7 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION
  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23171 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.3.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.3.1.1. If you begin upgrading to 7.3.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.3.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.3.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.3.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.3.1.1 from an earlier version 7.x or from version 6.7.4.4 or later. If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.
  – Downgrade from 7.3.1.1 to an earlier version 7.x or to version 6.7.4.4 or later.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.3.1.1

- SGOS 7.3.1.1 introduces new features and enhancements. See Features in SGOS 7.3.1.1.

Fixes in ProxySG 7.3.1.1

- This release includes various fixes. See Fixes in SGOS 7.3.1.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.3.1.1

SGOS 7.3.1.1 introduces the following new features:

Symantec Web Isolation

The Symantec Web Isolation solution is a client-less solution that enables and protects users to browse the internet safely on any device using any browser. The zero footprint negates the need for software installation on clients. Starting in SGOS 7.3.x, you can easily configure the ProxySG appliance to send HTTP and HTTPS requests to Symantec Web Isolation.

You can configure the appliance with your existing dedicated cloud or on-premises isolation service. This requires configuration through the command line interface (CLI) and Visual Policy Manager (VPM) or content policy language (CPL) policy.

> **NOTE**
> In the future, the Symantec cloud Web Isolation service will also be available for customers who do not have a dedicated web isolation service.

More information:

- KB article for configuration instructions: https://knowledge.broadcom.com/external/article/201609
- Content Policy Language Reference
- Command Line Interface Reference
- Web Visual Policy Manager Reference

ProxySG Admin Console 1.1.3

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

Policy Coverage Updates

- In previous releases, policy coverage statistics were reset to zero after policy was re-installed. Now, statistics persist after policy re-installations. In a multi-tenant deployment, policy coverage statistics are maintained separately per tenant and persist after tenant policy re-installation.
- In previous releases, policy coverage showed statistics for the policy that is currently installed. Now the feature also shows cumulative statistics that include coverage from previous policy versions.

  Access current statistics at **Statistics > Advanced > Policy > Show Current Policy Coverage** or https://<*ProxySG_IP_address*>:8082/policy/current-coverage.

  Access cumulative statistics at **Statistics > Advanced > Policy > Show Policy Coverage** or https://<*ProxySG_IP_address*>:8082/policy/coverage.

More information:

- How can I find which policy rules are being used?
- Content Policy Language Reference

Policy Compile Behavior Changes

When installing policy (CPL, legacy visual policy, or web visual policy), warnings might appear at compile time to reinforce the following recommendations for accurate policy coverage statistics:

- (CPL only) All policy sections should have labels
- (CPL only) All policy layers should have labels, and policy layers of the same type should have unique labels
- Rules in the same layer can't have the same conditions

If policy contains layers or sections with the same name, installing policy results in the message: "Warning: Coverage may not be consistent across policy versions: duplicate layer/section label". Assign unique labels to layers and sections to easily identify policy rules and ensure the continuity of cumulative policy coverage statistics.

If a policy layer contains rules with identical conditions, installing policy results in the message for the subsequent rule(s): "Warning: Unreachable rule, conditions will be matched by a preceding rule". Make sure that rule conditions are unique, so that policy coverage does not record duplicate statistics.

More Information:

- Content Policy Language Reference
- Web Visual Policy Manager Reference and Legacy Visual Policy Manager Reference

Additional Supported Apparent Data Types

The ProxySG appliance detects more apparent data types in HTTP requests and responses. The following types are now supported in apparent data type CPL properties and conditions:

Table 351: New apparent data types supported in this release

Label	Description	Common Extensions
7ZIP	7-Zip archive	.7z
ACE	ACE archive	.ace
ARJ	ARJ archive	.arj
COMPRESS	compress compressed file	.Z (different from .z)
CPIO	cpio archive	.cpio
DAA	Direct Access Archive	.daa
EGG	EGG archive	.egg
EML	raw email	.eml, .mht, .mhtml
LHA	LHA archive	.lha, .lzh
LZIP	Lzip compressed file	.lz
MACH-O	macOS application or library	
TNEF	file encoded in Microsoft Transport-Neutral Encapsulation Format	.dat, .tnef
UUE	file encoded with uuencode or xxencode	.uu, .uue, .xx, .xxe
XAR	Extensible Archive Format	.mpkg, .pkg, .xar
XZ		.xz

More Information:

- Content Policy Language Reference

Authentication Transaction Trace Logging

The `define probe` CPL definition now supports logging for authentication-related traffic. Use the following syntax:

```
define probe case_label
  condition=condition_label
  target=auth:log_level
  ...
end
```

More Information:

- Content Policy Language Reference

SSL Session Ticket and PSK Support for Session Resumption

In previous releases, the appliance used session ID to resume previously established TLS sessions. For better performance, this release improves SSL session resumption (caching) by using the SSL session ticket and pre-shared key (PSK), as follows:

- TLS connections up to version 1.2 use session tickets
- TLS 1.3 connections use the PSK

To support this feature, the SSL session cache size is doubled, with the following allocations:

- Session ID - 50% of overall cache size
- Session ticket and PSK - 50% of overall cache size

To track the session ticket hashes that the appliance sends or receives when resuming the session, include the following new fields to your access log format:

- `x-cs-session-hash` - SHA256 hash of session ticket issued to or resumed by client for current SSL session
- `x-rs-session-hash` - SHA256 hash of session ticket returned or resumed by server for current SSL session

If you downgrade SGOS , SSL session resumption will use SSL session ID.

> **NOTE**
> This feature is available in forward proxy mode.

More Information:

- SGOS Administration Guide
- ProxySG Log Fields and Substitutions

SSL Session Ticket and PSK Support for Host Affinity

In previous releases, the appliance used session ID to determine host affinity for HTTPS connections. This release supports using the SSL session ticket and PSK for host affinity, as follows:

- TLS connections up to version 1.2 use session tickets
- TLS 1.3 connections use the PSK

When SSL session is selected for host affinity in forwarding/SOCKS host configuration, the appliance dynamically uses the session ID, session ticket SHA256 hash, or PSK hash to make multiple client connections to the same forwarding host/group or SOCKS gateway/group.

In the CLI, the `ssl-session-id` flag is changed to `ssl-session` for the following commands:

```
# (config forwarding) host-affinity ssl ssl-session [host_or_group_alias]
# (config forwarding host_or_group_alias) host-affinity ssl ssl-session
# (config socks-gateways) host-affinity ssl ssl-session [host_or_group_alias]
# (config socks-gateways gateway_or_group_alias) host-affinity ssl ssl-session
```

In the Management Console, the **SSL Session ID** host affinity method in forwarding host and SOCKS gateway configurations is changed to **SSL Session**.

If you downgrade SGOS , hosts and gateways created or modified to use SSL session will use SSL session ID.

> **NOTE**
> This feature is available in forward proxy mode.

More Information:

- ProxySG Log Fields and Substitutions

SNI Hostname Policy

You can create policy that tests the Server Name Indication (SNI) hostname in client connections. The SNI hostname is available if the client connection is TLS and has a valid ServerName extension; otherwise, the policy has no effect.

The following policy gestures were added to support this feature:

Table 352: New SNI hostname policy

CPL condition and corresponding web VPM source object (if applicable)	Description
`client.connection.ssl_server_name=` **SSL Server Name** : This object is available in the SSL Access, SSL Intercept, Web Access, and Forwarding layers	Perform a string match for the SNI hostname.
`client.connection.ssl_server_name.exists=` **SSL Server Name**: This object is available in the SSL Access, SSL Intercept, Web Access, and Forwarding layers.	Test if the SNI hostname exists.
`client.connection.ssl_server_name.length=` No VPM object.	Test the total size of the SNI hostname.

In addition, you can include the `x-cs-connection-ssl-server-name` and `x-rs-connection-ssl-server-name` access log fields to log the SNI hostname.

More Information:

- Content Policy Language Reference
- Web Visual Policy Manager Reference
- ProxySG Log Fields and Substitutions

Network Stack Improvements

The SGOS network stack was updated to improve performance and stability. This release includes:

- Improved IPv6 handling.
- ARP, TCP, and IP conformance to the latest internet standards.
- Improved TCP throughput in the presence of out-of-order TCP packets.
- Updated PCAP file. The file downloaded from the appliance is in *.pcapng format, replacing the previous *.cap format.

Web Visual Policy Manager Improvements

- A new **HTTP Connect URL Category** destination object allows you to test the category of the host name in the HTTP CONNECT request. This object is available in the Web Access and Web Request layers.
- The existing **Application Group**, **Application Name**, and **Application Operation** destination objects are available in the Web Authentication and Web Content layers.
- Policy rule column headers (**Source**, **Destination**, **Track**, etc.) are sticky. The column headers remain visible when you scroll through layers containing many rules.
- For better navigation when creating and editing Combined Objects, you can sort objects by name or type.
- To provide better visibility into large policies with many rules, the rule view features a more condensed layout with less unused space.
- You can add a policy rule at a specific position within a layer. In the VPM, open the context menu in a rule and select **Insert Rule**. The new rule appears below the current rule.
- Various areas of the Web VPM interface were improved for a more consistent and intuitive user experience.

Trust Package Update

The trust package has been updated. To download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

Other Enhancements and Changes in SGOS 7.3.1.1

- The built-in Access Security Policy has been updated. Access Security Policy is part of Policy Services, which is available on all supported ProxySG appliances with a valid base license. No additional subscription is required to use the policy; however, the Policy Services subscription should be used to keep the policy up to date. To keep the subscription active, make sure that your Symantec support contract is valid.
- Some deny decisions are deferred until after an SSL intercept decision in policy. Previously, when policy included `deny.*` gestures and `ssl.forward_proxy(https)` , an HTTP handoff occurred before the deny. The behavior is now corrected so that `deny.connection` and `deny.request` decisions will occur before HTTP handoff. Other deny gestures are not affected.
- In previous releases, when policy was changed and re-installed, authenticated users in multi-tenant deployments had to re-authenticate for transactions subsequent to the policy change. Now, user authentication persists when non-authentication policy is changed and re-installed. Policy changes related to authentication configuration (realms, groups of interest, etc.) still require user re-authentication.

  The default tenant contains the authentication information for users who authenticate under multiple inline tenant policies.
- This release improves the accuracy of apparent-data-type recognition.

Deprecations and Removals in SGOS 7.3.1.1

- SkyUI is disabled by default in version 7.3.x. You can re-enable this management interface, but be aware that it is potentially vulnerable to security issues. For best security, do not enable SkyUI.
- Managing ProxyClient and Unified Agent is deprecated. You can enable these features, but the Management Console and the CLI indicate that support for these remote clients will be removed in a future release.
- In the Web VPM, the **Protocol Methods** service object no longer includes the Instant Messaging protocol and methods. IM policies were removed in a previous release.
- IPv6 site-local addresses are no longer supported in ProxySG configurations.
- Network adapters associated with unsupported platforms (such as SG300, SG600, SG900, and SG9000) are no longer supported.

Fixes in SGOS 7.3.1.1

SGOS 7.3.1.1 includes the following bug fixes.

Table 353: Authentication

ID	Issue
SG-22479	Fixes an issue where users experienced a redirect loop when using Chrome. This issue occurred because Chrome refused authentication cookies for not having Secure and SameSite=none properties.

Table 354: CIFS Proxy

ID	Issue
SG-20625	Fixes an issue where client machines lost connectivity to file shares after waking from sleep mode.

Table 355: CLI Console

ID	Issue
SG-4912, SG-19528	Fixes an issue where ProxySG advanced URLs used less-secure HTTP GET methods.

Table 356: Diagnostic Tools

ID	Issue
SG-22935	Fixes an issue where the appliance sent diagnostic reports to Symantec if the appliance was reinitialized.

Table 357: Health Checks

ID	Issue
SG-22116	Addresses an issue where the appliance experienced a restart in PG_HEALTH_CHECKS process: "HC Watchdog" in "" at .text+0x0 SWE : 0x3a0004.

Table 358: HTTP Proxy

ID	Issue
SG-18485	Addresses an issue where the system stopped responding in process "HTTP CW 15C1CFADA40" in "libmemory.so".

Table 359: ICAP

ID	Issue
SG-19149	Fixes an issue where patience pages took long to load when uploading a file for ICAP scanning. The issue occurred if the filename contained an ampersand character (&).

Table 360: Licensing

ID	Issue
SG-23360	Fixes an issue where creating a C16XS model on the Integrated Secure Gateway resulted in "Warning: Nonstandard memory configuration detected."

Table 361: SSL Proxy

ID	Issue
SG-22606	Addresses an issue where the appliance stopped responding in process group: "PG_CFSSL" and process: "SSLW 21BB8E14F90" in "libc.so" at .text+0x168cd.

Table 362: SSL/TLS and PKI

ID	Issue
SG-11173	Fixes an issue where the event log displayed "failed to copy keyring" and "failed to copy certificate file" errors after an upgrade from version 6.7.x to version 7.x.
SG-23060	Addresses an issue where the appliance stopped responding in process group: "PG_SSL_HNDSHK" and process: "HTTP CW 10EC3699A40" in "libcfssl.exe.so" at .text+0x39f1cc.

Table 363: TCP/IP and General Networking

ID	Issue
SG-4154	Fixes an issue where a restart occurred due to a high volume of IPv6 network traffic.
SG-11975	Fixes an issue where the appliance was vulnerable to a LAND attack.
SG-21102	Fixes an issue where the final TCP reset (RST) used a different interface from the rest of the TCP conversation.
SG-18904	Fixes an issue where running the `#(config)`**`ipv6 auto-linklocal disable`** command did not remove the auto link-local IPv6 address.
SG-21747	Fixes an issue where an IPv6 address could not be added using the `#(config connection-forwarding)`**`add`** command.
SG-22295	Fixes an issue where the Secure Web Gateway V100 platform experienced a memory leak due to an interface reinitializing repeatedly.
SG-20003	Fixes an issue where configuring failover with two ProxySG appliances with IPv6 addresses resulted in both appliances to be master.
SG-22879	Fixes an issue where configured routing tables on the appliance were not preserved after upgrading from version 6.7.5.6 to a later 6.7.x or 7.x.
SG-4156	Addresses an issue where the system stopped responding in process group: "PG_TCPIP" and process: "stack-bnd-1:0-rxq-0" in "libstack.exe.so" at .text+0x50657a.
SG-13300	Fixes an issue where policy traces contained an incorrect interface number when return-to-sender (RTS) was disabled and policy specified the interface in the `client.interface=` condition.

Table 364: Visual Policy Manager (Legacy)

ID	Issue
SG-20740	Fixes an issue where VPM policy did not detect when multi-tenant landlord mode was enabled. When this issue occurred, some related policy gestures such as Tenant ID were unavailable. This issue was also fixed in the Web VPM.

Table 365: Web VPM

ID	Issue
SG-20727	Fixes an issue where the Substitution Variables list in the **SNMP** and **Email** track objects displayed variables incorrectly due to font size.
SG-22513	Fixes an issue where the **SSL Server Name** source object did not generate the correct CPL when set to **Exact Match**.
SG-20740	Fixes an issue where VPM policy did not detect when multi-tenant landlord mode was enabled. When this issue occurred, some related policy gestures such as Tenant ID were unavailable. This issue was also fixed in the legacy VPM.
SG-20656	Fixes an issue where the **Request URL Category** destination object within a Combined Object did not allow you to press Enter to insert newlines.

SGOS 7.2.8.1 GA

Release Information

- Release Date: August 4, 2021
- Build Number: 264841

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1 and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x

  ATTENTION
  Support for Client Manager, ProxyClient, and Unified Agent will be removed in a future release.
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.2.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.x does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.x. If you begin upgrading to 7.2.x from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.2.x to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.x, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later.
  – Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

  NOTE
  If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.8.1

- SGOS 7.2.8.1 introduces new features and enhancements. See Features in SGOS 7.2.3.1.

Fixes in ProxySG 7.2.8.1

- This release includes various fixes. See Fixes in SGOS 7.2.8.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.8.1

SGOS 7.2.8.1 introduces the following new features and changes.

New Models for Virtual Appliances

For ProxySG virtual appliances, the following new models are available for GCP and ISG Enterprise VA deployments:

Virtual CPUs	Virtual Memory (GB)	ISG-Proxy-VA-100 Storage (GB)	ISG-Proxy-VA-200 Storage (GB)	Connection Count
6	24	2x100	1x200	37,500
6	40	4x100	2x200	62,500

Virtual CPUs	Virtual Memory (GB)	ISG-Proxy-VA-100 Storage (GB)	ISG-Proxy-VA-200 Storage (GB)	Connection Count
6	48	4x100	2x200	75,000
10	40	4x100	2x200	62,500
10	80	4x100	2x200	125,000
10	96	4x100	2x200	150,000
12	48	4x100	2x200	75,000
12	96	4x100	2x200	150,000
12	128	4x100	2x200	200,000
14	64	4x100	2x200	100,000
14	112	4x100	2x200	175,000
14	144	8x100	4x200	225,000
20	96	4x100	2x200	150,000
20	144	N/A	4x200	225,000
20	192	N/A	6x200	300,000
24	112	4x100	2x200	175,000
28	128	8x100	4x200	200,000
28	192	N/A	6x200	300,000
28	288	N/A	8x200	450,000
32	80	8x100	2x200	125,000
32	160	N/A	4x200	250,000
32	256	N/A	8x200	400,000
32	320	N/A	8x200	500,000

More information:

- *SGOS on GCP Configuration Guide*
- *ISG Enterprise VA Guide*

Timezone Database Update

As of July 10, 2021, a new timezone database (2021a) is available at https://download.bluecoat.com/release/timezones.tar

The database can be installed using the CLI command `load timezone-database` . The database will also be installed on an SGOS appliance running 7.2.7.1 or newer after a `restore-defaults factory-defaults` or on a new virtual appliance instance.

Support for New Network Interface Card

The Silicom bypass driver has been updated to support the PE310G4BPI40-T Quad port Copper 10 Gigabit Ethernet PCI Express Bypass Server Intel® x540 Based card.

Configure Local Categories for Web Filtering

You can disable or enable whether local categories for Web Filtering are included in the configuration for the proxy client with the following command:

```
#(config clients web-filtering)include-local-categories {disable | enable}
```

More Information:

- *Command Line Interface Reference*

New CLI Command for ARP Strict Matching

The following CLI command is available for enabling and disabling ARP strict matching (default `enable`):

```
#(config)tcp-ip arp-strict-matching {enable|disable}
```

More information:

- *Command Line Interface Reference*

Link Speed No Longer Displayed for Virtual Appliances

For virtual appliances that are using a para-virtual network adapter, when you view the output for the `show interface` command or the `SysInfo` , the link speed no longer displays and instead reads "virtual network" or "virtual link". Additionally, the MAC address now displays in the `show interface` output.

More Information:

- *Command Line Interface Reference*

Set IP Version Preferences for DNS Resolution

You can now configure preferences for which IP version to use for DNS queries by using the following command (default is `unspecified`):

```
#(config)dns ip-version {ipv4-only|ipv6-only|prefer-ipv4|prefer-ipv6|unspecified}
```

More information:

- *Command Line Interface Reference*

New `incorrect_content_length` Option for `response.raw_headers.tolerate`

Previously, the appliance would forward responses that exceeded the length specified in the response header to the ICAP server or client. Now the appliance drops additional bytes before sending a response. If you do want the appliance to forward responses that exceed the specified length, use the property `response.raw_headers.tolerate(incorrect_content_length)` .

More information:

- *Content Policy Language Reference*

New Policy Action for SOCKS Requests

To ensure that SOCKS requests use cached surrogate credentials for authentication, a new `socks.authenticate.mode()` policy action has been added. Use this policy instead of `authenticate.mode()` for SOCKS requests. The policy supports the `proxy` and `proxy-ip` challenge type and surrogate credential.

