Advanced Secure Gateway 6.7.x Release Notes

Version 6.7.x

Guide Revision: 6/17/2020

Symantec

Release Note Directory

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

Release Index

Information About All Releases

Advanced Secure Gateway 6.7.5.5 GA

Release Information

- **Release Date:** June 17, 2020
- **Build Number:** 251829

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.1 build 249992. Refer to Content Analysis documentation on myBroadcom for more information.

Third-Party Compatibility

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

  https://knowledge.broadcom.com/external/article/169081/supported-java-operating-system-and-brow.html

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to Article ID 173228:

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

Upgrading To/Downgrading From This Release

- After upgrading to Advanced Secure Gateway 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://knowledge.broadcom.com/external/article?legacyId=TECH254549

Fixes in Advanced Secure Gateway 6.7.5.5

- Advanced Secure Gateway 6.7.5.4 includes a critical fix. See "Fixes in Advanced Secure Gateway 6.7.5.5" on the next page.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway 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 "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.5.5

Bug Fixes in this Release

Advanced Secure Gateway 6.7.5.5 includes the following bug fix. This update:

HTTP Proxy

ID	Issue
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.

Advanced Secure Gateway 6.7.5.4 GA

Release Information

- **Release Date:** May 13, 2020
- **Build Number:** 250593

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.1 build 249992. Refer to Content Analysis documentation on myBroadcom for more information.

Third-Party Compatibility

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

  https://knowledge.broadcom.com/external/article/169081/supported-java-operating-system-and-brow.html

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to Article ID 173228:

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

Upgrading To/Downgrading From This Release

- This release has an issue where large amounts of IPv4 ARP traffic sometimes caused the appliance to restart. Upgrade to version 6.7.5.5 to avoid this issue.
- After upgrading to Advanced Secure Gateway 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://knowledge.broadcom.com/external/article?legacyId=TECH254549.

Changes in Advanced Secure Gateway 6.7.5.4

- Advanced Secure Gateway 6.7.5.4 introduces new features and enhancements. See "New Features in SGOS 6.7.5.4" on page 11.

Fixes in Advanced Secure Gateway 6.7.5.4

- Advanced Secure Gateway 6.7.5.4 includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.5.4" on the next page.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway 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 "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.5.4

Bug Fixes in this Release

Advanced Secure Gateway 6.7.5.4 includes bug fixes. This update:

Access Logging

ID	Issue
SG-15198	Fixes an issue where the appliance experienced a restart due to receiving an empty cache buffer
SG-18436	Fixes an issue where the appliance sometimes experienced a restart when encountering errors while publishing access logs via SCP.

HTTP Proxy

ID	Issue
SG-18526	Fixes an issue where the appliance sometimes experienced a restart when request.icap_mirror(yes) was triggered in policy under some circumstances.

Policy

ID	Issue
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.

SSL Proxy

ID	Issue
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.

TCP/IP and General Networking

ID	Issue
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.

New Features in SGOS 6.7.5.4

The following changes were first made in SGOS 6.7.5.4:

DNS Server Resolution Behavior Changes

The Advanced Secure Gateway 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)

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.

Advanced Secure Gateway 6.7.5.3 GA

Release Information

- **Release Date:** April 16, 2020
- **Build Number:** 250075

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.1 build 249992. Refer to Content Analysis documentation on myBroadcom for more information.

Third-Party Compatibility

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

  https://knowledge.broadcom.com/external/article/169081/supported-java-operating-system-and-brow.html

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to Article ID 173228:

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

Upgrading To/Downgrading From This Release

- This release introduced an issue where large amounts of IPv4 ARP traffic sometimes caused the appliance to restart. Upgrade to version 6.7.5.5 to avoid this issue.
- After upgrading to Advanced Secure Gateway 6.7.5 and configuring HTTPS forward proxy, some sites that were allowed in version 6.7.3 are now denied. For details on a workaround, refer to https://knowledge.broadcom.com/external/article?legacyId=TECH254549.
- Advanced Secure Gateway 6.7.5.3 introduces a new version of COE, which can affect upgrade/downgrade decisions. If you want to upgrade or downgrade from 6.7.5.3 and need to perform a factory reset to do so, Symantec recommends resetting to the target version of Advanced Secure Gateway. For example, if you are running 6.7.5.3 and need to perform a factory reset before downgrading to 6.7.4.14, reset the appliance to 6.7.4.14. If you perform a factory reset to 6.7.5.3, you will not be able to upgrade or downgrade to any version that was released prior to 6.7.5.3.

Changes in Advanced Secure Gateway 6.7.5.3

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

Fixes in Advanced Secure Gateway 6.7.5.3

- Advanced Secure Gateway 6.7.5.3 includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.5.3" on page 16.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway 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 "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

New Features in SGOS 6.7.5.3

The following changes were first made in SGOS 6.7.5.3:

SNMP Monitoring for HTTP Client Workers

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

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

- More information:

  SNMP Critical Resource Monitoring Guide

New Event Log Message for HTTP Client Workers

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

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

ICAP Monitoring for Deferred and Resumed Transactions

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

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

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

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

SSL Attributes for Access Logs and Policy

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

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

Fixes in Advanced Secure Gateway 6.7.5.3

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.5.3 includes security advisory fixes. This update:

ID	Issue
SG-5678	Fixes Apache Tomcat vulnerability (CVE-2018-1336). For details, refer to SYMSA1463.
SG-5574	Fixes Apache Tomcat vulnerabilities (CVE-2017-5664, CVE-2017-5647). For details, refer to SYMSA1419.

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.5.3 includes bug fixes. This update:

Access Logging

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

Authentication

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

CAS

ID	Issue
SG-16965	Fixes an issue where the localhost_access_log.txt file was not rotated.

CLI Consoles

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

COE

ID	Issue
SG-11589	Fixes an issue where the appliance experienced crashes after upgrading to 6.7.4.5 from 6.7.3.12.
SG-17073	Fixes an issue where verifying the birth certificate keytool consumed 100% of the CPU.
SG-5622	Fixes an issue where CAS SNMP was broken to return the correct value "No Such Object available on this agent at this OID".

DNS Proxy

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

ICAP

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

MAPI Proxy

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

Policy

ID	Issue
SG-13680	Fixes an issue where certain websites were incorrectly denied due to domain fronting detection CPL.

SSL Proxy

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

SSL/TLS and PKI

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

SSLV Integration

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

TCP/IP and General Networking

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

ID	Issue
SG-18876	Fixes an issue where the appliance experienced a restart in process group `"PG_TCPIP"` in process `"stack-admin"` in `"libstack.exe.so"` at `".text+0x5471ee"`.

TCP Tunnel Proxy

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

Web VPM

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

Advanced Secure Gateway 6.7.5.2 LA

Release Information

- **Release Date:** February 25, 2020
- **Build Number:** 248552

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Important Information About This Release

Advanced Secure Gateway 6.7.5.2 contains the following issues and has been made a Limited Availability release:

- Tunneled TLS 1.2 SSL connections fail with an SSL failed error message (SG-19003)
- SSL tunneled connections are bypassing forwarding rules (SG-18838)
- 6.7.5.2 crashes when a forwarding rule is configured for tunneled SSL traffic (SG-18824)
- SSL Proxy transactions were restarted when tunneled (SG-18971)
- `fwd proxy(no)` and `fwd proxy(on_exception)` policy was not applied to tunneled TLS 1.3 tunneled sessions (SG-19710)

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

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

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

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.5.2

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.5.2

Bug Fixes in this Release

Advanced Secure Gateway 6.7.5.2 includes the following bug fix. This update:

HTTP Proxy

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

Advanced Secure Gateway 6.7.5.1 LA

Release Information

- **Release Date:** February 13, 2020
- **Build Number:** 247742

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Important Information About This Release

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

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

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

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.5.1

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.5.1

Bug Fixes in this Release

Advanced Secure Gateway 6.7.5.1 includes bug fixes. This update:

Access Logging

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

ADN

ID	Issue
SG-13070	Fixes an issue where users attempted to restore the appliance from an archived file and received error messages because ADN attributes were not accepted into the configuration.

Authentication

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

CLI Consoles

ID	Issue
SG-3726	Fixes an issue where the Advanced URL "/diagnostics/hardware/info" the "write-required" attribute set.
SG-16378	Fixes an issue where changes made to Content Analysis settings via CLI would not save.