For example:

```
<proxy> client.protocol=socks
  socks.authenticate(testrealm) socks.authenticate.mode(proxy-ip)
```

More information:

- *Content Policy Language Reference*
- KB Article 166657

Event Log Trace Level Enhancement

The `#(config event-log)`**`level trace`** CLI command was added in version 7.2.5.1. In this release, the `trace` level also writes long-running ICAP REQMOD transactions, and deferred and resumed ICAP RESPMOD transactions to the event log.

More Information:

- *Command Line Interface Reference*
- *SGOS Upgrade/Downgrade*, "Behavior Changes in SGOS 7.2.x"

Fixes in SGOS 7.2.8.1

SGOS 7.2.8.1 includes the following bug fixes.

Table 366: Access Logging

ID	Issue
SG-27063	Fixes an issue where `show advanced-url /accesslog/tail` was taking a long time to respond because the buffers for `TE_Transaction::Generate_random_ipv6_address()` were too small.
SG-26885	Fixes an issue where Kafka uploads for sites with a large number of nodes would not succeed due to the size of the upload exceeding the maximum for the recoverable heap.

Table 367: Authentication

ID	Issue
SG-27405	Fixes an issue where details for group-async were not available for the `#show configuration` and `#(config windows-domains)view` commands.
SG-27378	Fixes an issue where users could not join or rejoin a domain if the username contained a dollar sign ($) character.
SG-26994	Fixes an issue where the appliance was unresponsive due to incorrectly prioritizing certain processes.

Table 368: Cloud Platform

ID	Issue
SG-25640	Fixes an issue where the appliance became unresponsive when loading a trust package.
SG-26843	Fixes an issue where sometimes ZTP would not successfully set up an appliance due to ZTP attempting to parse the JSON object as part of the jobTargetData.

Table 369: DNS Proxy

ID	Issue
SG-27367	Fixes an issue where the appliance experienced a restart when the DNS proxy incorrectly copied from or to a null pointer.
SG-25261	Fixes an issue where the appliance experienced a restart when attempting to free a pointer it had already freed.

Table 370: HTTP Proxy

ID	Issue
SG-25111	Fixes an issue where the `supplier.country` policy did not match for tunneled HTTPS connections when protocol detection was disabled.
SG-25593	Fixes an issue where protocol detection did not detect HTTP/2 when a server response was received before the client connection. When this issue occurred, the log displayed "Cannot detect server speakfirst protocol".

Table 371: Policy

ID	Issue
SG-26626	Fixes an issue where the appliance experienced a restart when the hostname was assigned "null" during address resolution.

Table 372: Security

ID	Issue
SG-26323	Patches the open-source Apache Tomcat library to resolve multiple vulnerabilities.

Table 373: SOCKS Proxy

ID	Issue
SG-25580	Fixes an issue where SOCKS requests failed due to not being matched to the IP surrogate credential. This fix requires using the new `socks.authenticate.mode()` policy action, as described in Features in SGOS 7.2.3.1.

Table 374: SSL Proxy

ID	Issue
SG-23430	Fixes an issue where the appliance experienced high memory usage. This issue occurred in reverse proxy mode with `#(config *service_name*)attribute forward-client-cert` enabled and Certificate Policies extensions in use.
SG-26999	Fixes an issue where the appliance experienced high memory usage during SSL handshakes.

Table 375: SSL/TLS and PKI

ID	Issue
SG-25640	Fixes an issue where the appliance became unresponsive when loading a trust package.
SG-25818	Fixes an issue where the appliance experienced a restart when attempting to install HSM configuration.

Table 376: TCP/IP and General Networking

ID	Issue
SG-27807	Fixes an issue where DNS flags were not set correctly for AAAA requests, causing the appliance to not retry with A requests after receiving invalid AAAA responses.
SG-27115	Fixes an issue where adding NICs to a virtual appliance running on VMware ESXi changed the order of NICs.
SG-25955	Fixes an issue where the appliance experienced a restart due to the appliance marking the mbuf with a weak INP.
SG-27375	Fixes an issue where the appliance experienced a restart when the database was updated.
SG-27677	Fixes an issue where the appliance returned the error "DNS Resolver Response: Unknown error response (202)" for a DNS-forwarding group that was associated with the default routing domain.
SG-26136	Fixes an issue where the interfaces showed the speed and duplex as unknown in the SysInfo for virtual appliances.

Table 377: Timezones and NTP

ID	Issue
SG-27893	Fixes an issue where the warning message when attempting to configure an NTP server that is not present included a leading "%" used for error messages.

Table 378: Transformer

ID	Issue
SG-25137	Fixes an issue where the appliance could not rewrite URLs that had empty HTML comments preceding them.

Table 379: Web Application Firewall

ID	Issue
SG-25723	Fixes an issue where interactions between `http.request.log.mask_by_name()` and `http.request.detection.bypass_cache_hit()` policy properties sometimes resulted in the appliance not decoding the URLs of payloads during internal analysis.

SGOS 7.2.7.2 PR

Release Information

- Release Date: June 28, 2021
- Build Number: 263784

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After upgrading, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.2.7.2

- This release includes various fixes. See Fixes in SGOS 7.2.7.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.2.7.2

Table 380: Security

ID	Issue
SG-27187	Fixes a security vulnerability. For more information, see SYMSA18331.

SGOS 7.2.7.1 GA

Release Information

- Release Date: May 26, 2021
- Build Number: 262380

NOTE
SGOS is cumulative. SGOS 7.2.7.1 is based on the SGOS 7.2.6.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.11 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.7.1

- SGOS 7.2.7.1 introduces new features and enhancements. See Features in SGOS 7.2.0.1.

Fixes in ProxySG 7.2.7.1

- This release includes various fixes. See Fixes in SGOS 7.2.7.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.7.1

New Maximum High Memory Threshold for ISG Licensed Deployments

For ProxySG virtual appliances deployed with Enterprise and Node-Locked licenses, the thresholds for the CFS high memory pool has been increased to 1600 MB.

New NIC Maximum for Virtual Appliances

The following types of ProxySG virtual appliances now have a new maximum number of virtual interfaces:

Platform	Maximum NICs
AWS	8
Azure	8
GCP	8
Hyper-V	8
KVM	16
VMware	10
Xen	8

New http.response Policy Gesture

The following property has been added to force the appliance to stop waiting for HTTP response data from the client:

```
http.response.response_data.prevent_inspection_delay(yes|no)
```

See the *Content Policy Language Reference* for more information.

Fixes in SGOS 7.2.7.1

SGOS 7.2.7.1 includes the following bug fixes.

Table 381: Access Logging

ID	Issue
SG-25675	Fixes an issue where an existing access log facility could not be deleted.

Table 382: Authentication

ID	Issue
SG-25860	Fixes an issue where the appliance had a hardware exception when the XML authentication realm contained a parsing issue.

Table 383: CLI Consoles

ID	Issue
SG-26539	Fixes an issue where some CLI commands returned a `kex protocol error` message.

Table 384: HTTP Proxy

ID	Issue
SG-25953	Fixes an issue where the appliance had a software exception when policy included `ssl.forward_proxy(yes)` and a deferred transaction was denied.
SG-25957	Fixes an issue where users cannot access alldata.com after an upgrade.

Table 385: ICAP

ID	Issue
SG-19774	Fixes an issue where "Request timed out" errors were incorrectly reported when ICAP connections were closed on the server side. Now, the ICAP error states "Failed due to dropped connection".
SG-26130	Fixes an issue where the ProxySG appliance performed extra scanning when Content Analysis sends an ISTag value of "0" in the ICAP response.

Table 386: Kernel

ID	Issue
SG-19721	Fixes an issue where the appliance stopped responding when there was a high number of HTTP/S connections on the appliance.

Table 387: Policy

ID	Issue
SG-25615	Fixes an issue where users could not connect to chat.google.com. The policy property `http.response.response_data.prevent_inspection_delay(yes|no)` has been added to resolve this issue.

Table 388: SSL/TLS and PKI

ID	Issue
SG-25924	Fixes an issue where the appliance stopped responding after deleting an SSL keyring.

Table 389: TCP/IP and General Networking

ID	Issue
SG-26046	Fixes an issue where the serial console showed the error message "Apply__DNS_fwd() ERRO DNS fibnum = 0" when the appliance booted up. The issue occurred because DNS forwarding group names were truncated if they were 16 characters or more in length.
SG-23835	Fixes an issue where users experienced slow browsing due to many failed DNS lookups on the appliance.
SG-26308	Fixes an issue where a DHCP vulnerability in FreeBSD could cause the appliance to stop responding.

Table 390: Web Application Firewall

ID	Issue
SG-26127	Fixes an issue where the SQL injection engine incorrectly blocked some Chrome headers.

SGOS 7.2.6.1 GA

Release Information

- Release Date: April 13, 2021
- Build Number: 260877

NOTE
SGOS is cumulative. SGOS 7.2.6.1 is based on the SGOS 7.2.5.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.10 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23187 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later.
  - Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

    NOTE
    If upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

    NOTE
    In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.6.1

- SGOS 7.2.6.1 introduces new features and enhancements. See Features in SGOS 7.2.2.1.

Fixes in ProxySG 7.2.6.1

- This release includes various fixes. See Fixes in SGOS 7.2.6.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.6.1

SGOS 7.2.6.1 introduces the following new features and changes.

Integrated Secure Gateway Enterprise Secure Web Gateway Virtual Appliance

A new Integrated Secure Gateway (ISG) Enterprise Secure Web Gateway Virtual Appliance (SWG VA) license is supported for ProxySG VAs running on VMware's vSphere Hypervisor. The ISG Enterprise SWG VA facilitates server consolidation by co-existing with other virtual machines on a single hardware platform, including Symantec Content Analysis. With the ISG SWG VA providing security, the other virtual machines can provide branch office services (such as Domain Controller, print, DNS, and DHCP), as well as any VMware-certified software applications.

For more information, refer to the *Integrated Secure Gateway Enterprise Secure Web Gateway Virtual Appliance Deployment Guide*.

Heartbeat Reports Enhancement

Heartbeat reports sent to Support now include environment information for physical and virtual appliances. In addition, the heartbeats for applications running on Integrated Secure Gateway report the serial number.

New HTTP Dwell Time Statistics

The following counters have been added for dwell time statistics:

- Transactions performing static and dynamic categorization
- Transactions performing authentication and authorization, and server authentication
- Transactions performing various upstream, downstream, and reverse proxy handshakes
- Transactions determining object disposition
- Transactions performing DNS lookup for clients and servers

HTTP Debug Log Enhancement for gateway_error Error

When the appliance treats detects a proxy loop, it returns a gateway_error exception page. To assist with troubleshooting this error, the HTTP debug log now displays the message: "Detected proxy loop while parsing X-BlueCoat-Via header, returning gateway_error exception". To prevent the issue from occurring, remove the `X-BlueCoat-Via` header when sending requests upstream. Refer to KB 167710 for information.

Web Visual Policy Manager Enhancements

This release includes the following web VPM enhancements:

Management Center Roles and Permissions

Management Center administrators can assign permissions to users, which determine whether users can:

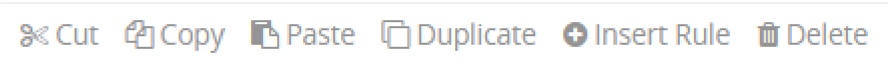
- View, add, edit, and delete policy layers.
- View, add, edit, and delete policy layer guards.
- View, add, edit, and delete policy rules.
- View, add, edit, and delete specific VPM objects.
- View and use the following options in the Operations menu: **Change Enforcement Domains**, **View All Objects**, **View Generated CPL**.

Improved Look and Feel

- The **Update policy** menu option to refresh generated CPL has been replaced with a 'refresh' icon:

  🔄

  . When you use the icon to refresh the CPL, the VPM notifies you of the change with a message, "Successfully refreshed generated CPL."
- All policy rule menu options now have icons:



Fixes in SGOS 7.2.6.1

SGOS 7.2.6.1 includes the following bug fixes.

Table 391: Authentication

ID	Issue
SG-18496	Fixes an issue where SAML authentication without client redirects did not work.

Table 392: Cache Engine

ID	Issue
SG-25363	Addresses potential denial of service attacks when there was a high number of simultaneous URL-based searches in /CE/Listing_Form.

Table 393: CLI Consoles

ID	Issue
SG-25564	Fixes an issue where attempting to view Advanced URLs results in an "Encrypted token has expired" message. This issue occurred when logging in to the console with a non-local admin user.

Table 394: Cloud Platform

ID	Issue
SG-25035	Fixes an issue where a ZTP-deployed appliance stopped responding when a routers option was not specified in the DHCP data source.

Table 395: HTTP Proxy

ID	Issue
SG-24969	Fixes an issue where users received error 502 "Content Encoding Error" when going to Facebook.
SG-22988	Fixes an issue where requests including both the Content-Length and Transfer-Encoding headers were forwarded to the OCS. Now, the Transfer-Encoding: identity header is removed from such requests before being forwarded.

Table 396: Management

ID	Issue
SG-24442	Fixes an issue where upgrading from version 6.7.4 to 7.2 did not preserve the previous non-default HTTPS console ciphers configuration or enable TLS 1.3 by default. This issue occurred if non-default SSL protocols were selected for the HTTPS console. If the appliance was never upgraded to 7.2.x or 7.3.x previously, upgrading to this release will preserve the previous ciphers selection and enable TLS 1.3 by default. To apply the fix if the appliance was previously upgraded to 7.2.x or 7.3.x, you must remove the existing SGOS 7.x configuration before upgrading. Issue the `#remove-sgos7-config` command, restart the appliance, and then install this release.
SG-25199	Fixes an issue where the Management Console exited with an error message, "SSL protocol negotiation failed. Logging out from Management Console".

Table 397: Policy

ID	Issue
SG-25255	Fixes an issue where authentication exceptions or `force_deny` caused ssl.tunnel transactions to bypass rules in `<forward>` layers.

Table 398: Reverse Proxy

ID	Issue
SG-25442	Fixes an issue where existing forwarding host names could not be edited to exceed more than 64 characters.

Table 399: SSL/TLS and PKI

ID	Issue
SG-24931	Fixes an issue where revoked intermediate certificates were added to the cached intermediate certificate list.

Table 400: SSL Proxy

ID	Issue
SG-13361	Fixes an issue where authenticated sessions persisted across browser sessions.
SG-25594	Fixes an issue where some SSL transactions were unexpectedly not denied. This issue occurred when policy included denials based on the response and SIPS protocol detection was enabled.
SG-25006	Fixes an issue where users received an "EXCEPTION(tcp_error): Request could not be handled" message when a site required a client certificate. This issue occurred when upgrading to version 7.2.
SG-25545	Fixes an issue where a site could not be accessed if protocol detection or TLS 1.3 was enabled.

Table 401: TCP/IP and General Networking

ID	Issue
SG-24139	Fixes an issue where outgoing connections intermittently went to an incorrect interface.

Table 402: Web VPM

ID	Issue
SG-25201	Fixes an issue where the **Combined Time Object** could not be added.
SG-24881, SG-23553	Fixes an issue where adding a **User** source object resulted in a "Cannot read property 'getAttribute' of undefined Retrieving base DN" error. The issue occurred if the LDAP realm was configured without a Base DN.
SG-20718	Fixes an issue where editing an IP address list in an object (such as **Send DNS Response**) immediately returned an inaccurate "IP address already exists" error.
SG-23981	Fixes an issue where authenticated users were allowed to access the HTTPS-Console service even though the Management Console login banner (Notice and Consent Banner) policy was configured in the web VPM. This occurred if CPL policy layers were not ordered correctly.
SG-21338	Fixes an issue where comparing generated CPL with deployed CPL incorrectly indicated differences between the two policies.
SG-23229	Fixes an issue where configured HSM keyrings were not available in the web VPM.
SG-21638	Fixes an issue where the **Allow user to override read-only** option in the **Web Isolation** object was not indented. It is now indented to indicate that it requires the preceding **Read-only, prevent user from entering data** option to be selected.

SGOS 7.2.5.1 GA

Release Information

- Release Date: February 4, 2021
- Build Number: 259008

  NOTE

  SGOS is cumulative. SGOS 7.2.5.1 is based on the SGOS 7.2.4.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.9 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23171 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later. If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.
  - Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.5.1

- SGOS 7.2.5.1 introduces new features and enhancements. See Features in SGOS 7.2.6.1.

Fixes in ProxySG 7.2.5.1

- This release includes various fixes. See Fixes in SGOS 7.2.5.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.5.1

SGOS 7.2.5.1 introduces the following new features:

Zero Touch Provisioning for Deployments

Zero Touch Provisioning (ZTP) allows you to easily deploy a ProxySG appliance or virtual appliance without using the terminal to configure the deployment. Instead, you prepare a ZTP payload containing the configuration and environment details, and provide the payload to the appliance. Additionally, if you are using Management Center to manage your ProxySG appliances, ZTP can automatically register the ProxySG appliance with Management Center.

NOTE
ZTP can only be performed on an appliance that is in a factory-reset state.

ZTP is available for all physical S-series appliances and the following virtual platforms:

- AWS
- Azure
- Cisco Cloud Services Platform
- ESXi
- KVM
- Microsoft Hyper-V

NOTE
ZTP is not currently available for ProxySG applications running on Integrated Secure Gateway.

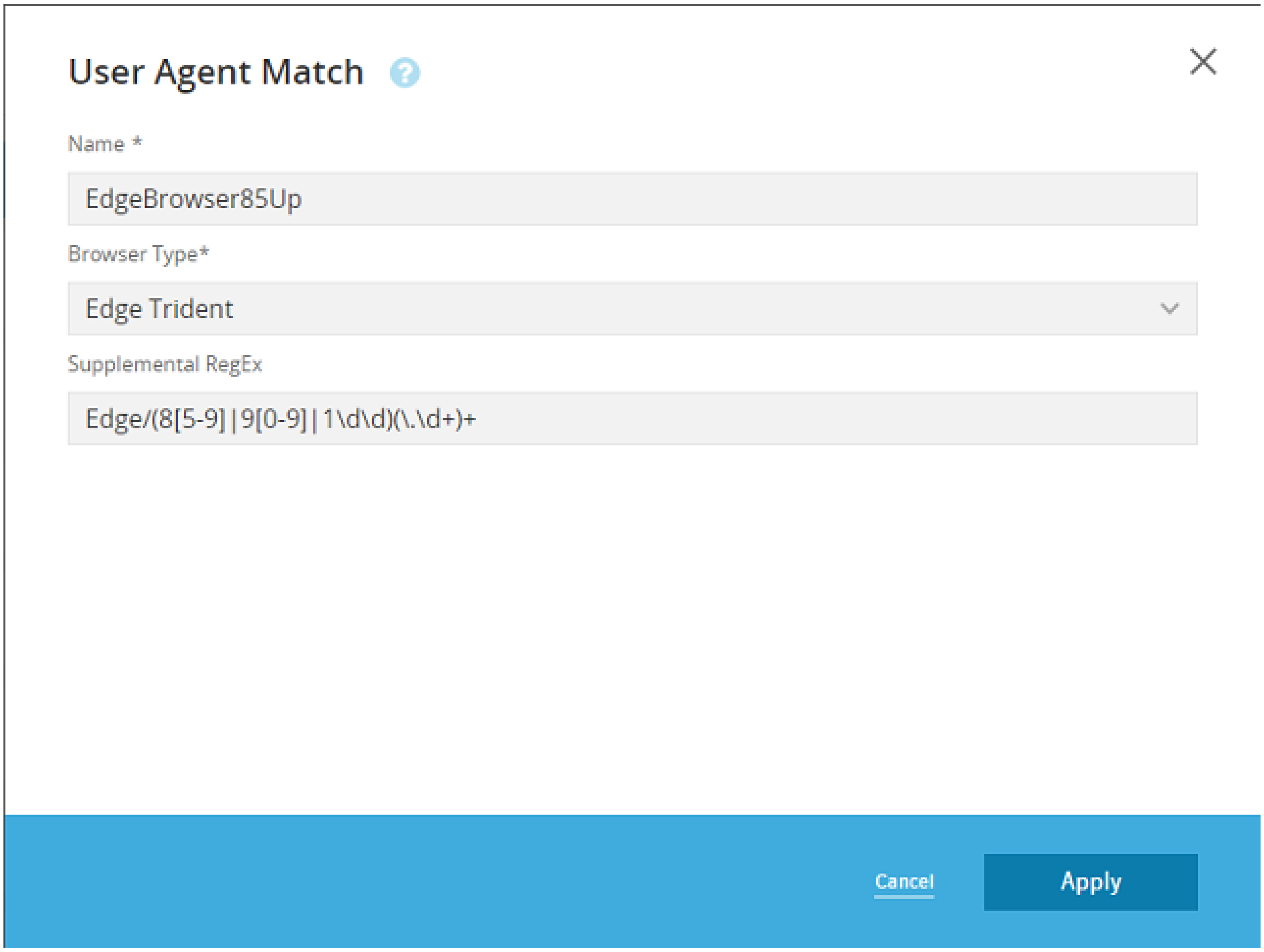
Clear the Serial Number When Restoring Factory Defaults

You now have the option to clear virtual appliance serial numbers when restoring factory defaults:

```
# restore-defaults factory-defaults [clear-va-serial]
```

New User Agent Match Object for VPM

The User Agent Match object provides a list of browsers types to select from and a field to further specify the type and version via a regEx.