Content Analysis

ID	Issue
SG-17788	Fixes an issue where the appliance would not allow users to save changes to their CASMA information

Health Checks

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

Kernel

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

Policy

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

SSL Proxy

ID	Issue
SG-6161	Fixes an issue where after upgrading to ASG 6.7.4.2 , when SSL traffic is not intercepted by policy, SSL attributes (such as negotiated cipher or TLS version) were not available for use in policy conditions and access log fields. Refer to TECH253316 for more information on this issue.
SG-12044	Fixes an issue where the SSL certificate hostname would be invalid when two virtual hosts are running in a reverse proxy configuration.

SSL/TLS and PKI

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

TCP/IP and General Networking

ID	Issue
SG-13840	Fixes an issue where interface 0:1 was unavailable.
SG-14848	Fixes an issue where the bandwidth management classes would reach their maximum.

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

Transformer

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

URL Filtering

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

VPM (Legacy)

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

Web VPM

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

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

Advanced Secure Gateway 6.7.4.14 GA

Release Information

- **Release Date:** March 16, 2020
- **Build Number:** 249051

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.
- **Advanced Secure Gateway Appliances:**
    - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.14

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.14

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.14 includes bug fixes. This update:

Authentication

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

Health Checks

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

SSL/TLS and PKI

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

This release also includes fixes from Advanced Secure Gateway 6.7.4.13. See "Fixes in Advanced Secure Gateway 6.7.4.13" on page 34 for more information.

Advanced Secure Gateway 6.7.4.13 GA

Release Information

- **Release Date:** December 11, 2019
- **Build Number:** 245574

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.
- **Advanced Secure Gateway Appliances:**
    - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.13

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.13

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.13 includes bug fixes. This update:

TCP/IP and General Networking

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

Advanced Secure Gateway 6.7.4.12 PR

Release Information

- **Release Date:** November 18, 2019
- **Build Number:** 244898

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.
- **Advanced Secure Gateway Appliances:**
    - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.12

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.12

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.12 includes bug fixes. This update:

TCP/IP and General Networking

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

Advanced Secure Gateway 6.7.4.10 PR

Release Information

- **Release Date:** November 5, 2019
- **Build Number:** 244309

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.
- **Advanced Secure Gateway Appliances:**
    - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.4.10

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

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

  1. Enable EDNS using the command:

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

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

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

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

  3. View the DNS settings:

     ```
     # show dns
     ```

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

Fixes in Advanced Secure Gateway 6.7.4.10

- This release includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.4.10" on page 41.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.10

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.10 includes bug fixes. This update:

Access Logging

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

Authentication

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

Content Analysis

ID	Issue
SG-14207	Fixes an issue where host memory usage was very high on version 6.7.4.8 in comparison to version 6.7.3.14.
SG-14925	Fixes an issue where an appliance experienced high memory usage and stopped responding.
SG-15262	Fixes an issue where ICAP transactions failed and the appliance stopped responding.

DNS Proxy

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

Environment

ID	Issue
SG-15747	Fixes an issue where high memory usage caused the appliance to stop responding.

FTP Proxy

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

IPv6

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

Management Console

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

Security

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

Services

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

SNMP

ID	Issue
SG-8026	Fixes an issue where SNMP periodically stopped working and reported an error, "Not in time window".
SG-14442	Fixes an issue where CPU usage reports incorrectly showed high usage.

SOCKS

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

SSL Proxy

ID	Issue
SG-13361	Fixes an issue where authentication sessions persisted across browser sessions, where the expected behavior was that users would be prompted to authenticate each new browser session. This issue occurred after upgrading to version 6.7.4.508

SSL/TLS and PKI

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

TCP/IP and General Networking

ID	Issue
SG-8965	Addresses an issue where the appliance experienced a restart in "stack-deletion-ISR" in "libstack.exe.so" at .text+0x4265b7.
SG-11899	Addresses an issue where the appliance stopped responding with error HWE: 0xe SWE: 0x0 PFLA: 0x15cfeca94a8 Process group: "PG_TCPIP" Process: "stack-api-worker-3" in "libstack.exe.so" at .text+0x50575b.
SG-13446	Addresses an issue where the appliance experienced a restart in m_dup_pkthdr HWE:0x3 SWE:0x0 PFLA:0x0 Process group: "PG_TCPIP" Process: "HTTP CW 21830453A40" in "libstack.exe.so" at .text+0x4d625f.
SG-14060	Fixes an issue where the appliance stopped passing traffic upstream when processing very high loads.
SG-14850	Addresses an issue where the appliance experienced a restart in HWE : 0xe SWE: 0x0 PFLA:0x0 PG: "PG_DNS" Process: "likewise Lwbase_WorkThread" in "libstack.exe.so" at .text+0x33d5b3
SG-14937	Fixed an issue where the bytes received statistics report (**Statistics > Network > Interface History > Bytes Received**) did not increment after an upgrade to version 6.7.4.9.
SG-16423	Fixes an issue where IPv4 TCP tunnel throughput was reduced to 1 Gbps.

Utility Libraries

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

Advanced Secure Gateway 6.7.4.9 PR

Release Information

- **Release Date:** August 13, 2019
- **Build Number:** 240930

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.4.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

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

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.9

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.9

Advanced Secure Gateway 6.7.4.9 includes bug fixes. This update:

Access Logging

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

Content Analysis

ID	Issue
SG-10009	Fixes an issue where ICAP errors occurred when Kaspersky Enhanced scanning was enabled.

Authentication

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

ID	Issue
SG-11130	Fixes an issue where CAPTCHA validation could not be implemented because the CAPTCHA request was looping on the proxy.
SG-11447	Fixes an issue where an authentication logout exception page was not returned when a SAML realm was used.
SG-12075	Fixes an issue where the post-setup archive configuration contained the Windows Domain hostname instead of the default hostname in IWA Direct (system created).
SG-12635	Addresses an issue where the proxy experienced a restart in process "Agent-Admin-CORP-233".
SG-12978	Fixes an issue where, after trying to join the domain, the proxy became unresponsive and stopped passing traffic. The admin could ping the proxy but could not access the Management Console or SSH CLI.

DNS Proxy

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

Event Logging

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

FTP Proxy

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

HTTP Proxy

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

ID	Issue
SG-11633	Addresses an issue where the proxy restarted in process group "PG_HTTP" in process "HTTP Admin" in "libhttp.exe.so".

Management Console

ID	Issue
SG-10839	Fixes an issue where ICAP object names did not appear under **Proxy > Statistics > Content Analysis**.
SG-11199	Fixes an issue where initial login attempts using the Management Console Launcher did not work.

SSL/TLS and PKI

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

SSL Proxy

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

TCP/IP and General Networking

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

ID	Issue
SG-4333	Fixes an issue where turning on/off EDNS support on the appliance was not reflected in the event log.
SG-11481	Fixes an issue where the proxy did not adhere to the configured TCP window size, which intermittently caused download slowness.

URL Filtering

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

Visual Policy Manager

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

Advanced Secure Gateway 6.7.4.804 LA

Release Information

- **Release Date:** October 16, 2019
- **Build Number:** 243435

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.
    - SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.
- **Advanced Secure Gateway Appliances:**
    - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.804

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.804

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.804 includes bug fixes. This update:

Content Analysis

ID	Issue
SG-15262	Fixes an issue where ICAP transactions failed and the appliance stopped responding.
SG-14207	Fixes an issue where host memory usage was very high on version 6.7.4.8 in comparison to version 6.7.3.14.
SG-14925	Fixes an issue where an appliance experienced high memory usage and stopped responding.

SNMP

ID	Issue
SG-14442	Fixes an issue where SNMP monitoring showed incorrect statistics for CPU usage.

Advanced Secure Gateway 6.7.4.8 GA

Release Information

- **Release Date:** July 24, 2019
- **Build Number:** 239880

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.8

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.8

Advanced Secure Gateway 6.7.4.8 includes bug fixes. This update:

Content Analysis

ID	Issue
SG-11504	Fixes an issue where AV service had high memory utilization.

Environment

ID	Issue
SG-12638	Fixes an issue where the appliance stopped responding and host memory utilization was high. This issue occurred after an upgrade to version 6.7.4.6.

Authentication

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

Health Checks

ID	Issue
SG-13643	Fixes an issue where health checks failed or reported that the monitored component was not found. This issue occurred after upgrading from version 6.6.5.14 to 6.7.4.7.
SG-13078	Fixes an issue where the health check subsystem did not notify the network stack when the internal Content Analysis health check was set to disabled healthy.

SSL/TLS and PKI

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

TCP/IP and General Networking

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

URL Filtering

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

Web Visual Policy Manager

ID	Issue
SG-11654	Fixes an issue where **Enable HTTPS Interception** was undefined when converting Java-based CPL to web VPM CPL.
SG-5050	Fixes an issue where installing VPM policy resulted in a "Duplicate definition" error although policy did not include duplicate definitions. This issue occurred when using Symantec Management Center to create tenant/landlord policies in the VPM. **Note:** This issue was fixed in version 6.7.4.6.
SG-13050	Fixes an issue where it was possible to create multiple identical **Client IP Address/Subnet** objects.
SG-10965	Fixes an issue where February 29th was not available in **Time** objects.

Advanced Secure Gateway 6.7.4.7 PR

Release Information

- **Release Date:** June 14, 2019
- **Build Number:** 238172

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.7

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.7

Advanced Secure Gateway 6.7.4.7 includes a bug fix. This update:

Authentication

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

Advanced Secure Gateway 6.7.4.6 PR

Release Information

- **Release Date:** June 4, 2019
- **Build Number:** 236887

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.4.6

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

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

Fixes in Advanced Secure Gateway 6.7.4.6

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.6

Advanced Secure Gateway 6.7.4.6 includes bug fixes. This update:

Boot

ID	Issue
SG-10409	Fixes an issue where the proxy experienced a restart after upgrading from 6.6.5.17 to 6.7.4.3.

Content Analysis

ID	Issue
SG-9047	Fixes an issue on the ASG-S400 and ASG-S200 platforms where Advanced Secure Gateway appliance are not accessing or updating AV scanners after a re-manufacture or PXE boot.

Authentication

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

IPv6 Stack and IPv6 Proxies

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

Policy

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

Transformer

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

Web Visual Policy Manager

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

Advanced Secure Gateway 6.7.4.5 PR

Release Information

- **Release Date:** April 25, 2019
- **Build Number:** 235456

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.4.5

The following changes were first made in SGOS 6.7.4.4.

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

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

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

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

Fixes in Advanced Secure Gateway 6.7.4.5

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.5

Advanced Secure Gateway 6.7.4.5 includes security advisory (SA) fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.4.5 includes security advisory fixes. This update:

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

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.5 includes bug fixes. This update:

Access Logging

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

Authentication

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

CLI Consoles

ID	Issue
SG-9030	Fixes a slow upgrade issue on the Advanced Secure Gateway appliance when the system image (BCSI file) was uploaded from the local file system.

Configuration

ID	Issue
SG-9126	Fixes an issue on the Advanced Secure Gateway appliance where upgrading to version 6.7.4.3 failed and the appliance reverted to a previous release.

DNS Proxy

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

HTTP Proxy

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

ICAP

ID	Issue
SG-8038	Fixes an issue where the exception page is not returned from the Symantec DLP server (in ICAP request mode) when **Use vendor's "virus found" page** is enabled for the ICAP service.
SG-5657	Fixes an issue where changes made to the internal ICAP settings were not seen in the configuration file or the SysInfo even though the changes took effect.

Policy

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

SSL/TLS and PKI

ID	Issue
SG-5162	Addresses an issue where the proxy experienced a restart in the Threshold_Monitor process where the highest consumers of memory were SSL and cryptography.
SG-5172	Fixes an issue where SSL inspection was inconsistent due to an invalid cache certificate.
SG-5328	Fixes an issue where the proxy reverted to version 6.6.5.17 after attempting to upgrade to version 6.7.4.1.
SG-5346	Fixes an issue where importing a CRL failed with an insufficient memory error.
SG-9067	Fixes an issue where the proxy experienced a restart in process group "PG_SSL_HNDSHK" in process "FTP CW 4098B026430" in "libcfssl.exe.so" .
SG-9252	Fixes an issue where an expanded archive configuration could not be restored when it contained a CCL that started with "bluecoat-".

TCP/IP and General Networking

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

URL Filtering

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

Web Visual Policy Manager

ID	Issue
SG-8624	Fixes an issue where the first installation of policy via the Web VPM caused errors in generated CPL. This issue occurred when condition block names contained quotation marks and whitespace.
SG-8818	Fixes an issue where the Web VPM changed Bandwidth Management objects from `limit_bandwidth.server.inbound(class_name)` to `limit_bandwidth.server.inbound(no)` by default.

Advanced Secure Gateway 6.7.4.4 LA

Release Information

- **Release Date:** April 16, 2019
- **Build Number:** 234975

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Important Information About This Release

Advanced Secure Gateway 6.7.4.4 contains an issue that causes some appliances to restart. Symantec recommends upgrading to "Advanced Secure Gateway 6.7.4.5 PR" on page 67 to resolve this issue. Advanced Secure Gateway 6.7.4.4 is no longer available for download through MySymantec. Please refer to your Symantec point-of-contact for details.

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Advanced Secure Gateway 6.7.4.3 PR

Release Information

- **Release Date:** January 25, 2019
- **Build Number:** 230906

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Important Information About This Release

Advanced Secure Gateway 6.7.4.3 fixes a serious issue where using the new Web Visual Policy Manager caused unintended policy behavior when applying policy save/changes. For details, refer to SG-8612 in "Fixes in Advanced Secure Gateway 6.7.4.3" on page 83. Symantec recommends upgrading to this release to use the Web VPM without issue.

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

> **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Changes in Advanced Secure Gateway 6.7.4.3

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

Fixes in Advanced Secure Gateway 6.7.4.3

- This release includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.4.3" on page 83.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

New Features in Advanced Secure Gateway 6.7.4.3

Advanced Secure Gateway 6.7.4.3 introduces the following new features.

Web Visual Policy Manager

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

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

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

Minimum Requirements

Supported browsers:

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

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

Display resolution:

- 1366 x 768

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

- More information:

  ProxySG Web Visual Policy Manager WebGuide

Periodic Upload of SysInfo Statistics

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

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

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

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

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

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

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

- More information:

  Command Line Interface Reference

External Services Access Log Fields

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

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

All times are expressed in milliseconds.

- More information:

  Content Policy Language Reference

Enhancements from SGOS 6.7.4.1

This release includes the following enhancements from SGOS 6.7.4.1:

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

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

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

Fixes in Advanced Secure Gateway 6.7.4.3

Advanced Secure Gateway 6.7.4.3 includes security advisory (SA) fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.4.3 includes security advisory fixes. This update:

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

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.3 includes bug fixes. This update:

Access Logging

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

Content Analysis

ID	Issue
SG-8242	Fixes an issue where Symantec Anti-Virus (AV) updates failed. For details, refer to https://www.symantec.com/docs/ALERT2640.

Authentication

ID	Issue
B#265632 SG-5058	Fixes an issue where the proxy stopped responding while performing LDAP authorizations.
B#265768 SG-5810	Fixes an issue where the proxy stopped responding when **Nested Groups Support** was enabled in LDAP realm configuration.

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

HTTP Proxy

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

ICAP

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

Management Console

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

Policy

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

SSL/TLS and PKI

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

TCP/IP and General Networking

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

URL Filtering

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

Web Visual Policy Manager

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

Fixes from SGOS 6.7.4.1

Advanced Secure Gateway 6.7.4.2 includes bug fixes from SGOS 6.7.4.1. See Fixes in 6.7.4.1.

Advanced Secure Gateway 6.7.4.2 LA

Release Information

- **Release Date:** December 27, 2018
- **Build Number:** 229541

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Important Information About This Release

Advanced Secure Gateway 6.7.4.2 contains an issue where using the new Web Visual Policy Manager causes unintended policy behavior when applying policy save/changes (SG-8612). Symantec recommends upgrading to "Advanced Secure Gateway 6.7.4.3 PR" on page 78 to use the Web VPM without issue.

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

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

Content Analysis

- This release includes Content Analysis version 2.3.5. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Advanced Secure Gateway 6.7.4.141 EA

Release Information

- **Release Date:** October 24, 2018
- **Build Number:** 226401

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

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **Web Isolation:** 1.10 and later
- **SSL Visibility:** 4.2.4.1 and later
    - When using TLS offload, Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1.

- SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4. SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1.

- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

- For information on Java 11 support, refer to TECH252566

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

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.4.141

- Advanced Secure Gateway 6.7.4.141 introduces new features and enhancements. See Features in 6.7.4.141 EA for details.

Fixes in Advanced Secure Gateway 6.7.4.141

- This release includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.4.141" on page 96.
- This release also includes fixes from SGOS 6.7.4.130. See "Fixes Included from SGOS 6.7.4.130" on page 100.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

New Features in Advanced Secure Gateway 6.7.4.141

Advanced Secure Gateway 6.7.4.141 introduces the following new features.

Domain Fronting Detection

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

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

  CPL condition: `http.connect.host=`

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

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

  CPL condition: `http.connect.port=`

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

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

  Content Policy Language Reference

  Visual Policy Manager Reference

  SGOS Administration Guide

IPv6 Support for WCCPv2

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

This feature has the following limitations in this release:

- Only **L2** redirection is supported.
- Only **Mask** assignment type is supported; **Hash** is not supported.
- The default **Mask** value is 0x3f is not supported; you must specify a different value.
- Only **Individual Home Router Addresses** are supported; **Multicast Home Router** is not supported.

- **Individual Home Router Addresses** must include only IPv4 or only IPv6 addresses within the same Service Group.
- More information:

  SGOS Administration Guide

New Features Included from Advanced Secure Gateway 6.7.4.130

This release includes the following features from Advanced Secure Gateway 6.7.4.130:

Include Surrogate Realms to realm= Tests in Policy

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

The following CPL was added to support this feature:

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

where:

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

Consider the following example:

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

...

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

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

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

- More information:

  Content Policy Language Reference

Default TCP Window Size Increase

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

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

```
> show tcp-ip
```

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

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

- More information:

  Command Line Interface Reference

  SGOS Upgrade/Downgrade WebGuide

Specify Upstream Server CCL for Forwarded Transctions

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

- More information:

  Content Policy Language Reference

Fixes in Advanced Secure Gateway 6.7.4.141

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.141 includes bug fixes. This update:

Authentication

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

HTTP Proxy

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

ICAP

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

IPv6 Stack and IPv6 Proxies

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

Mnanagement Console

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

Policy

B#	Issue
262506	Fixes an issue where changing the configured malware scanning from an internal to an external content analysis service required a manual VPM policy installation when tenant policy was used or pushed from the Management Center.
262197	Fixes an issue where users could not log in to or join a meeting using Skype for Business when the appliance was transparently deployed and had an authentication policy that allowed access to specific users and/or groups.
262711	Fixes an issue where some tenant policies were missing after upgrading to SGOS 6.7.3.x.

Security

B#	Issue
262574	Fixes an issue where a malicious server could cause a denial of service attack during a TLS handshake by sending a large prime number that the client would spend a long time generating a key for.
262706	Fixes an issue where the Advanced Secure Gateway was vulnerable to a denial of service attack.
262907	Fixes an vulnerability in the OpenSSL RSA key generation algorithm where an attacker could have a cache timing attack during the key generation process to recover the private key.

Services

B#	Issue
261499	Fixes an issue where the default listener for TCP Port 514 could not be removed.
262653	Fixes an issue where ADN attributes appeared on the HTTPS proxy service when using HTTPS on an Advanced Secure Gateway.

SSL/TLS and PKI

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

System Statistics

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

TCP/IP and General Networking

B#	Issue
256018	Fixes an issue where the appliance restarted in process group "PG_TCPIP" in process "HTTP SW 80F5AE4FA40 for 70FA5135A40" in "libstack.exe.so".
258974	Fixes an issue where the appliance stalled during start-up if the first DNS server in the primary group was unreachable.
262273	Fixes an issue where the failover did not work correctly if the interface was disabled for the backup appliance.
263272	Fixes an issue where the appliance returned a false attack in the progress status from an SNMP walk.
263341	Fixes an issue that caused a restart in process cookie-monster in libstack.exe.so on edge boxes that were using ADN after upgrading to 6.7.3.9.

URL Filtering

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

VPM

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

Web Application Firewall

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

Windows Media Proxy

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

Fixes Included from SGOS 6.7.4.130

This release includes the following security advisory (SA) fixes and bug fixes from SGOS 6.7.4.130.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.4.130 includes security advisory fixes. This update:

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

SAs are published as security vulnerabilities are discovered and fixed. To see SAs that apply to the version of Advanced Secure Gateway you are running, including ones published after this release, go to:

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.130 includes bug fixes. This update:

Access Logging

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

Authentication

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

Client Manager

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

Collaboration

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

Documentation

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

HTTP Proxy

B#	Issue
259384	Fixes an issue where the Advanced Secure Gateway antivirus engine and pattern update failed when policy contained a `reflect_ip(client)` rule that matched the internal Content Analysis subscription update request. This caused the appliance to attempt to reflect the internal IPv6 address when connecting upstream, which failed.
257793	Fixes an issue where downloads from www.filefactory.com did not work when CachePulse was enabled.

Licensing

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

Management Console

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

Policy

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

Proxy Forwarding

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

SNMP

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

SOCKS Proxy

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

SSL Proxy

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

SSL/TLS_and_PKI

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

SSLV Integration

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

Security

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

TCP/IP and General Networking

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

URL Filtering

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

Visual Policy Manager

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

Advanced Secure Gateway 6.7.4.111 EA

Release Information

- **Release Date:** April 18, 2018
- **Build Number:** 217327

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

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.2.4.1 and later
    - Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1 when using TLS offload.
    - SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1. SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4.

- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.4.111

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.111

Advanced Secure Gateway 6.7.4.111 includes bug fixes and changes included in the 6.7.4.108 EA. This update:

Authentication

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

SSL Proxy

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

Advanced Secure Gateway 6.7.4.107 EA

Release Information

- **Release Date:** March 22, 2018
- **Build Number:** 215847

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

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x, and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.2.4.1 and later
  - Advanced Secure Gateway 6.7.4 is not compatible with SSLV versions prior to 4.2.4.1 when using TLS offload.
  - SSL session reuse was previously not supported when using TLS offload with Advanced Secure Gateway 6.7.4 and SSLV 4.2.4.1. SSLV 4.2.5.1 and later now supports session reuse with SGOS 6.7.4.

- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.3.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.4.107

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

Fixes in Advanced Secure Gateway 6.7.4.107

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.4.107

Advanced Secure Gateway 6.7.4.107 includes the following security advisory fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.4.107 includes security advisory fixes. This update:

B#	Issue	Fixed In
N/A	Addresses NTP vulnerabilities. Refer to SA139.	6.7.4.101
N/A	Addresses NTP vulnerabilities. Refer to SA147.	6.7.4.101
N/A	Addresses OpenSSL vulnerabilities. Refer to SA141.	6.7.4.101
N/A	Addresses NSS security vulnerabilities. Refer to SA153.	6.7.4.102

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.4.107 includes bug fixes and fixes from 6.7.4.105 - Patch Release Fixes. This update:

Access Logging

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

Authentication

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

CLI Consoles

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

Configuration

B#	Issue	Fixed In
CAS-5024	Fixes an issue where the Sender e-mail address field in e-mail server configuration restricted the top-level domain to six characters.	6.7.4.105

Content Analysis

B#	Issue	Fixed In
255592	Fixes an issue where scanning of some archive files in Advanced Secure Gateway 6.7 was slower than it was in version 6.6.	6.7.4.105

Health Monitoring

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

Management Console

B#	Issue	Fixed In
254660	Fixes an issue where the Management Console did not accept system image download URLs consisting of more than 227 characters.	6.7.4.107

MAPI Proxy

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

Services

B#	Issue	Fixed In
254395	Addresses performance issues with AV scanning compressed files.	6.7.4.105
255120	Fixes issue where Symantec AV did not block sample test file (eicar) in REQMOD test.	6.7.4.105

SSL Proxy

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

SSL/TLS and PKI

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

TCP/IP and General Networking

B#	Issue	Fixed In
252086	Fixes an issue where the appliance might have experienced a restart in PG_TCPIP when Virtual IP was configured in failover mode.	6.7.4.107
255453	Fixes an issue where the appliance sent gratuitous ARPs showing a Sender MAC Address containing only zeroes (`00:00:00:00:00:00`). This occurred when the appliance was set as Master in a failover configuration and both aggregate interfaces and VLAN were configured.	6.7.4.107

URL Filtering

B#	Issue	Fixed In
254474	Fixed an issue where differential database updates for Intelligence Services were causing increased loads on disks, which caused delayed responses.	6.7.4.107

B#	Issue	Fixed In
249253	Fixes an issue where the WebPulse tab (**Configuration > Threat Protection > WebPulse**) did not display database download status if Intelligence Services was enabled.	6.7.4.105
256160	Fixes an issue where WebPulse did not categorize websites in a child/parent configuration when a valid forwarding host was not supplied.	6.7.4.107
248868	Fixes an issue where enabling the Application Classification service took longer.	6.7.4.107

Visual Policy Manager

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

Advanced Secure Gateway 6.7.3.12 PR

Release Information

- **Release Date:** September 24, 2018
- **Build Number:** 224782

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.3.12

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.12

Advanced Secure Gateway 6.7.3.12 includes the following security advisory fixes and bug fixes.