User Agent Match

Name *

EdgeBrowser85Up

Browser Type*

Edge Trident

Supplemental RegEx

Edge/(8[5-9]|9[0-9]|1\d\d)(\.\d+)+

Full information:

- *ProxySG Web Visual Policy Manager Reference*

New Counters for HTTP Dwell Time Statistics

The following counters have been added for dwell time statistics :

- Transactions performing static and dynamic categorization
- Transactions performing authentication and authorization, and server authentication
- Transactions performing various upstream, downstream, and reverse proxy handshakes
- Transactions determining object disposition
- Transactions performing DNS lookup for clients and servers

New HTTP/2 Connection and Stream Counts in the Heartbeat Report

New counters have been added to the heartbeat report for HTTP/2 connections and streams.

Port Numbers Added to Policy Traces

Port numbers are now available in the policy trace output.

Fixes in SGOS 7.2.5.1

SGOS 7.2.5.1 includes the following bug fixes.

Table 403: Access Logging

ID	Issue
SG-22694	Fixes an issue where the appliance restarted due to multiple log upload threads attempting to simultaneously initialize the SSL cryptographic parameters.
SG-24708	Fixes an issue where the HTTP transaction timing fields (x-cs-rp-https-handshake-time, x-cs-https-handshake-time, and x-sr-https-handshake-time) in the access log generate a "-" or a "0" in log output regardless of the latency coming from the client or server.

Table 404: Authentication

ID	Issue
SG-23880	Fixes an issue where the appliance restarted after memory was released for an invalid memory pointer.
SG-23983	Fixes an issue where the appliance experience high CPU and memory consumption due to memory fragmentation.

Table 405: FTP Proxy

ID	Issue
SG-4624	Fixes an issue where the s-action access log field was sometimes not populated when ICAP REQMOD mirroring was enabled.

Table 406: HTTP Proxy

ID	Issue
SG-20158	Fixes an issue where certain ICAP threads were not terminated and caused memory leaks when ICAP REQMOD mirroring was enabled.

Table 407: ICAP

ID	Issue
SG-23811	Fixes an issue where the response time for health checks was longer than expected when the appliance was sending Content Analysis traffic to the ICAP broker.

Table 408: Performance

ID	Issue
SG-22312	Fixes an issue where a memory leak occurred due to processing MS-TURN traffic, which is a protocol used by Skype for Business.

Table 409: Policy

ID	Issue
SG-21244	Fixes an issue where exception pages that were greater than 8080 bytes did not display in the browser.
SG-24288	Fixes an issue where authenticating traffic via NTLM with BCAAA did not work in 7.2.4.1.
SG-24326	Fixes an issue where accessing the /dme/configuration advanced URL caused the license key auto-update feature to be enabled when it was originally set to disabled.

Table 410: Security

ID	Issue
SG-24232	Patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.

Table 411: SSL Proxy

ID	Issue
SG-2311	Fixes an issue where a new intermediate CA certificate that had the same subject name as a expired or revoked CA certificate could not replace the current expired or revoked CA certificate.
SG-23828	Fixes an issue where the appliance experienced a memory leak when handling HTTPS reverse proxy traffic with forward-client-cert enabled.

Table 412: SSL/TLS and PKI

ID	Issue
SG-24706	Fixes an issue where the ProxySG Admin Console experienced a restart because the PCAP stack was not large enough to handle all the filter expressions.
SG-24065	Fixes an issue where the appliance listed the strength for the dhe-dss-des-cbc3-sha cipher as "high" when OpenSSL classifies the cipher as "medium" strength.

Table 413: TCP/IP and General Networking

ID	Issue
SG-24034	Fixes an issue where the appliance did not notify users that WCCP did not start after a reboot. Now when WCCP does not start after a reboot, error messages are logged in the debug log.
SG-24810	Fixes an issue where the appliance experienced a restart when an HTTP/2 transaction could not be completed due to a null socket.

Table 414: URL Filtering

ID	Issue
SG-24231	Fixes an issue where the appliance experienced a restart when testing the category of a URL in the format of an email address (for example, "/ContentFilter/TestUrl/testuser@broadcom.com").

Table 415: Web VPM

ID	Issue
SG-15678	Fixes an issue where checkboxes in VPM objects such as **Combined Source** were editable in read-only mode.
SG-20679	Fixes an issue where adding a **DNS Request Threat Risk Level** object resulted in an error, "Please ensure that you have enabled Threat Risk Levels" even though the Threat Risk Levels service was enabled.
SG-21326	Fixes an issue where the UI incorrectly displayed "Enable Enforcement Domains" when the enforcement domains were already enabled.

SGOS 7.2.4.1 GA

Release Information

- Release Date: December 10, 2020
- Build Number: 257580

NOTE

SGOS is cumulative. SGOS 7.2.4.1 is based on the SGOS 7.2.3.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.8 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23171 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process,

disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.x from an earlier version 7.x or from version 6.7.4.4 or later. If you are upgrading from version 6.7.4.2 or earlier, an interim upgrade to version 6.7.4.3 might be required. To determine whether you can upgrade directly to version 6.7.4.4, refer to KB Article 18536.
  - Downgrade from 7.2.x to an earlier version 7.x or to version 6.7.4.4 or later.

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.4.1

- SGOS 7.2.4.1 introduces new features and enhancements. See Features in SGOS 7.2.4.1.

Fixes in ProxySG 7.2.4.1

- This release includes various fixes. See Fixes in SGOS 7.2.4.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

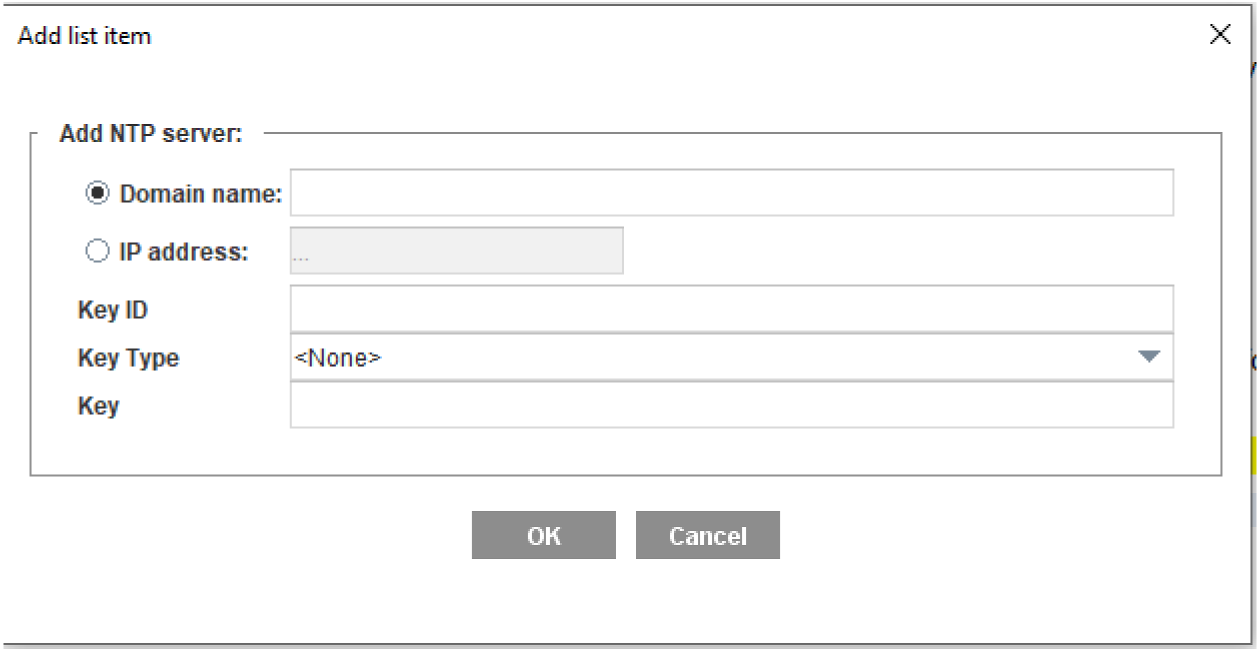
- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.4.1

SGOS 7.2.4.1 introduces the following new features:

Authenticated NTP

You can now specify NTP servers that support authentication where the time messages will be authenticated using symmetric-key encryption. After you obtain a key ID, unique encryption key, and key type from the NTP server authority, you can add the information to the ProxySG appliance. Currently, the appliance supports SHA1 key type.



Add list item

Add NTP server:

● Domain name:

○ IP address:

Key ID

Key Type <None>

Key

The following CLI commands were updated to support this feature:

```
#(config) ntp encrypted-server {domain_name|IP_address} key_id key_type key
```

Full information:

- *SGOS Administration Guide*
- *Command Line Interface Reference*

Absolute Management Console Session Timeout

A new command allows you to enable or disable an absolute timeout for all Management Console sessions:

```
#(config)security management [no] absolute-web-timeout <minutes>
```

where `minutes` is a value from 15 to 43200.

The appliance terminates all Management Console sessions after the specified timeout period. For best security, use this command to require users to re-authenticate to the Management Console after the timeout. Full information:

- *Command Line Interface Reference*

IPv6 Support for Console ACL

You can now enter IPv6 addresses for the console access control list (ACL) in the Management Console (**Configuration > Authentication > Console Access > Console Access**).

Additional Supported Apparent Data Types

The ProxySG appliance detects more apparent data types in HTTP requests and responses. The following types are now supported in apparent data type CPL properties and conditions:

Label	Description	Common Extensions
7ZIP	7-Zip archive	.7z
ACE	ACE archive	.ace
ARJ	ARJ archive	.arj
COMPRESS	compress compressed file	.Z (different from .z)
CPIO	cpio archive	.cpio
DAA	Direct Access Archive	.daa
EGG	EGG archive	.egg
EML	raw email	.eml, .mht, .mhtml
LHA	LHA archive	.lha, .lzh
LZIP	Lzip compressed file	.lz
MACH-O	macOS application or library	
TNEF	file encoded in Microsoft Transport-Neutral Encapsulation Format	.dat, .tnef
UUE	file encoded with uuencode or xxencode	.uu, .uue, .xx, .xxe
XAR	Extensible Archive Format	.mpkg, .pkg, .xar
XZ	xz compressed file	.xz

Full information:

- *Content Policy Language Reference*

Web Visual Policy Manager Improvements

- The existing **Application Group**, **Application Name**, and **Application Operation** destination objects are available in the Web Authentication and Web Content layers.
- For better navigation when creating and editing Combined Objects, you can sort objects by name or type.
- To provide better visibility into large policies with many rules, the rule view features a more condensed layout with less unused space.
- You can add a policy rule at a specific position within a layer. In the VPM, open the context menu in a rule and select **Insert Rule**. The new rule appears below the current rule.
- Various areas of the Web VPM interface were improved for a more consistent and intuitive user experience.

Trust Package Update

The trust package has been updated. To download the latest trust package, issue the following CLI:

```
#(config) load trust-package
```

DNS Transaction Access Log Fields

The following access log fields were added to help track HTTP transaction times:

- `x-client-dnslookup-time` : Total time taken (in ms) to perform the client DNS lookup.
- `x-server-dnslookup-time` : Total time taken (in ms) to perform the server DNS lookup.

HTTP Transaction Access Log Fields

The following access log fields were added to help track HTTP transaction times:

- `x-sr-https-handshake-time` : Total time taken (in ms) to complete the HTTPS handshake of the upstream connection.
- `x-cs-https-handshake-time` : Total time taken (in ms) to complete the HTTPS handshake of the downstream connection.
- `x-cs-rp-https-handshake-time` : Total time taken (in ms) to complete the HTTPS handshake of the reverse proxy connection.
- `x-client-object-disposition-time` : Total time taken (in ms) to determine the object disposition

Fixes in SGOS 7.2.4.1

SGOS 7.2.4.1 includes the following bug fixes.

Table 416: Access Logging

ID	Issue
SG-18288	Fixes an issue where access logs using a custom log format could not be uploaded via Kafka client to the broker.

Table 417: Authentication

ID	Issue
SG-23666	Fixes an issue where the Web Visual Policy Manager did not prompt users to sign in again after the session expired.
SG-23644	Fixes an issue by adding the IP address of the client to the event log message when the appliance receives a Krb5 replay error.
SG-22754	Fixes an issue where users received "Appliance Error (configuration_error). Your request could not be processed because of a configuration error. 'User has been logged out.'" This issue occurred when surrogate credentials expired with SAML authentication.
SG-21796	Addresses an issue where the appliance experienced a page fault (error code 0x4) within process "libauthenticator.exe.so" (0x40015).
SG-23208	Fixes an issue where the appliance experienced high memory usage in HTTP policy evaluation.
SG-22479	Fixes an issue where users experienced a redirect loop when using Chrome. This issue occurred because Chrome refused authentication cookies for not having Secure and SameSite=none properties.
SG-23878	Addresses an issue where authenticated users were allowed to access the HTTPS-Console service even though Management Console login banner (Notice and Consent Banner) policy was configured in the VPM. This occurred if CPL policy layers were not ordered correctly.

Table 418: Cache Engine

ID	Issue
SG-23589	Fixes a race condition where opening up a cached object sometimes resulted in the appliance to stop responding.

Table 419: CIFS Proxy

ID	Issue
SG-20625	Fixes an issue where client machines lost connectivity to file shares after waking from sleep mode.

Table 420: CLI Consoles

ID	Issue
SG-22064	Fixes an issue with high memory consumption in SSH.

Table 421: Diagnostic Tools

ID	Issue
SG-22935	Fixes an issue where the appliance sent diagnostic reports to Symantec if the appliance was reinitialized. Reinitialization is not an issue and does not require reports.

Table 422: Health Checks

ID	Issue
SG-22815	Fixes a timing issue where the appliance would stop responding when modifying an access log in configuration.
SG-22116	Addresses an issue where the appliance experienced a restart in PG_HEALTH_CHECKS process: "HC Watchdog" in "" at .text+0x0 SWE : 0x3a0004.

Table 423: HTTP Proxy

ID	Issue
SG-22779	Fixes an issue where the appliance experienced a restart after receiving an invalid request when using HTTP/2 and SSLV offload.
SG-23197	Fixes an issue where the appliance experienced a restart when there were multiple concurrent HTTP/2 requests and the web server closed the connection.
SG-23441	Fixes an issue where some webpages would not render correctly when an SSL Visibility appliance was decrypting traffic.
SG-20969	Addresses an issue where the appliance experienced a page fault in process group "PG_HTTP" and process "HTTP SW 109E777BA40 for 108F240BA40" in "libc.so" at .text+0x16b8c.
SG-20587	Fixes an issue where the policy trace and access log did not show categorization information. This issue occurred when a tenant matched policy rules after the categorization occurred.
SG-14408	Fixes an issue where Websocket tunnels inflated some HTTP transaction time statistics.

Table 424: ICAP

ID	Issue
SG-19149	Fixes an issue where patience pages took long to load when uploading a file for ICAP scanning. The issue occurred if the filename contained an ampersand character (&).

Table 425: Kernel

ID	Issue
SG-22879	Fixes an issue where configured routing tables on the appliance were not preserved after upgrading from version 6.7.5.6 to a later 6.7.x or 7.x.

Table 426: Licensing

ID	Issue
SG-23360	Fixes an issue where adding a C16XS model to Integrated Secure Gateway resulted in "Warning: Non-standard memory configuration detected."

Table 427: Network Drivers

ID	Issue
SG-21976	Fixes an issue where ProxySG instances running on Hyper-V and Azure experienced a reduction in performance due to batch processing being enabled.

Table 428: Proxy Forwarding

ID	Issue
SG-23369	Fixes an issue where forwarding groups did not balance the load equally when members of the group were in a failure state.

Table 429: SSL Proxy

ID	Issue
SG-23117	Fixes an issue where the appliance could not establish outbound connections using TLS 1.3 for Java applications.
SG-23380	Fixes an issue where `server.certificate.validate.cclpolicy` did not apply to tunneled SSL transactions.
SG-22606	Addresses an issue where the appliance stopped responding in process group: "PG_CFSSL" and process: "SSLW 21BB8E14F90" in "libc.so" at .text+0x168cd.

Table 430: SSL/TLS and PKI

ID	Issue
SG-23060	Fixes an issue where the appliance experienced a restart after upgrading in SGOS 7.2.2.1 when tunnel-on-protocol-error was enabled and a set of cascading SSL errors occurs.

Table 431: TCP/IP and General Networking

ID	Issue
SG-22295	Addresses an issue where the Secure Web Gateway V100 platform experienced a restart in process group: "PG_OBJECT_STORE" and process: "CEA Cache Administrator" in "" at .text+0x0.

Table 432: URL Filtering

ID	Issue
SG-23245	Fixes an issue where a requested URL matched policy for "None" category even though the URL was categorized in the local database.

Table 433: Web VPM

ID	Issue
SG-21942	Fixes an issue where adding a **User** object with an LDAP realm selected prepended "cn=" to the Full Name field.

SGOS 7.2.3.2 PR

Release Information

- Release Date: November 11, 2020
- Build Number: 256747

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- Upgrading from ProxySG 6.7.x to version 7.1.x might cause unexpected behavior with configured HSMs. See SG-23171 in Known Issues in SGOS 7.x for more information.
- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After you upgrade, reconfigure your malware scanning. For more information, see the *SGOS Administration Guide* and *ProxySG Web Visual Policy Manager Reference*.
- The following paths are the supported upgrade/downgrade paths for this release:
  – Upgrade to 7.2.1.1 from version 6.7.4.3 and later 6.7.x releases, or another version 7.x.
  – Downgrade from 7.2.1.1 to version 6.7.4.3 and later 6.7.x releases, or another version of 7.x.

  NOTE
  If you are upgrading from SGOS 6.7.4.2 or earlier, you might have to upgrade to version 6.7.4.3 as an interim step before upgrading to this release. For more information, refer to KB Article 18536

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Fixes in ProxySG 7.2.3.2

- This release includes various fixes. See Fixes in SGOS 7.2.3.2.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Fixes in SGOS 7.2.3.2

SGOS 7.2.3.2 includes the following bug fixes.

Table 434: Cloud Platform

ID	Issue
SG-22202	Addresses an issue where instances launched from the AWS Marketplace failed to complete bootstrapping and were unable to boot up. This issue affected only newly-created instances and instances where a `#`**`restore-defaults factory-defaults`** was issued in version 7.x. Version 6.7.x was unaffected.

Table 435: Health Checks

ID	Issue
SG-21726	Fixes an issue where HSM health check entries were missing after updating the HSM configuration.
SG-23269	Addresses an issue where the appliance stopped responding in process group: "PG_HEALTH_CHECKS" and process: "HC Watchdog" in "" at .text+0x0.
SG-23525	Addresses an issue where the appliance stopped responding in process group: "PG_HEALTH_CHECKS" and process: "HC Worker hsm.lunasp1p-nc" in "libcfssl.exe.so" at .text+0x3276fd.

Table 436: SSL/TLS and PKI

ID	Issue
SG-13787	Fixes an issue where new HSM health checks were lost after a restart. This issue occurred when the HSM names contained upper-case letters. If you add an HSM whose name contains upper-case letters, the name is converted to lower-case. To configure or refer to the HSM in the CLI, you must use the lower-case name. For example, if you add an HSM called EastHSM1, the name is converted to easthsm1. To edit the HSM, specify the lower-case name as in `#(config)edit hsm easthsm1` . You can verify HSM names using the `#`**`show ssl hsm`** command Note that this fix applies to newly-created HSMs only. Any existing HSMs whose names contain upper-case letters will continue to have failed health checks.
SG-23630	Addresses an issue where the appliance stopped responding in process group: "PG_SSL_KEY2K" and process: "** NO NAME **" in "libcfssl.exe.so" at .text+0x2fc493.

SGOS 7.2.3.1 GA

Release Information

- Release Date: September 28, 2020
- Build Number: 254850

NOTE

SGOS is cumulative. SGOS 7.2.3.1 is based on the SGOS 7.2.2.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.7 release.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S410, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE

  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- When upgrading to 7.2.1.1, your malware scanning configuration is not preserved. After upgrading, reconfigure your malware scanning. For more information, see the SGOS Administration Guide and ProxySG Web Visual Policy Manager Reference.
- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.1.1 from version 6.7.4.3 and later 6.7.x releases, or another version 7.x.
  - Downgrade from 7.2.1.1 to version 6.7.4.3 and later 6.7.x releases, or another version of 7.x.

    NOTE
    If upgrading from SGOS 6.7.4.2 or earlier, you might have to upgrade to version 6.7.4.3 as an interim step before upgrading to this release. For more information, refer to KB Article 18536

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.3.1

- SGOS 7.2.3.1 introduces new features and enhancements. See Features in SGOS 7.2.3.1.

Fixes in ProxySG 7.2.3.1

- This release includes various fixes. See Fixes in SGOS 7.2.3.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.3.1

SGOS 7.2.3.1 introduces the following features.

Apparent Data Type Detection Improvements

This release improved the accuracy of apparent-data-type recognition in non-ICAP cases.

Unsupported Platform Message in Initial Configuration Wizard

If you are upgrading to version 7.x on an unsupported platform, the initial configuration wizard displays the following message:

```
****************** CONFIGURATION ALERT ******************
```

```
This version of SGOS is no longer supported on this hardware.
System halted. Please reboot and select a supported version of SGOS.
```

Management Console Logout Message

When you log out of the Management Console, the web browser now displays the message, "You have successfully logged out. Please close the browser window."

Fixes in SGOS 7.2.3.1

SGOS 7.2.3.1 includes the following bug fixes.

Table 437: Access Logging

ID	Issue
SG-21506	Fixes an issue where the `s-action` and `sc-filter-result` fields returned incorrect values when a connection was blocked.

Table 438: Authentication

ID	Issue
SG-13697	Fixes an issue where users intermittently received a “Failure to authenticate a tunneled SSL request” error. This issue occurred in explicit deployments.
SG-21605	Fixes an issue where CAPTCHA validator configuration failed with an error message, "Redirect URL <*URL*> suffix is not found in generated list."
SG-22524	Fixes an issue where a SAML attribute that is no longer referenced in a SAML realm cannot be deleted.
SG-21196	Fixes an issue where the appliance failed to join an Active Directory (AD) domain. This issue occurred when the appliance used AD site information from different forests.
SG-20114	Fixes an issue where the appliance stopped responding after LDAP server connections were incorrectly determined to be pending.

Table 439: Cache Engine

ID	Issue
SG-22439	Addresses an unexpected restart in SWE: 0x0 HWE: 0x40018 PFLA: 0x0 in PG_OBJECT_STORE Process: "CEA Cache Administrator" in "" at .text+0x0.

Table 440: Health Checks

ID	Issue
SG-16671	Fixes an issue where changes to the `drtr.rating_service` health check did not persist after issuing the #**`restart regular`** command.

Table 441: HTTP Proxy

ID	Issue
SG-4886	Fixes an issue where chunked encoded responses with invalid data were handled incorrectly.
SG-20669	Addresses an issue where the appliance stops responding in context "PG_HTTP Process: "HTTP SW 21301F91A40 for 115F4961A40" in "libhttp.exe.so". This issue occurred on the SG-S500 platform.

Table 442: Management Console

ID	Issue
SG-21741	Fixes an issue where selecting a keyring in SSL proxy service configuration in the Management Console returned the message "Keyring <*name*> not found". This issue occurred when the keyring name included spaces.
SG-19397	Fixes an issue where clicking the **Documentation** and **Support** links in the Management Console displayed incorrect web pages.

Table 443: Policy

ID	Issue
SG-21910	Addresses a restart in process: "HTTP SW 40F7BD3CA40 for 111B47EDA40" in "libpolicy_enforcement.so" at .text+0x30b904.
SG-21556	Fixes an issue where WebEx application/operation policy did not work due to application renaming. In the current Application Classification database, the WebEx Application name is "Cisco WebEx".
SG-19798	Fixes an issue where online meeting applications terminated periodically after new central policy was installed. The online meeting application matches `<SSL>` rules in the central policy.

Table 444: Services

ID	Issue
SG-21637	Fixes an issue where WebPulse requests sometimes returned an "unavailable" status.

Table 445: SNMP

ID	Issue
SG-11869	Fixes an issue where the SNMP response from the appliance returned a value of 5 bytes for DeviceDiskTimeStamp; SNMP Manager accepts only 4 bytes.
SG-20949	Fixes an issue where using smilint on BLUECOAT-SG-AUTHENTICATION-MIB.txt resulted in numerous error messages.

Table 446: SSL/TLS and PKI

ID	Issue
SG-21941	Fixes memory leaks in Open SSH.
SG-22496	Fixes an issue where using the CLI command `#(config)`**`upgrade-path`** *`<URL>`* did not work.

ID	Issue
SG-20688	Fixes an issue where ProxySG certificate validation failed incorrectly. This issue occurred when the server certificate's chain of trust was rooted to an expired issuer certificate authority (CA), but was also cross-signed to a valid trusted CA. Now, when the primary certificate chain has an expired issuer CA, the alternate chain is validated if it is not expired.

Table 447: SSL Proxy

ID	Issue
SG-18062	Fixes an issue where frequent policy installations resulted in high memory consumption.
SG-22396	Addresses an issue where the appliance stopped responding in process group "PG_SSL_HNDSHK" Process: "HTTP SW 30F72E24A40 for 40D8A6E8A40" in "kernel.exe" at .text+0x1336fbc.
SG-17320	Fixes an issue where memory leaks occurred when running RWT scripts with SSLV offload enabled.
SG-22173	Fixes an issue where users received HTTP error 400 because client SSL certificates were not sent in forward proxy mode.

Table 448: System Statistics

ID	Issue
SG-22082	Addresses an exception in Process group: "PG_BDC_TUNNEL", Process: "bdc.tunnel.sw.004082E0.7055861A000" in "libbdc.exe.so" at .text+0x2ff3c4.

Table 449: TCP/IP and General Networking

ID	Issue
SG-12989	Fixes an issue where the CLI was unresponsive after issuing the `#`**`clear-arp`** CLI command. This issue occurred if routing domains were configured.
SG-20553	Addresses an issue where the appliance stopped responding in process group: "PG_TCPIP" Process: "CLI_Worker_2" in "libstack.exe.so" at .text+0x42da71.
SG-21850	Fixes an issue where memory usage was high due to too many packets in the netisr queue.
SG-21879	Fixes an issue where a network interface was unstable during peak hours.

Table 450: URL Filtering

ID	Issue
SG-19054	Fixes an issue where thresholds for CPU throttling set via `#(config content-filter)`**`cpu-throttle disk`** *`<low>`* *`<high>`* did not persist after a reboot.

SGOS 7.2.2.1 GA

Release Information

- Release Date: August 17, 2020
- Build Number: 253750

NOTE

SGOS is cumulative. SGOS 7.2.2.1 is based on the SGOS 7.2.1.1 release. In addition, this release includes all features and fixes that were included in the 6.7.5.6 release.

Supported Platforms

- ProxySG hardware appliances: S200, S410, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- Integrated Secure Gateway: 2.1.x and later
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.2.1 from version 6.7.4.3 and later 6.7.x releases, or another version 7.x.
  - Downgrade from 7.2.2.1 to version 6.7.4.3 and later 6.7.x releases, or another version of 7.x.

    NOTE
    If upgrading from SGOS 6.7.4.2 or earlier, you might have to upgrade to version 6.7.4.3 as an interim step before upgrading to this release. For more information, refer to KB Article 18536.

See SGOS Upgrade/Downgrade documentation details the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.2.1

- SGOS 7.2.2.1 introduces new features and enhancements. See Features in SGOS 7.2.4.1.

Fixes in SGOS 7.2.2.1

- This release includes various fixes. See Fixes in SGOS 7.2.2.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.2.1

SGOS 7.2.2.1 introduces the following features.

ProxySG Admin Console 1.1.2

This release introduces new ProxySG Admin Console (SGAC) features.

The SGAC is not associated with SGOS releases; thus, you can use these new features without having to change your SGOS version. See SGAC Releases in SGOS for feature and compatibility information. You can also refer to the following documentation at Tech Docs:

- *ProxySG Administration (Admin Console Edition)*
- Management Center documentation

Trust Package Update

The Hongkong Post Root CA 3 certificate has been added to the trust package. The trust package was made available for download on May 1, 2020.

DNS Server Resolution Behavior Changes

The appliance now contacts DNS servers in the order in which they appear if they are online. If a server is offline, it is skipped and the next online server is contacted. The server that the appliance successfully contacts will be contacted again for future queries.

More information:

- SGOS Upgrade/Downgrade Guide
- *How does the DNS resolution work on the ProxySG?* (article ID 165929)

Management Console JAR File Update

The certificate used to sign the Management Console loader.jar has been updated. If you downloaded the Management Console loader.jar from KB articles previously, refer to the appropriate article for the latest version of the JAR file:

- Launch SGOS management consoles using the Management Console Launcher https://knowledge.broadcom.com/external/article?articleId=169194
- Management Console Launcher for systems without Internet connectivity https://knowledge.broadcom.com/external/article?articleId=169208
- Support for Java 11 on ProxySG and Advanced Secure Gateway appliances https://knowledge.broadcom.com/external/article?articleId=173228

Timezone Database Enhancements

- A new timezone CLI command has been added to display timezone and timezone database information:
  ```
  # show timezones details
  ```
- A full timezone database is installed on newly-manufactured ProxySG virtual appliances, or when a system is re-initialized using the `# restore-defaults factory-defaults` CLI command. Previously, only a mini-database was available and running the `# load timezone-database` CLI command was required to get the full database. Now, the `# load timezone-database` command is needed only to download subsequent database updates from http://download.bluecoat.com.
- The timezone database has been updated to reflect changes in Release 2020a of the IANA timezone database.

More information:

- Command Line Interface Reference

Custom Upload Client Configuration

Custom access log upload client configuration now accepts hostname as an alternative to host IP address:

```
#(config log log_name)custom-client {alternate | primary} {hostname | host_IP_address} [port]
```

More information:

- Command Line Interface Reference

Deprecations and Removals

- TLS 1.3 offload support for SSLV has been disabled. This feature will be supported in a later release.

Fixes in SGOS 7.2.2.1

SGOS 7.2.2.1 includes the following bug fixes.

Table 451: Access Logging

ID	Issue
SG-11525	Fixes an issue where Kafka continuous upload was slow.
SG-18169	Fixes an issue where the config field in access logs was limited to fewer 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.
SG-15198	Fixes an issue where the appliance experienced a restart due to receiving an empty cache buffer.
SG-10110	Fixes an issue where the `s-action` access log field was blank.

ID	Issue
SG-20673	Fixes an issue where logs were not uploaded to the log server via custom client due to a server domain mismatch error. The issue occurred even when Verify Peer was disabled.

Table 452: Authentication

ID	Issue
SG-18357	Fixes an issue where authentication was impacted by Google Chrome's option for SameSite secure cookie settings being enabled by default.
SG-12666	Fixes an issue where appliance experienced CAC performance issues.
SG-8116	Fixes an issue where "undefined" appears instead of "admin" in the logout URL of the Management Console.
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-19013	Fixes an issue where the appliance could not join the active directory in GCP because its hostname was too long.
SG-20312	Fixes an issue where the CAPTCHA form was not displayed when using CAPTCHA authentication.

Table 453: BCAAA

ID	Issue
BCAAA-7	Fixes an issue where a security change in Windows Server 2019 prevented Windows SSO from receiving authenticated users from domain controllers. When this issue occurred, the BCAAA log displayed the message "Cannot query domain controller &lt;IP_address&gt;; status=5:0x5:Access is denied". This fix requires additional configuration steps; refer to KB article 194792 for instructions.

Table 454: Cache Engine

ID	Issue
SG-20885	Addresses an issue where the appliance stopped responding in Process group: "PG_OBJECT_STORE" Process: "CEA Cache Administrator".

Table 455: CLI Consoles

ID	Issue
SG-21358	Fixes an issue where`show xml-config concise` output was inconsistent with previous versions of SGOS.
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-17715	Fixes an issue where the character "?" was removed from data that the appliance imported.

Table 456: DNS Proxy

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

Table 457: Health Checks

ID	Issue
SG-21465	Addresses exceptions in DNS health checks in a SWG VA on Microsoft Azure deployment.

Table 458: Health Monitoring

ID	Issue
SG-14656, SG-20825	Fixes an issue where HTTPS health check connections to servers with multiple virtual hosts failed. When this issue occurred, the server returned a certificate containing a different CN from the one specified in configuration.

Table 459: HTTP Proxy

ID	Issue
SG-20933	Addresses an issue where the appliance stopped responding with HE 0xE (page fault) in process H2 CCH-* in libc.so.
SG-18526	Fixes an issue where the appliance sometimes experienced a restart when request.icap_mirror(yes) was triggered in policy under some circumstances.
SG-20412	Fixes an issue introduced in version 6.7.5.3 where large amounts of IPv4 ARP traffic sometimes caused the appliance to restart. This issue was not likely to occur in deployments with fewer appliances on the same network.

Table 460: 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.

Table 461: Kernel

ID	Issue
SG-21332	Fixes an issue where Secure Web Gateway virtual appliances running on Hyper-V or Microsoft Azure platforms with multiple network interfaces stopped processing on one or more interfaces, causing the VA to stop responding. This fix introduces an issue where the VA experiences lower throughput and performance (up to 10%) compared to other virtualization environments.
SG-21298	Addresses an issue where the appliance stopped responding in process Group:"" Process:"kernel.exe".

Table 462: 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.

Table 463: Policy

ID	Issue
SG-17978	Fixes an issue where the browser address bar showed an incorrect URL after successful LDAP authentication.
SG-18066	Fixes an issue where quota policy failed to compile on a new installation of version 7.2.1.1.
SG-13680	Fixes an issue where certain websites were incorrectly denied due to domain fronting detection CPL.
SG-19826	Fixes an issue where the appliance attempted to contact servers when policy contained `deny` or `access_server(no)` CPL in a Web Request layer.
SG-19540	Fixes an issue where the appliance experienced a restart when returning an exception page.
SG-22028	Addresses an issue where the appliance stopped responding in Process: "CLI_Worker_0" in "kernel.exe" at .text+0x12d6564.

Table 464: Registry

ID	Issue
SG-20565	Addresses an issue where the appliance stopped responding in PG_HEALTH_CHECKS in Process "HC Watchdog" in "" at .text+0x0.

Table 465: SNMP

ID	Issue
SG-20925	Fixes an issue where the BLUECOAT-SG-PROXY-MIB contained an invalid date. Download the latest MIB files from the Broadcom download portal.

Table 466: SSL Proxy

ID	Issue
SG-18193	Fixes an issue where the HTTP CONNECT hostname was not rewritten according to `rewrite()` policy when proxy forwarding was enabled.
SG-21147	Fixes an issue where the SNI hostname was not rewritten according to `rewrite()` policy in the initial proxied connection.
SG-21748	Fixes an issue where the appliance does not request a client certificate for TLS 1.3 in reverse proxy mode although the HTTPS service is configured to forward the client certificate.
SG-17104	Addresses an issue where the appliance stopped responding in PG: "PG_SSL_HNDSHK": Process: "SSLW 10B8E433FB0" in "libshared_dll.exe.so" at .text+0x2273ce.
SG-20873	Fixes an issue where uninitialized memory could cause the appliance to stop responding.
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 `ssl.forward_proxy(no)` and `ssl.forward_proxy(on_exception)` policy was not applied to TLS 1.3 tunneled sessions.

ID	Issue
SG-18824	Fixes an issue introduced in 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.
SG-19728	Fixes an issue where guest authentication was unexpectedly applied, causing users to be denied access to sites.
SG-17859	Fixes an issue where the appliance unexpectedly reached a `force_deny` verdict in policy evaluation due to missing HTTP request attributes.
SG-19727	Fixes an issue where the forwarding rules were ignored when a verdict was reached in an ssl.tunnel transaction.
SG-19407	Fixes an issue where the appliance did not close connections with a TCP RESET that received force_deny and force_exception verdicts.
SG-18488	Fixes an issue where appliance forwarded some but not all CH bytes and could not tunnel on error for SSLv2 traffic.

Table 467: SSL/TLS and PKI

ID	Issue
SG-20787	Fixes an issue where TLS 1.3 did not work in reverse proxy when a keylist was specified.
SG-20736	Fixes an issue where users received HTTP error 403 with multi-tenant policy installed. The policy worked as expected in version 6.7.5.3, but not in version 7.2.x.
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.
SG-9186	Fixes an issue where WebPulse service health checks failed after setting a default OSCP responder.
SG-18246	Fixes an issue introduced in version 6.7.4.9 where server connections were not reused in an HTTPS reverse proxy deployment.
SG-17567	Fixes an issue where memory usage per connection increased significantly when the appliance reached the maximum number of HTTPS connections via SSL tunnel and detect protocol was enabled.

Table 468: SSLV Integration

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

Table 469: TCP/IP and General Networking

ID	Issue
SG-20407	Fixes an issue where the appliance sent TCP window update packets to the client via an incorrect interface.
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 Management Console.
SG-17191	Fixes an issue where the appliance experienced a restart in process group "PG_TCPIP" in process "WCCP_Admin" in "libstack.exe.so".