Content Analysis

B#	Issue
262990	Fixes an issue where the scanned object status is showed as 'No scanner available' when using the Symantec AV engine.

SSL Proxy

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

Advanced Secure Gateway 6.7.3.11 PR

Release Information

- **Release Date:** September 14, 2018
- **Build Number:** 224429

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- See B#262122 in "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for details on a 6.6.x downgrade issue and workaround.

The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.3.11

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.11

Advanced Secure Gateway 6.7.3.11 includes the following security advisory fixes and bug fixes.

Authentication

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

CLI_Consoles

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

HTTP Proxy

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

SSLV Integration

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

TCP/IP and General Networking

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

URL Filtering

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

Advanced Secure Gateway 6.7.3.10 PR

Release Information

- **Release Date:** August 10, 2018
- **Build Number:** 222788

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- See B#262122 in "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for details on a 6.6.x downgrade issue and workaround.

The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.3.10

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.10

Advanced Secure Gateway 6.7.3.10 includes the following security advisory fixes and bug fixes.

Authentication

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

Policy

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

SSL/TLS and PKI

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

TCP/IP and General Networking

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

Advanced Secure Gateway 6.7.3.9 PR

Release Information

- **Release Date:** July 9, 2018
- **Build Number:** 220765

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.3.9

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.9

Advanced Secure Gateway 6.7.3.9 includes the following security advisory fixes and bug fixes.

ASG/CAS

B#	Issue
262021	Fixes an ASG issue where antivirus updates were unable to update when the /encrypted-data partition was full.

Authentication

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

HTTP Proxy

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

Proxy Forwarding

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

SSLV Integration

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

TCP/IP and General Networking

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

URL Filtering

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

VPM

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

Advanced Secure Gateway 6.7.3.8 PR

Release Information

- **Release Date:** June 1, 2018
- **Build Number:** 219265

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Fixes in Advanced Secure Gateway 6.7.3.8

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.8

Advanced Secure Gateway 6.7.3.8 includes the following security advisory fixes and bug fixes.

Content Analysis

B#	Issue
257842	Fixes an issue where the "/cache-data" partition, used for updating AV engine patterns and definitions, might have run out of space if the partition was too small.

TCP/IP and General Networking

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

Advanced Secure Gateway 6.7.3.7 PR

Release Information

- **Release Date:** May 1, 2018
- **Build Number:** 218080

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x andlater
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Fixes in Advanced Secure Gateway 6.7.3.7

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.7

Advanced Secure Gateway 6.7.3.7 includes the following security advisory fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.3.7 includes security advisory fixes. This update:

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

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.3.7 includes bug fixes. This update:

Authentication

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

Collaboration

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

Content Analysis

B#	Issue
255592	Fixes an issue where, on some occasions, scanning archive files was slower than in Advanced Secure Gateway 6.6.

Event Logging

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

HTTP Proxy

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

Management Console

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

SOCKS Proxy

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

SSL Proxy

B#	Issue
252087	Fixes an issue where the appliance did not use the SNI extension in server-side connections. The extension is required by some servers in order to respond with the correct server certificate in the TLS handshake.
258274	Fixes an issue where the proxy became unresponsive and failed to intercept traffic when using STunnel.

TCP/IP and General Networking

B#	Issue
256543	Fixes an issue where DNS resolution failed when the first listed server in a custom DNS group stopped working.
257053	Fixes an issue where the appliance became slow due to packets that were not processed within the queues associated with each NIC.
257272	Fixes an issue where attempts to download large files via SOCKS proxy on high-speed networks (2Mbps+ speed) timed out. This issue occurred because the proxy did not update the TCP window size.
257434	Fixes an issue where the proxy experienced a restart in PG_TCPIP in process "SGRP WOrker" in "libstack.exe.so" when the network cable was removed while SGRP was using the same multicast address.
258812	Fixes an issue where the `client.interface` property showed an invalid card number (such as 255:255.x) in the policy trace. This issue occurred when WCCP had router affinity set to "both" or “client”.

B#	Issue
258918	Fixes an issue where the proxy experienced slowness on a model with an ixgbe driver when using VLAN, bridging, and bypass.
259677	Fixes an issue where the proxy experienced a restart in TCP/IP process "stack-admin" in "libstack.exe.so.

URL Filtering

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

Visual Policy Manager

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

Advanced Secure Gateway 6.7.3.6 GA

Release Information

- **Release Date:** March 30, 2018
- **Build Number:** 216329

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Fixes in Advanced Secure Gateway 6.7.3.6

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.6

Advanced Secure Gateway 6.7.3.6 includes the following bug fixes. This update:

Access Logging

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

Authentication

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

CLI Consoles

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

ICAP

B#	Issue
257787	Fixes an issue where restoring defaults reset the Advanced Secure Gateway internal ICAP max connections to 25. Refer to ALERT2558 for details: http://www.symantec.com/docs/ALERT2558

Kernel

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

TCP/IP and General Networking

B#	Issue
255453	Fixes an issue where where the Advanced Secure Gateway appliance sent gratuitous ARPs showing a Sender MAC Address containing only zeroes (`00:00:00:00:00:00`). This occurred after the appliance was set as Master in a failover configuration and when both aggregate interfaces and VLAN are configured.

Advanced Secure Gateway 6.7.3.5 GA

Release Information

- **Release Date:** February 13, 2018
- **Build Number:** 213954

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x; 2.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Changes in Advanced Secure Gateway 6.7.3.5

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

Fixes in Advanced Secure Gateway 6.7.3.5

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

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.5

Advanced Secure Gateway 6.7.3.5 includes the following bug fixes. This update:

Access Logging

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

Authentication

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

Content Analysis

B#	Issue
255693	Fixes an issue where a Content Analysis process consumed an unexpected amount of memory which may have caused the Advanced Secure Gateway appliance to restart.

ICAP

B#	Issue
255415	Fixes an issue where the `#(config icap service_name)`**`defer-threshold`** and `#(config icap service_name)`**`max-conn`** commands could not be set for the `bluecoat-local-request` and `bluecoat-local-response` services.

Kernel

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

MAPI Proxy

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

Management Console

B#	Issue
255167	Fixes an issue where adding an "Authentication required" comment in policy in version 6.7.3.1 caused the Management Console to automatically log out after a successful policy installation.

Policy

B#	Issue
254751	Fixes a memory leak in configuration (Process group PG_CFG).

SSL Proxy

B#	Issue
253406	Fixes an issue causing increased SSL memory utilization.
254374	Fixes an issue where accessing an HTTPS site failed with an error "Client certificate not received" due to the appliance being unable to send the imported client certificate.
255468	Addresses an issue where the appliance might have restarted in Process group: "PG_CFSSL"in process "HTTP SW 1097B7B5A40 for 10968ABBA40".

TCP/IP and General Networking

B#	Issue
255536	Fixes an issue where bandwidth management did not work correctly when used in a nested class.
255540	Fixes an issue where Connection Forwarding (CCM) may cause the appliance to restart in Process "NIC I/O 0:0-em_n 0 Deallocation worker" when forwarding a connection to another ProxySG appliance via IPIP.
256204	Fixes an issue where the appliance might have restarted in Process: "cookie-monster" in "libmemory.so" when CCM (Connection Forwarding) is enabled.
256213	Fixes an issue where the appliance restarted when starting or stopping a packet capture (PCAP) with filters and the PCAP reaches its limit.
256391	Fixes an issue where the appliance might have restarted in Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so" with encapsulated IPv6 traffic.
256718	Fixes a memory leak In TCP/IP when port spoofing was configured.

Advanced Secure Gateway 6.7.3.2 GA

Release Information

- **Release Date:** 12/12/2017
- **Build Number:**211137

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Changes in Advanced Secure Gateway 6.7.3.2

- Advanced Secure Gateway 6.7.3.2 introduces the following new CLI to allow you to configure the defer threshold and maximum connections:

```
#(config)content-analysis
#(config content-analysis)edit bluecoat-local-request
#(config icap bluecoat-local-request)max-conn <number_of_connections>
ok
#(config icap bluecoat-local-request)exit
#(config content-analysis)edit bluecoat-local-response
#(config icap bluecoat-local-response)defer-threshold <threshold_as_percentage>
ok
#(config icap bluecoat-local-response)max-conn <number_of_connections>
ok
```

Note the following about the commands:

- `max-conn<number_of_connections>` applies to both request and response service.
- `defer-threshold <threshold_as_percentage>` applies to only the response service.

> **Note:** These settings are not persistent across reboots. This limitation will be addressed in a future release.

Fixes in Advanced Secure Gateway 6.7.3.2

- This release includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.3.2" on the next page.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.3.2

Advanced Secure Gateway 6.7.3.2 includes bug fixes. This update:

TCP/IP and General Networking

B#	Issue
253748	Fixes an issue where the appliance might have restarted in process "cookie-monster" due to a small race condition affecting connections that were required to retransmit packets over a long period.
254461	Fixes an issue where the appliance might have become unresponsive during the upgrade to 6.7.3.1 when IWA Direct authentication was used.

Advanced Secure Gateway 6.7.3.1 GA

Release Information

- **Release Date:** 11/21/2017
- **Build Number:** 210041

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x; 10.1.x and later
- **Management Center:** 1.5.x through 1.11.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and later
- **SSL Visibility:** 4.1.1.x and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.2.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

  > **Note:** Java 8 Update 144 is currently not compatible with Advanced Secure Gateway releases.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.3.1

- Advanced Secure Gateway 6.7.3.1 introduces new features and enhancements. See "New Features in Advanced Secure Gateway 6.7.3.1" on the next page.

Fixes in Advanced Secure Gateway 6.7.3.1

- This release includes a number of fixes. See "Fixes in Advanced Secure Gateway 6.7.3.1" on page 155.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

New Features in Advanced Secure Gateway 6.7.3.1

Advanced Secure Gateway 6.7.3.1 introduces the following new features.

Content Analysis Features

Symantec Antivirus

This release offers support for the Symantec antivirus engine.

Symantec antivirus is available with a subscription-based license. Configure antivirus scanning configuration in the Management Console (**Content Analysis > Services > AV Scanning Behavior**).

- Full information:

  ***Advanced Secure Gateway 6.7.x Help* — Set AV Scanning Behavior Options**

Symantec Advanced Machine Learning

By combining deep knowledge of threats and files with state-of-the-art machine learning, Symantec Advanced Machine Learning (AML) is able to understand characteristics of files and create a probability score to determine whether a file is safe. Rather than using signatures to match patterns, machine learning uses proven, well-tested, statistical methods to learn about files. Using this approach, new and previously unknown threats can be stopped. Even when the attack changes--through replication mechanisms, distribution mechanisms or the payload itself--AML works to stop threats effectively.

After scanning a file to understand its characteristics, the AML algorithm computes the probability of a file being malicious. This probability score determines what Content Analysis should do next with the file.

- Files with a high probability of being malicious will be blocked outright (convicted).
- Files with a low probability of being a threat are tagged "clean" and allowed for normal use (exonerated).
- Suspicious files will be sent to configured AV engines for further analysis.

Symantec Advanced Machine Learning is included with antivirus subscriptions. It is activated when you activate the Symantec Antivirus license.

- Full information:

  ***Advanced Secure Gateway 6.7.x Help* — Improve Malware Scanning Results with Predictive Analysis**

Symantec Cloud Sandboxing

Symantec offers a cloud-based dynamic malware analysis service that provides the ability to detect advanced threats. In addition to detonating and detecting malware on virtual machines, Symantec Cloud Sandboxing uses a suite of analysis technologies, coupled with Symantec global intelligence and analytics data, to accurately detect malicious code.

In addition, Cloud Sandboxing uses a behavioral analysis system that monitors files as they run, comparing the behaviors of the program to the behaviors of the billions of malicious samples Advanced Secure Gateway has

analyzed over the years. As opposed to signatures, Cloud Sandboxing employs behavioral profiles and file reputation data to accurately identify files as benign or malicious.

The Symantec Cloud Sandbox service is subscription-based and requires no configuration other than activating the license and enabling the service (**Sandboxing > Settings**).

- Full information:

  ***Advanced Secure Gateway 6.7.x Help* — Configure Sandbox General Settings**

Proxy Features

Policy for Specifying Cookie Persistence in Authentication

You can now control cookie persistence during user authentication. The following CPL action was added:

`authenticate.persist_cookies(auto|no|yes)`

where:

- `auto` means that the cookie persistency value configured in the realm will be used.
- `no` means that the session cookie will be used in authentication in this transaction.
- `yes` means that the persistent cookie will be used in authentication in this transaction.
- Full information:

  Content Policy Language Reference

Specify the Client Certificate Validation CCL via VPM

A **Set Client Certificate Validation CCL** object is available in the Visual Policy Manager (VPM). Use this object to specify the client certificate list (CCL) to use for matching intercepted SSL connections.

This policy object generates the following CPL (the condition was added in version 6.7.2):

`client.certificate.validate.ccl(`*`CCL_ID`*`)`

To use the policy object, add a rule to the **SSL Intercept Layer** and select **Set Client Certificate Validation CCL** from the Action column.

- Full information:

  Visual Policy Manager Reference

Enhancements and Changes in Advanced Secure Gateway 6.7.3.1

Advanced Secure Gateway 6.7.3.1 introduces the following enhancements and changes:

Configurable Port for Symantec Malware Analysis Sandboxing

This release allows you to configure the port for communication with Symantec Malware Analysis. When you add or edit a Malware Analysis server, the Add Server dialog shows a new **Port** field. This enhancement allows integration with an external Content Analysis 2.1 server, which includes Malware Analysis. By default, the port value is 443.

- For integration with Content Analysis on-box sandboxing, specify port 8082 (requires CA v2.1 or later).
- For integration with standalone Malware Analysis, use the default port 443.

SSL Intercept and DNS Layers Supported in Tenant Policy

SSL Intercept and DNS transactions now evaluate tenant determination policy in the landlord policy file. This allows `<ssl-intercept>` and `<dns>` layers to be defined and executed in tenant-specific policy. Previously, these layers were supported in the default tenant policy only.

ICAP Outbound Source IP Selection

When a network interface on the appliance is configured to use multiple IP addresses, the outbound source IP address used in the connection from the Advanced Secure Gateway appliance to the ICAP server is now selected in a round-robin manner. This selection process helps prevent port saturation under heavy load, especially when the connection is not persistent.

Data Leak Exception Page

Users now see a data leak exception page when HTTP/HTTPS POST requests are sent to Symantec DLP and a policy violation occurs.

HTTP Log Shows Reasons for Non-Cacheable Transaction

The HTTP log now indicates the reason(s) that a transaction is not cacheable. The information is logged as follows:

`"Server response made transaction Non-Cacheable:reason(s)=<set of reasons>"`

OpenLDAP Upgrade

This release supports OpenLDAP version 2.4.44.

Fixes in Advanced Secure Gateway 6.7.3.1

Advanced Secure Gateway 6.7.3.1 includes the following security advisory fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.3.1 includes security advisory fixes. This update:

B#	Issue
N/A	Addresses NTP vulnerabilities. Refer to SA139.
N/A	Addresses NTP vulnerabilities. Refer to SA147.
N/A	Addresses OpenSSL vulnerabilities. Refer to SA141.
N/A	Addresses NSS security vulnerabilities. Refer to SA153.

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.3.1 includes bug fixes. This update:

Access Logging

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

Authentication

B#	Issue
251438	Setting the windows-domains LDAP ping protocol as UDP might cause the appliance to restart.