ID	Issue
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".
SG-9432	Fixes an issue where the appliance's boot up was delayed or could not be completed if offline DNS servers appeared in the list of servers before online servers in the primary group or alternate groups if all primary DNS servers were offline.
SG-19941	Fixes an issue where the appliance experienced a restart when removing a non-configured IPv6 address from the VLAN.
SG-18333	Fixes an issue where the final TCP reset (RST) uses a different interface from the rest of the TCP conversation.
SG-19960	Addresses an issue where the appliance experienced a restart in process group: "PG_TCPIP" Process: "CLI_Worker_0" in "libstack.exe.so" at .text+0x435ed7.
SG-20486	Addresses an issue where the appliance experienced a restart in process "SSLW 80F319F0FA0" in "libstack.exe.so" at .text+0x4f1e1a.
SG-18519	Fixes an issue where responses to SNMP polls were sent to the default routing domain interface even though SNMP traffic was configured for a different routing domain.

Table 470: TCP Tunnel Proxy

ID	Issue
SG-19940	Fixes an issue where TCP-Tunneling/tunnel-stats did not display IPv6 server address.
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.

Table 471: Visual Policy Manager (Legacy)

ID	Issue
SG-20277	Fixes an issue where clicking Install Policy multiple times cleared all VPM policy, despite a message indicating that installation was in progress.

Table 472: 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 7.2.1.1 GA

Release Information

- Release Date: May 29, 2020
- Build Number: 250985

NOTE

SGOS is cumulative. SGOS 7.2.1.1 is based on the SGOS 6.7.5.2 release. In addition, this release includes all features and fixes that were included in the 7.1.1.1 and 7.2.0.1 releases.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- HSM Agent: 2.0 and later
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later

  NOTE
  The new ProxySG Admin Console (SGAC) requires Management Center 2.4.x or later.
- ProxyAV: 3.5.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228.

Upgrading To/Downgrading From This Release

- ProxySG 7.2.1.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.
- If you are downgrading from ProxySG 7.2.1.1 to a version earlier than 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers were

deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running versions earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.1.1 from version 6.7.4.3 and later 6.7.x releases, or another version 7.x.
  - Downgrade from 7.2.1.1 to version 6.7.4.3 and later 6.7.x releases, or another version of 7.x.

    NOTE
    If you are upgrading from SGOS 6.7.4.2 or earlier, you might have to upgrade to version 6.7.4.3 as an interim step before upgrading to this release. For more information, refer to KB Article 18536

  See SGOS Upgrade/Downgrade documentation for the supported upgrade/downgrade paths for this release.

  NOTE
  In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.1.1

- SGOS 7.2.1.1 introduces new features and enhancements. See Features in SGOS 7.2.5.1.

Fixes in ProxySG 7.2.1.1

- This release includes various fixes. See Fixes in SGOS 7.2.1.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.1.1

SGOS 7.2.1.1 introduces the following features.

Introduction of ProxySG Admin Console

This SGOS release coincides with the initial release of the Blue Coat ProxySG Admin Console (SGAC), which is designed to help you manage and monitor the appliance more efficiently. This next-generation web interface is the successor to the Java-based Management Console and can be accessed through the latest browsers. This initial release of the ProxySG Admin Console focuses on replacing the most commonly utilized configuration and workflow steps, with additional releases to follow.

The ProxySG Admin Console is not associated with SGOS releases; thus, you can access new workflows and configurations without having to change your SGOS version.

To access the Admin Console, you require Symantec Management Center version 2.4 or later. Download Management Center from the Broadcom Support site.

More information:

- SGAC Releases in SGOS
- SGOS Administration (Admin Console Edition) Guide
- Management Center 2.4 Configuration and Management Guide

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

- Display resolution:
  - 1366 x 768
- 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.

In addition, the web-based VPM and all of its functionality are available in Symantec Management Center. Refer to Management Center documentation for details.

More information:

- ProxySG Web Visual Policy Manager Reference

Policy Services Subscription and Security Policies

Symantec’s Policy Services is a policy subscription service that delivers curated security policies to the appliance to block malware downloads and web threats, and enable compliance to quickly configure network security policies. Use this feature to implement best-practices security coverage, and to facilitate setup, deployment, and testing of policies.

Policy Services is available on all entitled ProxySG hardware and virtual appliances:

- An entitled appliance must have an active and valid support maintenance contract.
- An entitled virtual appliance must be under an active subscription or extension (that is, the subscription term is valid and has not reached its termination end date).
- The subscription is enabled by default and no additional purchase is required to use the policy; however, for optimum coverage, the Policy Services subscription should be enabled to keep the policy up to date. To keep the subscription active, make sure that your Symantec support contract or subscription term is valid.

NOTE
Content Security Policy has superseded Malware Scanning from version 6.7.x, but Symantec Web Security Service (WSS) is not yet updated with Content Security Policy rules. In the interim, deployments using Content Security Policy on the appliance with Universal Policy enforcement will continue to use the previous threat protection policy. Content Security Policy levels are mapped to WSS security levels; refer to the SGOS Upgrade/ Downgrade documentation for details.

Access Security Policy

Enable this policy to block malicious transactions. Refer to https://knowledge.broadcom.com/external/article/174668 for details.

Content Security Policy

Enable this policy to secure content scanning. Refer to https://knowledge.broadcom.com/external/article/174669 for details.

More information:

- SGOS Administration Guide - Using Policy Services
- ProxySG Web Visual Policy Manager Reference
- SGOS Security Best Practices
- SGOS Upgrade/Downgrade Guide - Behavior Changes Applicable to SGOS 7.1.x Upgrade/Downgrade
- Integrating Content Analysis 3.0 with Other Symantec Products: ProxySG and Malware Analysis

TLS 1.3 Support

For improved security and performance, this release supports the TLS 1.3 protocol in configurations and policy gestures. SSLv2 support has been removed (see **Removals and Deprecations**).

When configuring the following services/profiles in the Management Console and in the CLI, TLS 1.3 is available and SSLv2 has been removed:

- HTTPS Console service
- HTTPS reverse proxy service
- SSL client profile
- SSL device profile

For the following VPM objects and associated policy gestures, TLS1.3 has been added as an option and SSLV2 has been removed:

- **Client Negotiated SSL Version** objects (legacy and web VPM)
  `client.connection.negotiated_ssl_version=`
- **Server Negotiated SSL Version** objects (legacy and web VPM)
  `server.connection.negotiated_ssl_version=`

New Cipher Suites

The following TLS 1.3 cipher suites have been added:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

In addition, 40- and 56-bit ciphers, and Export and Low strength ciphers have been removed.

Refer to https://knowledge.broadcom.com/external/article/170130 for a list of all cipher suites shipped with the appliance.

> **NOTE**
> TLS 1.3 is not supported in ADN mode. When ADN is enabled, TLS 1.3 client connections are downgraded to TLS 1.2.

Impact on FIPS Mode

This release is based on OpenSSL 1.1.1, which supports TLS 1.3 but does not support FIPS 140-2. As a result, this release is not FIPS-capable. See the Limitations in SGOS 7.x and the SGOS Upgrade/Downgrade documentation for more information.

More information:

- SGOS Administration Guide
- Command Line Interface Reference
- Content Policy Language Reference
- Web Visual Policy Manager Reference
- Legacy Visual Policy Manager Reference

Symantec HSM Agent 2.0

This release supports Symantec HSM Agent 2.0 for the Thales Luna 7 HSM. This agent integrates with a network-based HSM to communicate with ProxySG and SSLV appliances. Signing requests for certificate emulation are sent to the HSM, where the intermediate resigning CA resides in the HSM. To allow your network-based Luna HSM to accept certificate signing requests from your ProxySG and SSL Visibility appliances, host the HSM Agent in a Docker container. Use Docker secrets to protect sensitive certificate and password data in your HSM deployment.

More information:

- Symantec HSM Agent 2.0 for the Thales Luna 7 HSM

HTTP/2 Support

The SGOS appliance now supports the HTTP/2 protocol. HTTP/2 offers improved performance due to its compression of HTTP headers, and multiplexing multiple requests and responses over a single connection. The feature is enabled by default, without the need for additional configuration or policy, and includes the following:

You can change these default settings by configuring settings and policy.

Configuring HTTP/2 Settings and Policy

To configure HTTP/2 on the appliance, use the new `#(config) http2` commands. Refer to the Command Line Interface Reference for details.

The following policy objects and gestures have been added or updated for this feature.

Table 473: HTTP/2 Policy Changes

VPM Object	CPL	Description
New static Action objects: • **Accept HTTP/2 Client-Side Connections** • **Do Not Accept HTTP/2 Client-Side Connections**	New property: `http2.client.accept(yes|no)`	Specifies whether the proxy accepts HTTP/2 on the client-side connection. Default behavior is yes.
New Action object: **Set HTTP/2 Client Max Concurrent Streams**	New property: `http2.client.max_concurrent_streams(streams)`	Specifies the maximum number of concurrent HTTP/2 streams that the client may initiate on the current client connection. Default maximum is 15.
New Action object: **Request HTTP/2 On Server-Side** Set object to **Yes**, **No**, or **Preserve Client-Side Setting**	New property: `http2.server.request(yes|no|preserve)`	Specifies whether the proxy requests HTTP/2 on the server-side connection. Default behavior is preserve
N/A	Condition supports new parameter: `http.request.version=2`	Tests if the client used HTTP/2 to make the request to the appliance.
N/A	Condition supports new parameter: `http.response.version=2`	Tests if the origin content server used HTTP/2 to deliver the response to the appliance.

Verifying HTTP/2 Traffic

- Add the `cs-version` field to the access log format to display the protocol and version from the client request, such as `HTTP/2` .
- Add the `rs-version` field to the access log format to display the protocol and version from the server response, such as `HTTP/2` .

> **NOTE**
> When offloading SSL from an attached SGOS appliance running version 7.1 or later, an SSL Visibility appliance running version 4.5.x supports HTTP/2 traffic between the two appliances.
>
> `http2.client.accept(yes|no)` is not honored for STunnel-intercepted connections.
>
> If protocol detection is enabled and policy includes certain combinations of `ssl.forward_proxy(yes)` and `http2.client.accept(no)` , some server responses fail. If this issue occurs, Symantec recommends controlling HTTP/2 with the `http2.server.request(no)` property.

More information:

- Command Line Interface Reference
- Content Policy Language Reference
- ProxySG Web Visual Policy Manager Reference and Legacy Visual Policy Manager Reference
- SGOS Administration Guide

DNS over HTTPS Support

The ProxySG appliance supports DNS over HTTPS (DoH) in the following modes:

- The ProxySG appliance acts as a HTTPS forward proxy. In this mode, the appliance detects and intercepts DoH requests, and serves the response from its DNS proxy. The appliance can detect DoH requests for any externally deployed DoH server as long as HTTPS interception is enabled for that server.
- A DoH service is configured inside the ProxySG reverse proxy services. In this mode, a forwarding server may or may not be configured as well. If no forwarding server is configured, the reverse proxy service is used exclusively as a DoH server.

> **NOTE**
> The appliance's DNS proxy cannot be used as a DoH client.

The following policy was added or updated to support this feature:

- In the DNS Access layer, the **DNS Client Transport** source object has a new HTTPS option (legacy VPM only).The `dns.client_tranport=` condition now tests for https.
- In the Web Access layer, new static VPM objects **Disable/Enable Handoff of DNS over HTTPS** allow for disabling/enabling handoff of DoH requests (legacy VPM only).The `http.dns_handoff(yes|no)` property was added.

More information:

- SGOS Administration Guide
- Content Policy Language Reference
- Legacy Visual Policy Manager Reference

Domain Fronting: Look Up Content Filtering Categories Associated with Hostnames

Use policy to test for categories associated with the hostname in an `HTTP CONNECT Host` header:

```
http.connect.host.category={status|category_name1[,category_name2,...]|category_group1[,category_group2,...]}
```

The following access log fields have been added to support this feature:

```
cs-http-connect-categoriescs-http-connect-categoriescs-http-connect-categories-bluecoatcs-http-connect-
categories-external cs-http-connect-categories-local cs-http-connect-categories-policy cs-http-connect-
categories-providercs-http-connect-categories-qualifiedcs-http-connect-category
```

More information:

- Content Policy Language Reference
- ProxySG Log Fields and CPL Substitutions Reference

Origin Header Categorization Policy

The following CPL has been added:

```
request.header.Origin.url.category={status|category_name1[,category_name2,...]|category_group1[,category_group2,...]}
```

This condition tests the content filter categories associated with the hostname in the Origin request header.

```
request.header.Origin.url.risk_level={status|risk_level1[,risk_level2,...]}
```

This condition tests the Threat Risk Level associated with the hostname in the Origin request header.

More information:

- Content Policy Language Reference

Brotli Encoding Support

The following properties support Brotli encoding:

```
http.client.allow_encoding()
http.server.accept_encoding()
```

Specify Brotli using the `br` parameter.

More information:

- Content Policy Language Reference

OCSP Stapling for Forward Proxy

This release supports OCSP stapling for forward proxy. When CRLs (certificate revocation lists) become outdated, OCSP stapling can be used to determine the status of certificates in a CRL. The OCSP stapled response is valid for seven days.

Use the following commands to enable and disable the feature:

```
#(config ssl)proxy ocsp-stapling {disable | enable}
```

More information:

- Command Line Interface Reference

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 5 reached." 0 80010:1
 htp_admin_testable.cpp:87
```

More information:

- SNMP Critical Resource Monitoring Guide

Syslog Supports TCP and TLS

This release allows you to configure Syslog monitoring. In addition to UDP log hosts, you can now specify TCP and TLS log hosts. Use the following new subcommands:

```
#(config event-log) syslog add [udp]{host_name | ip_address} [port]
#(config event-log) syslog add tcp {host_name | ip_address} [port]
#(config event-log) syslog add tls {host_name | ip_address} [port] [ssl_device_profile_name]
```

More information:

- Command Line Interface Reference

Authenticated NTP

Commands have been added to support adding authenticated NTP servers to the appliance:

```
#(config) ntp encrypted-server {domain_name|IP_address} key_id key_type encrypted_key


#(config) ntp server {domain_name|IP_address} [key_id key_type [key]]
```

More information:

- Command Line Interface Reference

SSH Enhancements

SSHv2 Host Key Pairs for the SSH Console

This release supports additional, selectable algorithms for creating SSHv2 host key pairs for the SSH console:

- RSA with 2048, 3072, or 4096 bit size
- ECDSA with nistp256, nistp384, or nistp52 curve
- Ed25519

To manage the SSHv2 host key pairs, select **Configuration > Authentication >SSH Inbound Connections > SSH Host Keys**.

In the CLI, use the `#(config ssh-server)` **`create host-keypair`** command. Refer to the Command Line Interface Reference for new arguments for this command.

> **NOTE**
> Before a backup and restore of the appliance, you can securely display the host keys by issuing the show config command. The settings specified by `#(config)` **`security private-key-display`** determine whether or not host keys are included in the output and whether they are output in encrypted form.

SSH KEX and Host Key Algorithms for the SSH Console

This release supports SSH KEX and host key algorithms for the SSH console. The following subcommands were added:

```
#(config ssh-console)hostkey-algs {add | remove | reset | set | view}
#(config ssh-console)kex-algs {add | remove | reset | set | view}
```

More information:

- *Command Line Interface Reference*
- *SGOS Administration Guide - Configuring Management Services*

SCP Upload Configuration Archives

Commands have been added to support configuration archive upload via SCP:

```
#(config)archive-configuration protocol scp
```

Use the following to configure SCP authentication:

```
#(config)archive-configuration scp-authentication {password | client-key | all | none}
```

More information:

- Command Line Interface Reference
- SGOS Administration Guide - Backing Up the Configuration

Periodic Upload of Configuration Archives

Commands have been added to support periodic configuration archive uploads:

```
#(config)archive-configuration periodic-upload {daily
upload_hour | minutes minutes}
```

where:

- *upload_hour* is the daily upload time
- *minutes* is the interval at which to upload archives

More information:

- Command Line Interface Reference

Periodic Upload of Service Information

Commands have been added to support periodic service information uploads to Symantec Support:

```
#(config service-info)periodic {count | custom | disable | enable | interval | no | sr-number}
```

More information:

- Command Line Interface Reference

Expanded Traffic Taps

The appliance now supports tap of:

- Unencrypted intercepted HTTP, TCP, and FTP traffic on the client and server sides
- Decrypted data from intercepted HTTPS or STunnel SSL traffic on the server side

For HTTP/2 traffic, `client.connection.encrypted_tap()` has conditional-policy limitations. Certain policy conditions require request information that arrives too late for the appliance to use to evaluate whether it should tap the connection. When you add conditions to client-side encrypted tap, add only conditions that the appliance can evaluate before it parses HTTPS requests, such as `client.address` , `http.connect.host` , or `client.connection.ssl_server_ name` . Do not use conditions that the appliance cannot evaluate before it parses HTTPS requests, such as `url.domain=` or `url.category=` . Also, do not use `http.connect.host.category=` as a known issue currently prevents it from working with `client.connection.encrypted_tap()` .

To enable tap, use the following policy gestures:

```
client.connection.tap(no|interface)
server.connection.tap(no|interface)
server.connection.encrypted_tap(no|interface)
```

where:

- *no*: Disable tap of client-side or server-side traffic.
- *interface*: Specify the interface for tapped content on the client side or server side. The form is*adapter*:*interface*.

In addition, new **Enable Client Tap** and **Enable Server Tap** action objects have been added to the legacy Visual Policy Manager.

More information:

- Content Policy Language Reference
- Legacy Visual Policy Manager Reference

Diagnostic Policy Support

This release introduces the `<Diagnostic>` layer. Include this layer, with valid rules, to obtain diagnostic information about transactions. For example, you can write policy to trace transactions or send notifications to specified recipients. Policy rules in this layer have no effect on traffic.

The `<Diagnostic>` layer supports the following CPL:

- all existing conditions
- all existing variables, including variables set in other layers and layer types
- the following existing properties, which are useful for troubleshooting and monitoring transactions:
  - `log_message()`
  - `notify_email()`
  - `notify_snmp()`
- the existing `define policy` macro, which can be called from any other layer and layer type
- the following new gestures:
  - `diagnostic.stop(pcap)`
  - `random=`
  - `transaction.field.name=`
  - `transaction.type=`

Use the `define policy` macro and refer to it in other policy rules that need examining or troubleshooting, as follows:

```
; define policy to trace requests to sample_domain.com
; where time taken to process request is 3000 ms or more
define diagnostic policy slow_traffic
<diagnostic>  trace.request(yes)
    url.domain=sample_domain.com transaction.field.time-taken=3000..
end

; apply specified diagnostic policy when authenticated user is 'research'
<proxy>
     user=research policy.slow_traffic
```

More information:

- Content Policy Language Reference

Enhanced Policy Variables Tests

You can test if a specified variable is set in policy using the following condition:

```
is_set.variable.name={yes|no}
```

In addition, variables can be tested in layers other than the ones in which they were set.

More information:

- Content Policy Language Reference

Policy Profiling Statistics

When policy profiling is enabled, the appliance collects statistics on policy for:

- How long the appliance took to evaluate each layer and rules
- Which policy rules were missed during evaluation

To enable or disable policy profiling, use the following CLI:

```
#(config) policy profiling {none | layer | rule | all}
```

You can view policy profiling statistics via the Management Console URLs Policy/Profiling/Statistics and Policy/Profiling/Results, or via the show config CLI command.

More information:

- Content Policy Language Reference

New CPL Diagnostics Probe and CLI to Upload Diagnostics to Syslog Host

You can collect diagnostics (policy traces, debug logs) with the new CPL `define probe` and view the details at the advanced URL page at https://*IP_address*:*port*/Diagnostics/Traces.

You can also upload diagnostics reports to a Syslog host using the CLI. TCP and TLS protocols are supported.

> **NOTE**
> You can only specify one hostname or IP address. For example, if you set the `syslog tcp` hostname and then set the `syslog tls` hostname, the TCP hostname is removed and the TLS hostname set.

```
# (config diagnostics) syslog tcp {hostname | IP_address} [port]
# (config diagnostics) syslog tls {hostname | IP_address} [port] [ssl_device_profile]
```

More information:

- SGOS Administration Guide
- Content Policy Language Reference
- Command Line Interface Reference

Policy for Positive Security Controls

This release introduces CPL that you can use to define whitelisted (monitored) traffic in a positive security implementation.

- Define field constraints that, when violated, trigger a block or monitor action:

  ```
  define constraint_set constraint_id
    part="attribute" [pattern.string_modifier="string"] {key|value|path}.modifier=constraint
   end
  ```

- Block or monitor transactions that violate defined field constraints:

  ```
  http.request.detection.constraint_set.constraint_id(block|monitor)
  ```

The bcreporterwarp_v1 log format includes two new fields that are populated when a constraint violation occurs:

- the `x-bluecoat-waf-attack-family` field shows `Constraint Violation`
- the `x-bluecoat-waf-block-details` or `x-bluecoat-waf-monitor-details` field shows details with the following syntax:

  ```
  "{""detection"":""constraint"",""part"":""{name|query_arg_name|query_arg|
  arg_name|arg|cookie_name|cookie|post_arg_name|post_arg|header_name|header|
  path}"",""line"":""constraint_set_defn_cpl_line"",""data"":""matched_data""}"
  ```

More information:

- Content Policy Language Reference

Client IP Reputation Policy

Determine a client's IP address’s reputation category and the confidence in the reputation designation. Then, reference the reputation category and confidence level (expressed as a level from 1 to 10) in policy to control inbound traffic. For example, you can:

- Monitor and access-log client requests if an IP address has a reputation as spam, and the service is moderately confident—such as level 6 out of 10—that the reputation category is correct.
- Block client requests if an IP address has a reputation as a bot, and the service is highly confident—such as level 9 out of 10—that the reputation category is correct. When a client request is blocked due to IP reputation policy, the client receives an exception page.
- Allow client requests if there is high confidence that an IP address is benign.
- In a future release, Client IP address reputation categories will be added through an Intelligence Services datafeed; however, you can define custom IP reputation categories in CPL policy without an Intelligence Services datafeed.

The following CPL was added to support this feature:

```
client.[effective_]address.ip_reputation[.category1[,category2, …]]=(status|range)
```

where:

- address is either the client IP address or effective client IP address
- category is an IP reputation category
- status is one of the following system-defined statuses: none, unavailable, unlicensed
- *range* is one of the following:
  - *..level* - the confidence level is less than the specified level
  - *level..* - the confidence level is greater than or equal to the specified level
  - *level1..level2* - the confidence level is between the specified levels, inclusive

```
client.ip_reputation.category1[,category2,...](value, none)
```

where:

- *category* is an IP reputation category, including user-defined categories. User-defined categories are specified as user_defined.category
- *value* is the confidence level for the specified reputation category or categories
- *none* means that any database entries for the specified reputation category or categories are suppressed and not access-logged

You can add the following fields to the bcreporterwarp_v1 log format:

- `x-bluecoat-client-address-reputation` - Logs the client IP address reputation
- `x-bluecoat-client-effective-address-reputation` - Logs the effective client IP address reputation

The log shows transaction details in the following format:

```
[{""reputation"":""spam"",""confidence"":9}]
```

More information:

- SGOS Administration Guide
- Content Policy Language Reference

PBKDF2 Storage for SGOS Appliance Passwords

The appliance now uses PBKDF2 to store and validate passwords for:

- Console accounts
- Enable mode for the appliance
- The front-panel PIN for systems that have front panels
- The secure serial port passwordUsers defined in a local user list

PBKDF2 hashes are automatically used when creating, updating, and verifying passwords for the aforementioned cases. A new CLI command is available for destroying the hashed passwords for SGOS versions prior to 7.2.1.1:

```
#(config) security destroy-old-passwords [force]
```

More information:

- Command Line Interface Reference

ProxySG SWG VA for Microsoft Azure

You can deploy a ProxySG virtual appliance (Secure Web Gateway edition) directly on Microsoft Azure.

More information:

- ProxySG SWG VA for Microsoft Azure Deployment Guide

Feature Changes and Enhancements

Geolocation Policy Supports Renamed Countries

A "Warning: Obsolete country name" message now appears when you try to install CPL policy that includes an outdated country name. An example of the message is, “Warning: Obsolete country name: 'Russian Federation' is now 'Russia'”.

If this occurs, replace the outdated country name in policy with the suggested name in the message. You can also refer to the geolocation database for current country names and codes. In the Management Console, select **Configuration > Geolocation > General** and click the link to display the list.

Geolocation Lookup Supports IPv6

Geolocation lookup (client geolocation in reverse proxy mode) now supports both IPv4 and IPv6.

Renamed Application Attribute Support

If a policy rule includes an attribute that has been renamed in the currently downloaded database, policy warnings occur when you try to install policy through CPL or the VPM. The following is an example of the warning:

```
Deprecation warning: 'old_attribute'; 'old_attribute' has been replaced by 'new_attribute' due to Too obscure
 and will no longer be accepted after Sat, 27 Jun 2020 00:00:00 UTC. Please switch to the new name before
 then.
```

To ensure that policy performs as intended, edit all instances of the renamed attribute and re-apply policy by the specified date. You can verify the current name of the attribute by clicking **View Attributes List** (**Configuration > Application Classification > Attributes > Attributes**).

Renamed Category Name Support

(Intelligence Services data source only) If a policy rule includes a category that has been renamed in the currently downloaded database, policy warnings occur when you try to install policy through CPL or the VPM. The following is an example of the warning:

```
Deprecation warning: 'old_category'; 'old_category' has been replaced by 'new_category' due to Category name
 updated and will no longer be accepted after Sat, 11 Jul 2020 00:00:00 UTC. Please switch to the new name
 before then.
```

To ensure that policy performs as intended, edit all instances of the renamed category and re-apply policy by the specified date.

You can verify the current name of the category by clicking **View categories** (**Configuration > Content Filtering > General**) and checking Blue Coat categories.

Default TCP Window Size Increase

The default TCP window size has been increased from to 256k bytes to 1 MB.

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
```

Test for Domain List Definitions

You can now test for domain list definitions with the `server.certificate.hostname=` condition. Use the following syntax:

```
server.certificate.hostname.list=pattern
```

where the list is configured in policy using `define server_url.domain condition`.

Realm Name is Now Logged in the Event Log

When a user accesses the CLI, event log messages now log the realm name (if applicable) and whether the user is read-only.

New SSLV Platforms

New SSLV platforms have been added to BLUECOAT-MIB.

Changes to Default 2MSL Value

To help reduce port exhaustion, the default 2MSL value has changed from 120 seconds to 60 seconds.

Encryption Changes to the Access Log

Encrypting an access log now produces a single ENC file, which contains all encrypted access log content. Previously, encrypting access logs produced an ENC file and a DER file. Refer to the "Configuring the Access Log Upload Client" chapter in the *SGOS Administration Guide* for details.

CPU Monitor Enabled By Default

CPU monitor is now enabled by default. Use CPU monitoring to troubleshoot CPU-related issues. To disable CPU monitoring, use the command `#(config diagnostics) cpu-monitor disable`.

Removals and Deprecations

- In some scenarios, the Blue Coat WebFilter service is discontinued. If you are upgrading to SGOS 7.2.0.1 and were using Intelligence Services as the data source previously, you will not have the option to use the WebFilter as a data source after you upgrade to 7.2.0.1. The option to set the data source in the Management Console and the CLI command `#(config application-classification) data-source {web-filter | intelligence-services}` have been removed.

  NOTE
  The appliance can restore a configuration archive that includes WebFilter as a data source, but it issues a deprecation warning.

  If you are running a new installation of 7.2.x, you will only have the option to purchase Intelligence Services for content filtering.

  If you are upgrading to 7.2.1.1 and were using WebFilter as the data source previously, there will be no change to your existing content filtering functionality.
- SSLv2 is no longer supported on the appliance. Options for SSLv2 have been removed from the Management Console and the CLI.
- The following ciphers are no longer available:
  - 40- and 56-bit ciphers
  - Export and low strength ciphers:

- DHE-DSS-DES-CBC-SHA
- DES-CBC3-MD5
- RC2-CBC-MD5
- DES-CBC-SHA
- DES-CBC-MD5
- EXP-DES-CBC-SHA
- EXP-RC4-MD5
- EXP-RC2-CBC-MD5
- EXP-DHE-DSS-DES-CBC-SHA

NOTE
If your policy contains reference to the deprecated low strength ciphers, recommends removing the references. If the references are not removed, policy will compile and a warning message will be issued.

For information on supported ciphers, refer to https://knowledge.broadcom.com/external/article/170130/cipher-suites-shipped-with-the-proxysg-a.html.

– DES and DES3 are no longer available for the #(config ssl)**view keypair** and #**show ssl keypair** commands. To display keypairs in an encrypted format, specify either aes128-cbc or aes256-cbc, for example:

```
#(config ssl)view keypair aes256-cbc
keyring_id
```

– The #(config)**security destroy-old-passwords** and #(config socks-gateway)**destroy-old-passwords** commands have been removed.

– For best security, SSHv1 commands have been removed from the CLI.

– Built-in malware scanning policy in previous versions of SGOS (previously in **Proxy > Configuration > Threat Protection > Malware Scanning**) has been removed. Use Content Security Policy with the Policy Services subscription instead. See **CC-419** in Known Issues in SGOS 7.x for a known issue when using Content Security Policy with Universal Policy enforcement.

– IM Proxies have been removed from the Management Console and CLI.

– The following platforms are no longer supported:

- SG300, SG600, SG900, and SG9000 physical appliances
- SWG-V100 (Gen1) virtual appliances
- MACH5 (Gen1) virtual appliances

Fixes in SGOS 7.2.1.1

SGOS 7.2.1.1 includes the following bug fixes.

Table 474: HTTP Proxy

ID	Issue
SG-17671	Fixes an issue where HTTP/2 requests might have been handled incorrectly if the HTTP/2 pseudo header fields were split across HEADERS and CONTINUATION frames. When the issue occurred, the proxy sent a GOAWAY frame and terminated the client HTTP/2 connection.
SG-17265	Fixes an issue where a missed policy condition triggered a diagnostics probe trace and log update.
SG-17062	Fixes an issue where YouTube pages did not load sidebar content.
SG-16206	Fixes an issue where the HTTP proxy did not capture the debug logs based on a tenant's probe condition. This occurred when tenancy was not determined yet (RCP, SEP-CIA) and the decision from policy was cached.
SG-4961	Fixes slow HTTP performance. This issue occurred when a forwarding group was configured to use Accelerator-Cookie host affinity.

ID	Issue
SG-14789	Fixes potential HTTP/2 denial of service vulnerabilities.
SG-13027	Fixes an issue where server-side HTTP/2 connections were not reused when using HTTP/2 in reverse proxy deployments.
SG-15704	Fixes an issue where the appliance did not upgrade new connections to HTTP/2 when ADN was enabled.

Table 475: Management Console

ID	Issue
SG-15003	Fixes an issue where the Management Console did not display Syslog host entries when a port number was specified.

Table 476: Performance

ID	Issue
SG-17333	Fixes an issue where the appliance experienced a memory leak in SSL and Cryptography.

Table 477: Policy

ID	Issue
SG-17634	Addresses an issue where the appliance stopped responding when certain diagnostic policy was installed.
CC-419	Fixes an issue where Content Security Policy exemptions (using the **Set Content Security Scanning** VPM object, set to **Exempt From Content Security**) were not supported in Symantec Web Security Service.
SG-12593	Fixes an issue where requests with "none" category and Threat Risk Level 5 were not blocked, but the access log incorrectly stated they were blocked. This issue occurred when the Access Security Policy layer was configured with Strong protection level.
SG-12845	Fixes multiple issues (including response code 500 and authentication errors) that occurred in a multitenant deployment with IWA Direct authentication, where landlord policy included the `tenant.request_url()` property.

Table 478: SNMP

ID	Issue
SG-13054	Fixes an issue where the SensorCode values defined in BLUECOAT-SG-SENSOR-MIB did not support the S450 and S550 platforms.

Table 479: SSL Proxy

ID	Issue
SG-4574	Fixes an issue where whitespaces in field values were not ignored when adding a keyring through the CLI. This issue did not occur when creating keyrings through the Management Console.
SG-9716	Fixes incorrect access log values for the `x-cs-sessionid` and `x-rs-sessionid` fields.

Table 480: SSL/TLS and PKI

ID	Issue
SG-3988	Fixes an issue where the `client-side-negotiated-cipher` access field was incorrectly populated.

Table 481: TCP/IP and General Networking

ID	Issue
SG-12469	Fixes errors in TCP congestion control logic that led to sub-optimal performance. Performance on congested networks has been increased.

Table 482: Web VPM

ID	Issue
SG-12971	Fixes an issue where the web VPM and legacy VPM each showed different options in the **Enable SSL Interception** action object.
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 Response 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 that was 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.
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 that were 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.

SGOS 7.2.0.1 EA

Release Information

- Release Date: January 21, 2020
- Build Number: 246815

NOTE
This release 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 LA release method meant that 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 with access to new and advanced functionality. Early Availability releases are supported like any other current release. Once the Early Availability release achieves broader adoption, it will transition to GA status.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances and ProxySG Tech Docs for platform documentation.

Compatible With

- BCAAA: 6.1
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later
- ProxyAV: 3.4.x
- Content Analysis: 2.3.x, and 3.0.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228

Upgrading To/Downgrading From This Release

- SGOS 7.2.0.1 does not support FIPS mode. Disable FIPS mode **before** you attempt to upgrade to 7.2.1.1. If you begin upgrading to 7.2.1.1 from an appliance that has FIPS mode enabled, abort the upgrade at the boot process, disable

FIPS mode, and attempt the upgrade again. If you upgrade to 7.2.1.1 without disabling FIPS mode, your appliance will not function as expected.

- If you are downgrading from SGOS 7.2.0.1, ensure that after you downgrade your policy includes CPL that protects against low strength ciphers (RC4, CBC, DES, and 3DES). These ciphers are deprecated in 7.2.0.1 and any policy that references them is no longer necessary. For appliances running SGOS that is earlier than 7.2.0.1, use the following CPL:

```
<ssl>
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny

<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5,EXP-DES-CBC-SHA) force_deny
```

- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.2.0.1 from version 6.7.4.3 and later 6.7.x releases, or another version 7.x.
  - Downgrade from 7.2.0.1 to version 6.7.4.3 and later 6.7.x releases, or another version of 7.x.

    NOTE
    If you are upgrading from SGOS 6.7.4.2 or earlier, you might have to upgrade to version 6.7.4.3 as an interim step before upgrading to this release. For more information, refer to KB Article 18536

  See SGOS Upgrade/Downgrade documentation details the supported upgrade/downgrade paths for this release.

    NOTE
    In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.2.0.1

- SGOS 7.2.0.1 introduces new features and enhancements. See Features in SGOS 7.2.1.1.

Fixes in SGOS 7.2.0.1

- This release includes various fixes. See Fixes in SGOS 7.2.0.1.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.2.0.1

SGOS 7.2.0.1 introduces the following features:

- TLS 1.3 Support
- DNS over HTTPS Support
- New CPL Diagnostics Probe and CLI to Upload Diagnostics to Syslog Host

For feature descriptions, see Features in SGOS 7.2.1.1.

Removals and Deprecations

- In some scenarios, the Blue Coat WebFilter service is discontinued.

  If you are upgrading to SGOS 7.2.0.1 and were using Intelligence Services as the data source previously, you will not have the option to use the WebFilter as a data source after you upgrade to 7.2.0.1. The option to set the data source in the Management Console and the CLI command `#(config application-classification)` **`data-source`** `{`**`web-filter`** `|` **`intelligence-services`**`}` have been removed.

  > **NOTE**
  > The appliance can restore a configuration archive that includes WebFilter as a data source, but it issues a deprecation warning.

  If you are running a new installation of SGOS 7.2.x, you will only have the option to purchase Intelligence Services for content filtering. functionality.

  If you are upgrading to SGOS 7.2.0,1 and were using WebFilter as the data source previously, there will be no change to your existing content filtering
- SSLv2 is no longer supported on the appliance. Options for SSLv2 have been removed from the Management Console and the CLI.
- The following ciphers are no longer available:
  - 40- and 56-bit ciphers
  - Export and low strength ciphers:
    - DHE-DSS-DES-CBC-SHA
    - DES-CBC3-MD5
    - RC2-CBC-MD5
    - DES-CBC-SHA
    - DES-CBC-MD5
    - EXP-DES-CBC-SHA
    - EXP-RC4-MD5
    - EXP-RC2-CBC-MD5
    - EXP-DHE-DSS-DES-CBC-SHA

    > **NOTE**
    > If your policy contains reference to the deprecated low strength ciphers, recommends removing the references. If the references are not removed, policy will compile and a warning message will be issued.

  For information on supported ciphers, refer to https://knowledge.broadcom.com/external/article/170130/cipher-suites-shipped-with-the-proxysg-a.html.

Fixes in SGOS 7.2.0.1

SGOS 7.2.0.1 includes bug fixes. This update:

Table 483: HTTP Proxy

ID	Issue
SG-13027	Fixes an issue where server-side HTTP/2 connections were not reused in HTTP/2 in reverse proxy deployments.
SG-15704	Fixes an issue where the appliance did not upgrade new connections to HTTP/2 when ADN was enabled.

Table 484: Performance

ID	Issue
SG-17333	Fixes an issue where the appliance experienced a memory leak in SSL and Cryptography.

Table 485: Policy

ID	Issue
CC-419	Fixes an issue where Content Security Policy exemptions (using the **Set Content Security Scanning** VPM object, set to **Exempt From Content Security**) were not supported in Symantec Web Security Service.
SG-12593	Fixes an issue where requests with "none" category and Threat Risk Level 5 were not blocked when the Access Security Policy layer was configured with Strong protection level.

Table 486: Security

ID	Issue
SG-10271	Addresses Linux Kernel issues. For more information, see SYMSA1467.
SG-15870	Addresses session-hijacking vulnerability in the Management Console. For more information, see SYMSA1752.

Table 487: SSL Proxy

ID	Issue
SG-4574	Fixes an issue where whitespaces in field values were not ignored when adding a keyring through the CLI.

Table 488: SSL/TLS and PKI

ID	Issue
SG-3988	Fixes an issue where client-side negotiated-cipher fields were populated incorrectly in the access log for the SSL reverse proxy service when GCM or SHA384 ciphers were used.

Table 489: CP/IP and General Networking

ID	Issue
SG-12976	Fixes an issue where SGOS on AWS deployments experienced increased HTTP request/response latency when ICAP scanning was enabled.

SGOS 7.1.1.1 EA

Release Information

- Release Date: July 9, 2019
- Build Number: 239238

NOTE
This release 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 LA release method 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 with access to new and advanced functionality. Early Availability releases are supported like any other current release. Once the Early Availability release achieves broader adoption, it will transition to GA status.

Supported Platforms

- ProxySG hardware appliances: S200, S400, S500
- Standard/Advanced Reverse Proxy hardware appliances: S200, S400, S500
- High-performance Gen2 virtual appliances: SG-VA, ARP-VA, SRP-VA

See Hardware Appliances for platform documentation.