CLI Consoles

B#	Issue
250624	Fixes an issue where exceptions viewed via the Management Console (exceptions_config.html) had links that did not show current exceptions.

Collaboration

B#	Issue
252297	Fixes an issue where a failure during handoff caused the WebEx proxy to restart in process "WebExWorkerManager" in "libc.so".
249338	Fixes an issue where the **Details** field in Active Sessions didn't display information for 'symc.webex.com' connections.

HTTP Proxy

B#	Issue
247731	Fixes an issue where pipelined requests did not follow routing domain rules.

Kernel

B#	Issue
246322	Fixes an issue where the appliance restarted due to a page fault at 0xfffffffffffffc0 in process group "PG_CFSSL" in process "HTTP CW 3D18931B50" in "kernel.exe".
250933	Fixes an issue where the appliance was unresponsive until it was rebooted. The issue was caused by a large memory allocation from CFS downloader.

Policy

B#	Issue
250453	Fixes an issue where the CPU0 usage was high when policy was updated in a multi-tenant policy configuration.
250179	Fixes an issue where the exceptions file (**Configuration > Exceptions > View > Exceptions Configuration**) did not show currently-defined exceptions. Clicking any link of a known exception displayed the message "No exception found called '<*exception_name*>'".

SSL Proxy

B#	Issue
252794	Fixes an issue where the RSA public exponent was always 3 for emulated certificates. For best security, the public exponent now copies the existing public exponent for RSA server certificates.

SSL/TLS and PKI

B#	Issue
248792	Fixes an issue where the threshold monitor restarted the proxy. This issue occurred when the SSL and crypto memory usage were high.

TCP/IP and General Networking

B#	Issue
249805	Fixes an issue where both proxies in a failover group reported as master. This issue occurred when the group was configured with link aggregate (LAG) interfaces.
252709	Fixes an issue where the proxy stopped sending requests to the origin content server (OCS).
251889	Fixes an issue where Bandwidth Management Class with a child configured stopped a TCP connection. This issue occurred when the parent's maximal bandwidth was reached.
244784	Fixes an issue where packets might have exited an incorrect interface in IPv6 configuration when static routes were configured.

Advanced Secure Gateway 6.7.2.3 PR

Release Information

- **Release Date:** November 14, 2017
- **Build Number:** 209947

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x through 1.10.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.1.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

- An incompatibility exists between Advanced Secure Gateway 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:
  http://www.symantec.com/docs/TECH246741

Fixes in Advanced Secure Gateway 6.7.2.3 PR

- For fixes in this release, see "Fixes in Advanced Secure Gateway 6.7.2.3 PR" on the next page.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.2.3 PR

Advanced Secure Gateway 6.7.2.3 includes bug fixes. This update:

SSL Proxy

B#	Issue
253377	Fixes an issue where random HTTPS pages did not load when SSL Proxy was used. Refer to TECH248154 for details: http://www.symantec.com/docs/TECH248154

TCP/IP and General Networking

B#	Issue
250616	Fixes an issue where the appliance might have restarted in Process group: "PG_TCPIP", Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so". This issue occurred when delayed intercept was enabled.
250637	Fixes an issue where the appliance might have restarted in Process group: "PG_TCPIP" in Process: "stack-api-worker-0" in "libmemory.so". This issue occurred when dynamic bypass was enabled.

Advanced Secure Gateway 6.7.2.2 PR

Release Information

- **Release Date:** September 12, 2017
- **Build Number:** 206525

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x through 1.10.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.1.x. Refer to Content Analysis documentation on MySymantec for more information.

Upgrading To/Downgrading From This Release

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Third-Party Compatibility

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

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

- An incompatibility exists between Advanced Secure Gateway 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:
  http://www.symantec.com/docs/TECH246741

Fixes in Advanced Secure Gateway 6.7.2.2 PR

- For fixes in this release, see "Fixes in Advanced Secure Gateway 6.7.2.2 PR" on the next page.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

Fixes in Advanced Secure Gateway 6.7.2.2 PR

Advanced Secure Gateway 6.7.2.2 is a patch release that includes the following bug fixes.

Bug Fixes in this Release

HTTP Proxy

B#	Issue
250638	ProxySG may restart in Process: "HTTP SW 100C7373A40 for 4062EB83A40" in "libce_admin.exe.so" when FSH caching is enabled, disk is full and reinitializing.

SSL Proxy

B#	Issue
251011	When running SGOS 6.7.2.1, accessing some HTTPS sites will fail with Chrome or Fire Fox, when Protocol Detection is enabled or SSL Interception is not enabled.
250323	SG may restart in process: "CFSSL Cert Proprietor" in deployments with hundred(s) of CCL's and 600+ certificates.

TCP/IP and General Networking

B#	Issue
250732	Bandwidth Management may stop working after a while for higher limits (range of 100 Mbps and up).
250495	ProxySG may experience a software exception code: 0x810001 in Process group: "PG_TCPIP" in Process: "stack-admin" causing the unit to restart when Bandwidth Management is enabled.

Advanced Secure Gateway 6.7.2.1 GA

Release Information

- **Release Date:** July 31, 2017
- **Build Number:** 204794

Compatible With

- **BCAAA:** 5.5 and 6.1
- **Reporter:** 9.5.x and 10.1.x
- **Management Center:** 1.5.x through 1.10.x
- **ProxyClient:** 3.4.x (ADN functionality not supported)
- **Unified Agent:** 4.7.x and 4.8.x
- **SSL Visibility:** 4.1.1 and later
- **Advanced Secure Gateway Appliances:**
  - S500, S400, S200

  See "Advanced Secure Gateway Appliance Resources" on page 201 for links to platform documentation.

Content Analysis

- This release includes Content Analysis version 2.1.x. Refer to Content Analysis documentation on MySymantec for more information.

Third-Party Compatibility

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

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

Upgrading To/Downgrading From This Release

- The following are the supported upgrade/downgrade paths for this release:
  - Upgrade to Advanced Secure Gateway 6.7.2.1 from version 6.6.5.7 or later.
  - Downgrade from Advanced Secure Gateway 6.7.2.1 to version 6.6.5.7 or later.
- After upgrading or downgrading to this release, clear the browser cache to ensure you are displaying the correct version of Content Analysis help topics.
- After an upgrade or downgrade, the current list of ciphers and the current list of HMACs—as shown in `view`

subcommand output—may change. If you modify the current list using the `add`, `remove`, and `set` subcommands, the changes persist after system upgrades, downgrades, and reboots; however, the current list will not be identical to the list prior to upgrade/downgrade if the system must consider deprecated ciphers and HMACs. (B#241332)

To understand the behavior after upgrade/downgrade, refer to `#(config ssh-console)`**`ciphers`** and `#(config ssh-console)`**`hmacs`** in the "Privileged Mode Configure Commands" chapter in the SGOS *Command Line Interface Reference*.

- An incompatibility exists between Advanced Secure Gateway 6.7.2 and older versions of vsftpd FTPS server using weak ciphers. Refer to TECH246741 for details:

  http://www.symantec.com/docs/TECH246741

- The *Advanced Secure Gateway Upgrade/Downgrade Quick Reference* details the supported upgrade/downgrade paths for this release:

  https://www.symantec.com/docs/DOC11230

Changes in Advanced Secure Gateway 6.7.2.1

- Advanced Secure Gateway 6.7.2.1 introduces new features and enhancements. See "New Features in Advanced Secure Gateway 6.7.2.1" on the next page.

Fixes in Advanced Secure Gateway 6.7.2.1

- Because this is the inaugural 6.7.x release, Symantec is reporting only security-related fixes for Advanced Secure Gateway 6.7.2.1. See "Fixes in Advanced Secure Gateway 6.7.2.1" on page 177.
- To see any Security Advisories that apply to the version of Advanced Secure Gateway you are running, go to:

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

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

Limitations

- See "Advanced Secure Gateway 6.7.x Limitations" on page 180 for a description of limitations in this release.

Known Issues

- See "Advanced Secure Gateway 6.7.x Known Issues" on page 182 for a list of all issues that Symantec is aware of in Advanced Secure Gateway 6.7.x.

New Features in Advanced Secure Gateway 6.7.2.1

Advanced Secure Gateway 6.7.2.1 introduces the following new features.