Compatible With

- BCAAA: 5.5 and 6.1
- ProxySG Admin Console: 1.1.1 and later
- Reporter: 9.5.x, 10.1.x, and 10.2.x
- Management Center: 2.2.2.3 and later
- ProxyAV: 3.4.x
- Content Analysis: 1.3.x, 2.1.x, 2.2.x, and 2.3.x
- ProxyClient: 3.4.x
- Unified Agent: 4.7.x and 4.8.x
- SSL Visibility: 4.2.x, 4.3.x. 4.4.x, 4.5.x, and 5.x
- Web Isolation: 1.10 and later

Third-Party Compatibility

- For supported Java, operating system, and browser versions, refer to KB Article 169081.
- For information on Java 11 support, refer to KB Article 173228

Upgrading To/Downgrading From This Release

- The following paths are the supported upgrade/downgrade paths for this release:
  - Upgrade to 7.1.x from version 6.7.4.3.
  - Downgrade from 7.1.x to version 6.7.4.3.

  See SGOS Upgrade/Downgrade documentation details the supported upgrade/downgrade paths for this release.

NOTE
In a future release of 7.x, support for WebFilter (BCWF) will be removed.

Changes in SGOS 7.1.1.1

- SGOS 7.1.1.1 introduces new features and enhancements. See Features in SGOS 7.1.1.1.

Fixes in SGOS 7.1.1.1

- Because this release is the inaugural 7.1.x release, Symantec is reporting only the security fix SG-4862 for SGOS 7.1.1.1. SG-4862 patches the open-source OpenSSL library to resolve multiple vulnerabilities. The OpenSSL library is used to implement the SSL protocol.
- To see any Security Advisories that apply to the version of 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 Limitations in SGOS 7.x for a description of limitations in this release.

Known Issues

- See Known Issues in SGOS 7.x for a list of all issues that Symantec is aware of in SGOS 7.x.

Features in SGOS 7.1.1.1

SGOS 7.1.1.1 introduces the following features. For feature descriptions, see Features in SGOS 7.2.6.1.

NOTE
Some features were available in a limited 6.8.x beta release.

- Web Visual Policy Manager
- Policy Services Subscription and Security Policies
- HTTP/2 Support
- Origin Header Categorization Policy
- Brotli Encoding Support
- OCSP Stapling for Forward Proxy
- Syslog Supports TCP and TLS
- Authenticated NTP
- SSH Enhancements
  - SSHv2 Host Key Pairs for the SSH Console
  - SSH and SSH KEX Host Key Algorithms for the SSH Console
- SCP Upload Configuration Archives
- Periodic Upload of Configuration Archives
- Periodic Upload of Service Information
- Server-Side Encrypted Tap
- Diagnostic Policy Support
- Enhanced Policy Variables Tests
- Policy for Positive Security Controls
- Client IP Reputation Policy
- ProxySG SWG VA for Microsoft Azure
- Feature Changes and Enhancements

- – Geolocation Policy Supports Renamed Countries
- – Geolocation Lookup Supports IPv6
- – Renamed Application Attribute Support
- – Renamed Category Name Support
- – Default TCP Window Size Increase
- – CPU Monitor Enabled by Default

Deprecations and Removals

These deprecations and removals apply when upgrading to version 7.1.x.

- DES and DES3 are no longer available for the `#(config ssl)`**`view keypair`** and `#show ssl keypair` commands. To display keypairs in an encrypted format, specify either aes128-cbc or aes256-cbc, for example:

  ```
  #(config ssl)view keypair aes256-cbc
  keyring_id
  ```

- The `#(config)`**`security destroy-old-passwords`** and `#(config socks-gateway)`**`destroy-old-passwords`** commands have been removed.
- For best security, SSHv1 commands have been removed from the CLI.
- Built-in malware scanning policy in previous versions of SGOS (previously in **Proxy > Configuration > Threat Protection > Malware Scanning**) has been removed. Use Content Security Policy with the Policy Services subscription instead. See **CC-419** in Known Issues in SGOS 7.x for a known issue when using Content Security Policy with Universal Policy enforcement.
- IM Proxies have been removed from the Management Console and CLI.
- The following platforms are no longer supported:
  - – SG300, SG600, SG900, and SG9000 physical appliances
  - – SWG-V100 (Gen1) virtual appliances
  - – MACH5 (Gen1) virtual appliances

SGAC Releases in SGOS

View the release notes for Edge SWG Admin Console (SGAC) releases.

The Admin Console is the next-generation web interface for the Edge SWG appliance. If you have a Management Center appliance, you can deploy the Admin Console as a standalone product. For more information, see the Admin Console documentation.

SGAC 2.2.3

SGAC 2.2.3 was released on July 17, 2024 and was first included in the following SGOS releases:

- SGOS 7.3.21.1
- SGOS 7.4.5.1

SGAC 2.2.3 includes the following features and fixed issues:

New Category Details Report

You can now view and sort details for the category that the appliance assigned to the sites it accessed, such as the number of hits for the different categories, or the composition of the hits for each category. To view Category Details, in the Admin Console, navigate to **Reports** > **Category Details**. You can find the following details on the Category Details page:

- **Category Hits:** This bar graph allows you to view and sort the number of hits for each category over the selected time period.
- **Category Composition:** This pie chart gives you a visual representation of the hits for each category over the selected time period. You can hover over the pieces of the chart to see the exact percentage of hits the group received.
- **Category Details:** This table allows you to sort data by the number of hits, and filter on each column for specific text and numbers.

More information:

- SGAC Admin Guide

New Group Filter for Threat Risk Details

On the Threat Risk Details report page (**Reports** > **Threat Risk Details**), you can now filter every chart and table on the page by a specific group. To filter the data on the page by a specific group, click the **Group** dropdown and select a group.

HSM Keylists Renamed to Keygroups

HSM keylists have been renamed to HSM keygroups. No changes to functionality have been made. Configure HSM keygroups in the Admin Console under **Configuration** > **SSL** > **HSM**.

Table 490: Fixes in 2.2.3

ID	Issue
SWGMGT-9708	Fixes an issue where you could create invalid password policy in the SGAC (**Configuration** > **Authentication** > **Password Policy**) that could not be saved. For example, if you created policy where the sum of the requirements was greater than the 64-character limit, the SGAC would not notify you that the policy was invalid. Now, if you create invalid password policy, the **Save** button is disabled and an error message displays.
SWGMGT-9639	Fixes an issue where the SGAC accepted strings for forwarding hostnames (**Configuration** > **Networking** > **Forwarding Hosts**) that were not compatible with Edge SWG specifications. Now, if you attempt to add an invalid hostname, a warning message appears and the SGAC cannot create the host until the hostname is corrected.

SGAC 2.2.2

SGAC 2.2.2 was released on May 21, 2024 and was first included in the following SGOS releases:

- SGOS 7.3.20.1
- SGOS 7.4.4.1

SGAC 2.2.2 includes the following features and fixed issues:

New Threat Risk Details Report

You can now view and sort details for the level of risk that the appliance assigned to the sites it accessed. Before you can view details on threat risk levels, you must have Threat Risk Levels enabled and have the Threat Risk Levels database downloaded. To view Threat Risk details, in the Admin Console, navigate to **Reports** > **Threat Risk Detail**. You can find the following details on the Threat Risk Details page:

- **Threat Risk Levels Hits**: This bar graph allows you to view and sort the number of hits for each Threat Risk level.
- **Threat Risk Composition**: This pie chart gives you a visual representation of the hits for each Threat Risk level. You can hover over the pieces of the chart to see the exact percentage of hits the level received.
- **Threat Risk Details**: This table allows you to sort data by the number of hits, and filter on each column for specific text and numbers.

More information:

- SGAC Admin Guide

Filter on the Access Log

To easily filter for specific log lines in access logs, you can now apply filters in the Admin Console from the page **Reports** > **Access Logging**. You can add multiple parameters to the filter. If you add multiple parameters, the Admin Console displays lines that contain all the values. You can only apply a filter when the **Log Tail Refresh Interval** is set to **continuous**.

More information:

- SGAC Admin Guide

Option to Select CCL and ECL for Certificates

When importing CA certificates or external certificates, you can now simultaneously add them to their respective CCL or ECL. Before you can assign a CCL or ECL, the CCL or ECL must exist. To manage your CA certificates, in the Admin

Console, navigate to **Configuration** > **SSL** > **CA Certificates**. To manage your external certificates, in the Admin Console, navigate to **Configuration** > **SSL** > **External Certificates**.

More information:

- Manage CA Certificates
- Manage External Certificates

Table 491: Fixes in 2.2.2

ID	Issue
SWGMGT-9358	Fixes an issue where the mode could not be saved for a hardware bridge on the Adapters page.
SWGMGT-9514	Fixes an issue where the Content Filtering page displayed the incorrect categories when testing a URL that contained "http" or "https." This issue only occurred when the SGAC was launched from Management Center.

SGAC 2.2.1

SGAC 2.2.1 was released on April 1, 2024 and was first included in the following SGOS releases:

- SGOS 7.4.3.1
- SGOS 7.3.19.1

SGAC 2.2.1 includes the following features and fixed issues:

Configure Notification Overrides for SNMP

You can now configure default settings and overrides for event log notifications that are sent over SNMP.

More information:

- SGAC Admin Guide

New Warning for Auto-Logout

To warn inactive users that they're about to be automatically logged out, a warning message displays in the Admin Console. Inactive users are only automatically logged out if you have the web auto-logout feature enabled.

Table 492: Fixes in 2.2.1

ID	Issue
SWGMGT-9278	Fixes an issue where IPv6 DNS servers configured for a DNS forwarding group were not being displayed in SGAC. Attempting to load the Health Checks page with a health check for an IPv6 DNS server resulted in a "Bad Configuration" error in SGAC preventing health checks from being configured.
SWGMGT-9308	Fixes an issue where a proxy service listener with an IPv6 address and a /128 prefix length added through the CLI was incorrectly displayed in SGAC with a /32 prefix length, and could not be edited.
SWGMGT-9323	Fixes an issue where the Access Logging "Test Format" action in SGAC was incorrectly returning a "Format Syntax incorrect" error.
SWGMGT-9354	Fixes an issue where attempting to add a certificate containing the Authority Key Identifier extension to a keyring sometimes resulted in a ”Bad certificate” error, preventing the certificate from being applied.

ID	Issue
SWGMGT-9472	Fixes an issue when editing a health check, where the 'Log A Transition To Sick As' event logging default notification setting was mislabeled as 'Log A Transition To Healthy As".

SGAC 2.1.5

SGAC 2.1.5 was released on November 9, 2023 and was first included in the following SGOS releases:

- SGOS 7.4.1.1
- SGOS 7.3.17.1

SGAC 2.1.5 includes the following features and fixed issues:

- The health monitoring metric for HTTP client utilization provides the percentage of the maximum number of simultaneous HTTP client sessions that the appliance is processing. You can view the HTTP Client Utilization in the Admin Console (**Reports > Health Monitoring > General**).
- View statistics for proxied sessions and bypassed connections (**Reports > Sessions**). You can terminate and clear historical errored sessions for proxied sessions. You can also download information for both proxied sessions and bypassed connections. The **Sessions** page replaces the **Active Sessions** page.
- Ensure your local passwords on the Edge SWG appliance are secure and strong (**Configuration > Authentication > Password Policy**). Enforce requirements, such as minimum length, characters used, the number of passwords the appliance saves to compare new passwords against, and whether common words or whitespace are allowed.
- Configure an SSL device profile and username for the SSL device when configuring SMTP email notifications (**Administration > Logging > Event Logging**).

Table 493: SGAC 2.1.5

ID	Issue
SWGMGT-8827	Fixes an issue where the maximum character limit was incorrect for interfaces and VLANs.
SWGMGT-8928	Fixes an issue where the packet capture was missing the minimum size limit.
SWGMGT-8941	Fixes an issue where a large list of forwarding hosts caused the page to not finish loading.
SWGMGT-8974	Fixes an issue where a success message incorrectly displayed when the configuration install was unsuccessful.
SWGMGT-8993	Fixes an issue where the tasks page did not finish loading.
SWGMGT-9068	Fixes an issue where the DNS forwarding group reported misleading "Bad Configuration" error.
SWGMGT-9107	Fixes an issue where the Kerberos Credentials dialog did not display the current username.
SWGMGT-9110	Fixes an issue where the Admin Console could not finish testing the configuration of the realms and domains.
SWGMGT-9137	Fixes an issue where the misleading error message "Sequence not supported in this version" displayed.
SWGMGT-9139	Fixes an issue where the system health status did not refresh.
SWGMGT-9149	Fixes an issue where the proxy services did not finish loading.
SWGMGT-9157	Fixes an issue where the adapter link speed did not display correctly.

SGAC 2.1.4

(With SGOS 7.3.14.1) the SGAC has no new features and only fixes. See Fixes in SGOS 7.3.14.1.

SGAC 2.1.3

(With SGOS 7.3.14.1) the SGAC has no new features and only fixes. See Fixes in SGOS 7.3.14.1.

SGAC 2.1.2

(With SGOS 7.3.12.1) You can launch the SGAC from the appliance. Previously, SGAC was available in Management Center only. Refer to the following documentation:

- KB 251426: https://knowledge.broadcom.com/external/article/251426

SGAC 2.1.1

Refer to the following documentation:

- 2.1.1 features and changes: https://support.broadcom.com/external/content/ReleaseAnnouncements/0/21104
- KB 251426: https://knowledge.broadcom.com/external/article/251426

SGAC 1.2.4

(With SGOS 7.3.8.2) The SGAC has the following new features:

- When creating self-signed certificates and certificate signing requests (CSRs), you can specify values for the following extensions:
  - Subject Alternative Name
  - Basic Constraints
  - Key Usage
  - Extended Key Usage

  When viewing the certificate, the extensions are displayed in an **Extensions** section (**Configuration > SSL > CA Certificates**).
- Configure Certificate Revocation Lists (CRLs) to check certificates against CA-provided lists of invalid and expired certificates (**Configuration > SSL > CRLs**).
- Import external certificates, for which Symantec does not have the private key, to the appliance and manage external certificate lists (**Configuration > SSL > External Certificates**).
- Specify a range of SSL/TLS versions to use for all intercepted SSL connections (**Configuration > Services > SSL Proxy Settings**). Select minimum and maximum SSL/TLS protocol versions for client connections and server connections.

  To support this feature, when configuring the SSL client, device profile, reverse proxy listener service, and HTTPS management service, you must specify a contiguous range of SSL/TLS versions (for example, TLSv1.1, v1.2, and v1.3). If you specify only TLSv1.3 and v1.1, for example, you receive an error "SSL versions must be contiguous" and cannot save the configuration.
- Keep the central policy file up to date by automatically downloading a new file when it is updated, and receiving email notifications if a policy file change. You can view and update policy files on the appliance and view the policy source (**Configuration > Policy > Policy Options**).
- Enable SNMP functionality on the appliance and configure SNMPv1, SNMPv2c, or SNMPv3 to monitor network devices for health or status conditions (**Administration > SNMP > SNMP**).
- View and edit settings for system, licensing, status, and subscription metrics (**Administration > Health Checks and Monitoring > Health Monitoring**).
- Configure global event logging settings such as maximum event log file size, SMTP server, and Syslog loghosts. You can also select different event logging levels for Syslog and email and specify overrides (**Administration > Logging > Event Logging**).
- Perform routine and troubleshooting tasks such as restart, shutdown, clearing caches, and resetting the system (**Administration > General > Task**

The System Image Catalog (**Administration > Systems > Software System Images**) is updated:

- The list of system images now shows the index number for each system.
- The **Signed** column has been removed from the list (all system images are signed).

SGAC 1.2.3

(With SGOS 7.3.6.1) The SGAC has the following new features:

- Manage HTTP, HTTPS, SSH, SNMP, and Telnet services for administrative access to the ProxySG appliance.
- Configure SOCKS gateways and gateway groups for forwarding.
- Manage the SSL client profile of the appliance.
- Offload processing of SSL/TLS traffic to a configured SSLV device.
- Add existing Online Certificate Status Protocol (OCSP) OCSP responders to perform real-time certificate revocation checks and send responses to the appliance.

In addition, forwarding host lists have been renamed to forwarding groups.

SGAC 1.2.2

(With SGOS 7.3.4.1) The SGAC has the following new features:

- You can configure a UDP Tunnel proxy service.
- A new MS Teams proxy service is available in **Proxy Services** (**Configuration > Services**).
- As of version 7.3.2, proxy service listeners now support two more default actions:
  - drop: Silently drops matching incoming packets.
  - reject: Responds to the sender indicating that the packet was rejected.
- You can now send the following header information in ICAP requests. Configure an ICAP service (**Administration > ICAP > ICAP Services**):
  - `X-SYMC-Groups`
  - `X-SYMC-User-Email-Address`
- Global policy tracing is now available under **Administration > Service Information > Policy Tracing**.
- You can enable policy coverage (**Configuration > Policy > Policy Options**).
- You can enable or disable parallel DNS lookups using RFC8305 (Happy Eyeballs algorithm).
- A Troubleshooting report, which summarizes the current statuses of packet capture and policy tracing, has been added to the **Dashboards** view.
- You can configure virtual IP addresses and failover groups (**Configuration > Network > Advanced**).
- The **Administration > Upgrade** page has been renamed to **Administration > Systems > Software System Images**.

SGAC 1.2.1

(With SGOS 7.3.2.1) The SGAC has the following new features:

- Statistics graphs have been added (**Dashboards > Home**).
- Explicit HTTP and External HTTP services now include an **Expect Proxy Protocol**.
- Isolation configuration (**Administration > Data Services > Isolation**) supports sending the **Appliance ID** in the HTTP headers of traffic that is forwarded to the isolation service.

SGAC 1.1.3

(With SGOS 7.3.1.1) The SGAC has the following new features:

- SAML authentication realm configuration
- geolocation configuration
- Web Isolation configuration

SGAC 1.1.2

(With SGOS 7.2.2.1) The SGAC has the following new features:

- Health checks
- Service info and snapshot jobs
- IWA, LDAP, and RADIUS authentication realms
- Thales Luna HSM integration
  Refer to Symantec HSM Agent 2.x documentation for details on HSM configuration.
- SSH inbound connections
- SSH outbound connections

SGAC 1.1.1

The initial release of the SGAC coincided with the SGOS 7.2.1.1 GA.

Web VPM Releases in SGOS

View the release notes for Web Visual Policy Manager (VPM) releases.

The Web VPM is a graphical policy editor that is included with the Edge SWG appliance. If you have a Management Center appliance, you can deploy the Web VPM as a standalone product. See the Web VPM documentation.

Web VPM 2.2.3

Web VPM 2.2.3 was released on July 17, 2024 and was first included in the following SGOS releases:

- SGOS 7.3.21.1
- SGOS 7.4.5.1

Web VPM 2.2.3 includes the following features and fixed issues:

New Action Objects for Web Access Layer

In the Web Access layer, the following static action objects are now available:

- Log out/Do Not Log out Other Users With Same IP
- Log out/ Do Not Log out User
- Log out/ Do Not Log out User’s Other Sessions

More information:

- Web Access Layer: Action Objects
- Static Action Objects
- Action Column/Policy Layer Matrix

New Permit SOCKS Authentication Error Object

The Permit SOCKS Authentication Error object is available from the Action column of the SOCKS Authentication layer. Use this action object to allow or deny transactions that could not be authenticated to proceed based on the authentication error.

More information:

- Web Visual Policy Manager Reference

New Combined Action Objects for SOCKS Authentication Layer

For the SOCKS Authentication layer, combined action objects are now available.

More information:

- SOCKS Authentication Layer: Action Objects
- Combined Action Object
- Action Column/Policy Layer Matrix

Table 494: Fixes in Web VPM 2.2.3

ID	Issue
SWGMGT-9729	Fixes an issue where the Web VPM was slow to open the window to add objects to layers that contained many rules. Also, the options in dropdowns were not immediately highlighted when the cursor moved over them.
SWGMGT-9926	Fixes an issue where the policy objects did not load properly in the "All Objects" modal.
SWGMGT-9966	Fixes an issue where the `group.log_order` definition doubled in the generated CPL when policy was saved in the Web VPM.
SWGMGT-9981	Fixes an issue where the Subject Directory Attributes (**Configuration** > **Subject Directory Attributes**) were duplicated when policy was saved in the Web VPM.
SWGMGT-10028	Fixes the following issues for large policies with numerous nested objects: • Loading layers and rules took more than a minute for large policies. • Loading policy objects took between 5 seconds to one minute. While objects were loading, the Web VPM was unresponsive. • Adding or editing objects (including combined objects) in a rule took longer than expected. When you attempted to add or edit an object, the Add or Edit window would take up to 2 seconds to display or close.

Web VPM 2.2.2

Web VPM 2.2.2 was released on May 21, 2024 and was first included in the following SGOS release:

- SGOS 7.3.20.1
- SGOS 7.4.4.1

Web VPM 2.2.2 includes the following fixed issues:

Table 495: Fixes in Web VPM 2.2.2

ID	Issue
SWGMGT-8894	Fixes an issue where creating a list for shared object URLs with the option **Use server_url.* triggers instead of url.* triggers** selected resulted in an empty define condition in the generated CPL policy.
SWGMGT-9195 SWGMGT-9504	Fixes an issue where you could not scroll to the bottom of the page when there were more rules in a layer than could be displayed on the screen.
SWGMGT-9217 SWGMGT-9363	Fixes an issue where the remove and modify icons for the name of the Request URL Category rule appeared on the next line of the Category Objects list. This issue occurred when the name was long and the list contained multiple categories.
SWGMGT-9220	Fixes an issue where an extra enforcement tag was not added to the CPL policy generated by the Web VPM when policy contained a Socks Authentication layer.
SWGMGT-9399	Fixes a Stored Cross Site Scripting (XSS) vulnerability in the confirm modal of the Subject Directory Attributes.
SWGMGT-9518	Fixes an issue where a warning message for a rule prevents you from selecting the preceding rule.

Web VPM 2.2.1

Web VPM 2.2.1 was released on April 1, 2024 and was first included in the following SGOS releases:

- SGOS 7.4.3.1
- SGOS 7.3.19.1

Web VPM 2.2.1 includes the following fixed issues:

Table 496: Fixes in Web VPM 2.2.1

ID	Issue
SWGMGT-8722	Fixes an issue where the request URL object was not selectable in the destination field of the rule and was unable to set it in the rule.
SWGMGT-8915	Fixes an issue where the same name categories from different providers were not selected properly in the category object.
SWGMGT-8925	Fixes an issue where excluded URL categories in a category object resulted in incorrect CPL and caused an 'unknown category' warning.
SWGMGT-8982	Fixes an issue where CPL was not generated properly for a condition name with spaces, which caused an error when installing the policy.
SWGMGT-9019	Fixes an issue where user roles with "all objects: view" and "VPM Policy Edit: view, View generated CPL, view objects" were not able to view the details of the rule.
SWGMGT-9374	Fixes an issue where the "SSL intercept with protocol detection" option on the Enable SSL Interception object resulted in the warning "Unreachable statement (previous policy rule always matches)", and the warning "'detect_protocol() is deprecated in <SSL-Intercept> layers".
SWGMGT-9409	Fixes an issue where excluded URL categories in a category object resulted in incorrect CPL and caused an 'unknown category' warning.

Web VPM 2.1.6

Web VPM 2.1.6 was released on June 11, 2023 and was first included in the following SGOS releases:

- SGOS 7.4.1.1
- SGOS 7.3.14.1

Web VPM 2.1.6 includes the following features and fixed issues:

- You can now search all levels of nested objects.
- Installing policy that includes the Set Effective Client IP object no longer triggers a deprecation warning.

Table 497: Fixes in Web VPM 2.1.6

ID	Issue
SWGMGT-4809	Fixes an issue where the VPM combined warning messages and incorrectly reported there was a duplicated layer. This issue occurred when the isolation service was disabled and policy included an isolation action.
SWGMGT-8528 SWGMGT-8826 SWGMGT-8863	Fixes an issue where the VPM incorrectly limited the maximum number of characters for the Set/Edit value for 'Control Request Header' and 'Control Response Header'.
SWGMGT-8551	The following documentation has been updated to include information on an issue where policy does not install when "SSL intercept with protocol detection" and "Disable SSL Intercept" are within the same layer: • https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/visual-policy-manager/action-column-objects/enable-ssl-interception.html • https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/overview/_properties/ssl-forward_proxy.html

ID	Issue
SWGMGT-8671	Fixes performance issues that occurred when trying to perform any action in 'Set Object'.
SWGMGT-8686	Fixes performance issues that occurred when saving policy.
SWGMGT-8943	Fixes an issue where editing policy caused rules to reorder.

Known Issues in Web VPM

Symantec is aware of the following issues in the Web VPM.

ID	Issue	Fixed In
SG-28393	When web VPM is launched outside of the Management Center, long comments content is no longer replaced with ellipsis (...) and tooltip location is off.	Fixes in SGOS 7.3.8.1
SWGMGT-9374 SG-29819	Selecting the "Enable SSL interception with automatic protocol detection" option in the **SSL Interception** VPM object generates a non-working policy.	Web VPM 2.2.1
SWGMGT-10341	**Issue:** In Web VPM 2.2.4, agents and versions of agents were removed from the User Agent object (see Web VPM 2.2.4). If you create policy using Web VPM 2.2.3 or earlier that uses the removed agents and agent versions, and you upgrade to 2.2.4 or later, those agents and versions are still available in the objects (while editing the old objects) that were present before the upgrade. Those agents and versions should not be available in new objects (while setting new objects in rules), but they are appearing as options. **Workaround:** Do not use the removed agents and agent versions in new objects. If your policy requires matching to removed agents or versions, use the **User Agent Match** object and, for the **Browser Type**, select **Other**. You can then use the **Supplemental RegEx** field to specify the agent to match against.	
SWGMGT-9548	When you save policy that contains more than 1900 rules in each layer, the Web VPM does not indicate it is saving the files. The Web VPM only indicates that the save is complete.	
SWGMGT-9572	The following known issue affects Web VPMs containing policy files that have more than 2000 rules per layer. When you set or edit a rule, the window appears after a two-second delay. When you save changes that you made to a gesture or object, the window closes after a few seconds of a delay.	
SWGMGT-9962	When you duplicate a layer, the components in the layer are duplicated except for any comments in the rules.	
SWGMGT-10230	When scrolling through a long list of rules, the rule headers are not static at the top of the columns.	
SWGMGT-10250	In Firefox browsers, when you load policy, or set or edit policy in Combined Object windows, the spinner wheel is static. This issue may cause users to think that the Web VPM is frozen.	
SWGMGT-10252	When you save policy, the Web VPM does not capture some errors that occur during the save. The error appears for a few seconds near the top-right corner of the screen and disappears. For example, the error message `Error: Object XSOAR has been removed but it is still referenced. The rule referencing this object must be removed` might appear on the screen but does not appear in the Problem section. This issue may lead to confusion over what error occurred and whether the policy was saved.	

SGOS 7.x Reference Information

The following sections provide reference information for the SGOS 7.x software series.

- SGAC Releases in SGOS
- Web VPM Releases in SGOS
- Known Issues in SGOS 7.x
- Limitations in SGOS 7.x
- Documentation and Feedback

Known Issues in SGOS 7.x

Symantec is aware of the following issues in SGOS 7.x.

Table 498: Admin Console

ID	Issue	Fixed In
SWGMGT-8936 SWGMGT-8890 SG-34702	**Issue:** In 7.3.12.1 and later, when you launch the web-based SG Admin Console from the ProxySG appliance, the SG Admin Console does not log users out when the session reaches the web-timeout threshold. This issue does not affect the Java-based management console. **Workaround:** Do one of the following workarounds: • If you launched the SG Admin Console from the appliance and have finished using it, manually log out of the SG Admin Console. • Only use Management Center to launch the SG Admin Console and the appliance will log you out when the session reaches the web-timeout threshold.	
SGAC-2842	**Issue:** When adding an interface in a Web Cache Service Group, the first value in the dropdown list appears to be selected even though it is not selected. This issue occurs when using Safari. **Workaround:** To select the first interface in the list, select another interface and then select the first interface again.	

Table 499: Authentication

ID	Issue	Fixed In
SG-20312	In SGOS 7.2.1.1, CAPTCHA forms are not displayed when the appliance invokes CAPTCHA validators in policy. If you are currently using CAPTCHA validators in policy, do not upgrade to 7.2.1.1. If you are installing 7.2.1.1, do not write policy that uses CAPTCHA validators.	Fixes in SGOS 7.2.2.1

Table 500: Boot

ID	Issue	Fixed In
SG-32627	Upon bootup, the appliance stops responding before rebooting successfully. This issue occurs infrequently.	Fixes in SGOS 7.3.11.1

Table 501: CLI Consoles

ID	Issue	Fixed In
SG-23745	A memory leak occurs when there is an SSH host key mismatch between the appliance and Management Center (for example, if the SSH host keypair is deleted and recreated after the appliance is added to Management Center).	Fixes in SGOS 7.3.2.1

Table 502: FTP Proxy

ID	Issue	Fixed In
SG-4624	When ICAP REQMOD mirroring is enabled for the FTP proxy, the `s-action` access log field is occasionally not populated.	Fixes in SGOS 7.3.2.1
SG-13013	Encrypted Tap does not contain any FTP data for intercepted FTPS connections.	

Table 503: HTTP Proxy

SG-30438	CPU usage may be increased by 3% due to HTTP performance. For more information, see KB article 235104.	Version 7.3.9.1 addresses this performance issue.
SG-28290	When server-side persistence is disabled either by policy or by ProxySG configuration, the appliance does not release memory for HTTP/2 connections. Not releasing memory can result in high memory usage and may eventually require a restart to correct. **Workaround:** Either enable HTTP-server persistence or disable the server-side HTTP/2 proxy with the policy property `http2.server.request(no)` .	Fixes in SGOS 7.3.6.1
SG-15704	When ADN is enabled, the appliance does not upgrade new connections to HTTP/2; however, if ADN is enabled when there are existing HTTP/2 connections open, the existing HTTP/2 connections could break or cause crashes.	Fixes in SGOS 7.2.0.1
SG-15679	For HTTP/2 connections, the active session is associated with individual streams in the connection and ends when the stream is released, which causes idle HTTP/2 connection to not display in the Active Sessions.	

Table 504: Java Management Console and Java VPM

ID	Issue	Fixed In
SG-36758	**Issue:** The certificate chain used to code sign the Java Management Console and Java VPM was updated in June 2023. However, the chain references a root CA which is not yet included by default in the Java trust store. Because the CA is not included, the chain reports security errors when you access the Java Management Console and Java VPM. The following versions of SGOS are affected by this issue: • 7.3.16.1 • 7.3.15.2 • 7.3.15.1 • 7.3.14.3 • 7.3.13.4 • 6.7.5.24 In upcoming releases of SGOS, the code-signing certificate chain will be updated to use a root CA that is present by default in the Java trust store. **Workaround:** To allow Java to trust SGOS releases that are signed with the June 2023 signing chain, see https://knowledge.broadcom.com/external/article/270160.	Fixes in SGOS 7.3.16.2 Fixes in SGOS 7.3.15.3 Fixes in SGOS 7.3.14.4 Fixes in SGOS 7.3.13.5

Table 505: Kernel

ID	Issue	Fixed In
SG-21332	Secure Web Gateway virtual appliances running on Hyper-V or Microsoft Azure platforms sometimes experience lower throughput and performance (up to 10%) compared to other virtualization environments.	Fixes in SGOS 7.2.2.1

Table 506: Policy

ID	Issue	Fixed In
SG-24288	In 7.2.4.1, authenticating traffic via NTLM with BCAAA does not work.	Fixes in SGOS 7.3.2.1 Fixes in SGOS 7.2.5.1
SG-17978	If you are using LDAP authentication and have installed policy to display a redirect link, the redirect link does not display the correct URL in the address bar.	Fixes in SGOS 7.2.2.1
SG-18066	After installing 7.2.1.1, if you previously didn't use policy quota and had it disabled in configuration, and then attempted to enable it and install time quota policy via either the Legacy VPM or Web VPM, policy does not compile and the CPL displays the error message "Error: Variable Linker Error: variable not defined: 'variable.time_quota_limit(5)'". A similar error occurs when attempting to install volume quota policy. **Workaround:** Downgrade to the latest version of 6.7.x, enable policy quota, and then upgrade to 7.2.1.1.	Fixes in SGOS 7.2.2.1
CC-419	Content Security Policy exemptions (using the **Set Content Security Scanning** VPM object, set to **Exempt From Content Security**) are not supported in Symantec Web Security Service. Do not use this setting in policy rules when using Universal Policy enforcement.	Fixes in SGOS 7.2.0.1
SG-12593	When the Access Security Policy layer is configured with Strong protection level, requests with "none" category and Threat Risk Level 5 are not blocked, but the access log incorrectly states they are blocked.	Fixes in SGOS 7.2.0.1

ID	Issue	Fixed In

SG-4058	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)`	

SG-28416	Poor hash algorithm causes false match and incoherent warnings on specific policy rules.	Fixes in SGOS 7.3.7.1

Table 507: Proxy Forwarding

ID	Issue	Fixed In
SG-23770	Upgrading from version 7.2.x to 7.3.x with an existing web isolation policy causes web isolation to stop working, with web pages that should be isolated displaying a "No connectivity to the proxy server" message.	Fixes in SGOS 7.3.2.1

Table 508: SSL Proxy

ID	Issue	Fixed In
SG-13014	FTPS uploads using Filezilla fail with error code 1048576. This issue occurs when OCSP stapling is enabled on the appliance.	
SG-4230	In STunnel and Bypass modes, the `x-cs-session-id` and `x-cs-server-certificate-key-size` access log fields are not populated.	
SG-3605	The appliance stops responding when the CRL distribution point host name field (**Configuration > Proxy Settings > SSL Proxy**) includes special characters.	
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.	
SG-4373	On a resumed connection, the `x-cs-server-certificate-key-size` access log field always displays RSA[1024].	
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.	Fixes in SGOS 7.2.0.1 Fixes in SGOS 7.2.1.1

Table 509: SSL/TLS and PKI

ID	Issue	Fixed In
SG-28279	For ADN deployments, the appliance sometimes experiences high memory usage when processing SSL traffic.	Fixes in SGOS 7.3.6.1
SG-17567	If the appliance reaches the maximum number of HTTPS connections via SSL tunnel and detect protocol is enabled, memory usage per connection increases significantly.	Fixes in SGOS 7.2.2.1

SG-4598	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-11173	When upgrading from SGOS 6.7.x, the event log displays errors about HSM keyrings and external certificates. These messages are inaccurate, and there are no issues with the HSM keyring or external certificate.	Fixes in SGOS 7.3.1.1
SG-4583	Loading signed configuration files on the ProxySG virtual appliance fails with an error: `% Attempt to load configuration failed: signature verification failed: The message did not match the PKCS7 signature.`	
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.	Fixes in SGOS 7.2.0.1

Table 510: SSLV Integration

ID	Issue	Fixed In
SG-4612	When SSLV is enabled, SSL access log fields report SSLV cipher values instead of ProxySG values. This issue occurs when certain cipher enforcement conditions exist in policy. For example, instead of displaying `AES256-SHA` a field shows `RSA-AES256-CBC-SHA`.	
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.	

Table 511: TCP/IP and General Networking

ID	Issue	Fixed In
SG-12976	SGOS on AWS deployments experience increased HTTP request/response latency when ICAP scanning is enabled.	Fixes in SGOS 7.2.0.1
SG-28822	The connection pair of a transparent IPv6 session via SSLV will reuse the same TCP source port if 'reflect client IP' option is enabled. This is a regression caused by some UDP-Tunnel changes in 7.3.4	Fixes in SGOS 7.3.7.1

ID	Issue	Fixed In
SG-36503	When tcp-fast-finwait2-recycle is enabled, TCP connections close after the maximum idle time is reached (usually ten minutes) instead of closing when the specified idle time is reached (usually one minute). This behavior is the same as having tcp-fast-finwait2-recycle disabled.	

Table 512: URL Filtering

ID	Issue	Fixed In
SG-25492	Purging the databases of Intelligence Service subscription services changes the previously-configured download method.	Fixes in SGOS 7.3.4.1

Limitations in SGOS 7.x

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.

FIPS Mode

This release is based on OpenSSL 1.1.1, which does not support FIPS 140-2. As a result, this release is not FIPS-capable. Attempting to use the `# fips-mode enable` command results in the message:

```
% Current system image is not FIPS capable.
% Cannot enter FIPS mode. See attributes in "show installed-systems".
```

Importing CA Certificates

The Management Console allows you to import a CA certificate with an empty name. Make sure that all imported CA certificates have names. (SG-10474)

Keyring and Keylist Limitations

- The appliance does not correctly distinguish letter cases when creating SSL and HSM keyrings and keylists. For example, you can create a keyring named "Default", which is similar to the "default" keyring. If you attempt to delete "Default", you receive an error "% Keyring is referenced by one or more [service]."

  To avoid this issue, do not create keyring/keylist names that are differentiated from system keyring/keylist names only by letter case. (SG-20495,20497,20498)
- When creating a keyring through the Management Console, you can include parentheses "( )" in the keyring name; however, attempting to select the keyring in VPM policy produces an "unknown keyring" error.

  To avoid this issue, do not include parentheses in keyring names. (SG-2700)
- When configuring a keylist through the CLI, you can add keyrings whose certificate Common Names are differentiated only by whitespace, such as " www.example.com" and "www.example.com". To avoid this issue, use the Management Console to configure keylists. (SG-4574,4575)

TLS

TLS 1.3 connections over ADN will be downgraded to TLS 1.2.

Documentation and Feedback

Refer to the following documentation and feedback options.

Documentation

Table 513: SGOS documentation

Document	Description
SGOS Upgrade/Downgrade	Steps for upgrading or downgrading SGOS. Also covers behavior changes and policy deprecations.
SGOS Administration Guide	Detailed information for configuring and managing the appliance.
Command Line Interface Reference	Commands available in the appliance CLI and how to use them to perform configuration and management tasks.
ProxySG Web Visual Policy Manager Reference	How to create and implement policy in the appliance's web-based Visual Policy Manager, including layer interactions, object descriptions, and advanced tasks.
Content Policy Language Reference	CPL gestures available for writing the policy by which the appliance evaluates web requests.
Required Ports, Protocols, and Services for Symantec Enterprise Security Products	Basic configurations, and some commonly used options, for ports and protocols.
ProxySG Security Best Practices	Best-effort security considerations for your deployment.
Hardware documents	Quick start guides, safety guides, and other hardware documentation. Refer to these release notes for supported platforms.
Appliance online help (**Help** button)	Access online help from within the Management Console or Admin Console; however, note that documentation posted on MyBroadcom supersedes online help.

Provide Feedback

- Send any questions or comments about documentation: documentation.inbox@broadcom.com
- For Customer Care requests, go to: https://www.broadcom.com/company/contact-us/feedback-and-comments

Documentation Legal Notice

Symantec™

by Broadcom Software