Content Analysis Features

Integration with Symantec Endpoint Protection Manager

This Advanced Secure Gateway release supports integration with Symantec Endpoint Protection Manager (SEPM). After configuring SEPM, the system sends administrators a threat alert when sandbox analysis determines a file to be malicious. Administrators can then add the file hash to a file fingerprint hast list (blacklist) on the SEPM. Once the SEPM knows about the threat, no other end users will be able to run the blacklisted file; this stops the lateral spread of a malicious file on the network. In addition, administrators can use SEPM remediation policy to clean up the initial infection.

To configure this feature, select **Settings > Endpoint Integration** in the Sandboxing module.

- Full information:

  ***Content Analysis 2.1 WebGuide* — Integrate with Symantec Endpoint Protection Manager**

Send Sandboxing Results to Reporter

After the Advanced Secure Gateway appliance sends Content Analysis files to be executed in a configured sandbox, it receives a report on that activity and the data is visualized in the Overview and Content Analysis modules. The appliance can also forward this data to Reporter, where it is matched with ProxySG data (based on the connection's transaction ID) to create a set of reports for visualization in Symantec Management Center.

To configure content analysis uploads to Reporter, select **Settings > Reporter** in the Content Analysis module. To configure ProxySG log uploads to Reporter, select **Configuration > Access Logging > Logs > Upload Client** in the Proxy module.

> **Note:** This feature requires the following additional software versions:
> - Reporter version 10.4.1 and later
> - Management Center version 1.6.1 and later

- Full information:

  ***Content Analysis 2.1 WebGuide* — Send Sandboxing Results to Symantec Reporter**

  ***SGOS Administration Guide* — Configuring the Access Log Upload Client**

Proxy Features

Support for Universal Policy

Universal policy is a set of global rules that you create in Symantec Management Center and apply to users in any location. The policy can include global rules that apply to both on-premises and Web Security Service (WSS) users, as well as individual rules that apply to only one or the other. It can also include location-specific policy when necessary. In essence, universal policy comprises the various rules that reflect your organization's acceptable use policy. Using Management Center to distribute the policy to on-premises devices and the WSS makes it easy to apply the relevant policy to all users in your organization.

To support universal policy, this release of SGOS allows you do the following on the appliance:

- Specify and change enforcement domains in the ProxySG Visual Policy Manager.
- Designate sections of policy as being appliance- or WSS-specific using the `#if enforcement=appliance` and `#if enforcement=wss` variables, respectively.
- Specify the ICAP service type in the Management Console or in the CLI.
- Configure the enforcement classification file in the CLI.

Caution: Universal policy settings are not retained after a downgrade if you install VPM policy in the downgraded version. For example, if you enable enforcement domains, downgrade to a previous version of Advanced Secure Gateway (that does not support universal policy), install VPM policy, and then upgrade to 6.7.x again, enforcement domains are disabled and universal policy is lost. If you do not install VPM policy in the downgraded version, however, universal policy settings are preserved if you upgrade to 6.7.x. This is expected behavior.

- Full information:

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

  ***Content Policy Language Reference* — Overview of the Content Policy Language**

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

Cloud Policy Configuration in Management Console

You can now configure cloud policy in the Proxy module (**Configuration > Cloud Configuration > Cloud Registration**); previously, only CLI commands were available. See the Auto Policy Synchronization Quick Reference.

Detection and Improved Handling for Invalid Characters

In this release, support has been added for:

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

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

DNS Access Logging

A new DNS access log for the DNS proxy was added as a default access log:

- dns is included in the `#(config access-log) default-logging` command.
- To configure the DNS access log, go to **Proxy > Configuration > Access Logging > Upload Client**. To trigger log transfers to the client, go to **Proxy > Configuration > Access Logging > Upload Schedule**.
- IPv6 is not supported at this time.
- On downgrade, the DNS default log facility remains visible in the Management Console, though logging will not work. Issue the `#restore-defaults factory-defaults` command to remove DNS access log objects.

SSLV Offload

In this release, you can connect one or more appliances to an SSL Visibility appliance running version 4.1.1 and later to offload SSL/TLS traffic processing. Configuring SSLV offload requires that you identify the Advanced Secure Gateway and SSLV appliances to each other using their respective serial numbers.

Configure SSLV offload on the appliance using one of the following methods:

- Managing SSLV appliances in the Proxy module (**Configuration > SSL > SSLV Offload**)
- Issuing the `#(config ssl)sslv-offload` command

You must also add Advanced Secure Gateway appliance information to the SSLV appliance(s). Refer to the following documentation for complete steps.

- Full information:
  SSL Visibility Appliance Administration & Deployment Guide

  ***SGOS Administration Guide* — Managing the SSL Proxy**

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

Routing Domains Configuration in Management Console

Routing Domains allow you to route traffic for unique networks through the same appliance, where each network has its own gateway and DNS server. This release introduces this feature as a configurable option in the Proxy module (**Configuration > Network > Routing > Routing Domains**).

Network HSM Failover

Hardware security module (HSM) failover applies to HSM keyrings contained in an HSM keygroup. If the appliance encounters an error when attempting to use an HSM keyring, it is flagged as failed. The signing operations will be tried on another member of the HSM keygroup, if applicable. The appliance will periodically attempt to see if the error has been corrected. Once it has been, the HSM keyring will be put back into service.

- Full information:
  Intercepting SSL with the SafeNet Java HSM

IWA Direct Feature Enhancements

- Previously, the appliance sent LDAP pings for domain controller discovery over the TCP protocol. In this release, you can specify UDP or TCP as the protocol using the following command:

  ```
  #(config security windows-domains)ldap-ping-protocol {tcp | udp}
  ```

  When upgrading to this release, the TCP setting is preserved for existing Windows domains and the default for new domains is UDP.

- By default, the appliance now uses the SMB2 protocol for connecting to the Active Directory server. If the server still uses the SMB1 protocol, issue the following command:

  ```
  #(config security windows-domains)smb2 disable
  ```

User Email Address Reporting

The appliance can report on the email address of an authenticated SAML or IWA Direct user. This allows you to include the email address in:

- HTTP/S requests to the Elastica Cloud Access Security Broker (CASB) Gateway
- Access log formats, using the new field `x-cs-user-email-address`
- Exception pages and policy, using the new `$(user.email_address)` substitution variable

For unsupported authentication realms, the field returns an empty string.

Refer to TECH246128 for an example of how to send the email address in requests to the CASB service.

The following CLI subcommands were added for IWA Direct:

```
#(config iwa-direct realm_name)email-address enable
```

Enable the feature to report on the user's email address. Use in conjunction with the **email-attribute** subcommand.

```
#(config iwa-direct realm_name)email-attribute attribute
```

Specifies the attribute that represents the user's email address. Enable retrieval of this attribute with the **email-address enable** subcommand.

The following CLI subcommand was added for SAML:

`#(config saml realm_name)email-address-attribute attribute`

Specifies the attribute that represents the user's email address and retrieves the value of the attribute.

> **Note:** Map the SAML email address attribute to the relevant field on the IDP. For example, if your IDP is Shibboleth, map the `emailAddress` attribute to the `mail` field.

- Full information:

  Support article TECH246128**:** http://www.symantec.com/docs/TECH246128
  ***Command Line Interface Reference* — Privileged Mode Configure Commands**

  ***SGOS Administration Guide* — Access Log Formats**

Client Certificate Emulation

To facilitate choosing signing certificates for the client in a reverse proxy deployment, this release includes client certificate emulation. When this feature is enabled:

- The appliance requests a certificate from the client.
- If the client returns a certificate, the appliance copies the certificate attributes to a new client certificate (so that it appears to originate from the client). Emulation does not occur if the client does not return a certificate.
- The appliance presents the certificate during the SSL/TLS handshake when an OCS requests a client certificate.

The following CPL action was added to support this feature:

```
server.connection.client_issuer_keyring(no|<keyring_id>|
 <hsm_keyring_id>|<hsm_keygroup_id>)
```

where:

- no disables client certificate emulation; this is the default setting
- *<keyring_id>* means to use the specified keyring for client certificate emulation. This must be a valid keyring, specified on the appliance with a CA certificate.
- *<hsm_keyring_id>* means to use the specified HSM keyring for client certificate emulation.
- *<hsm_keygroup_id>* means to use the specified HSM keygroup for client certificate emulation.
- Full information:
  ***SGOS Administration Guide*- Managing X.509 Certificates**

  ***Content Policy Language Reference*— Action Reference**

TLS and Cipher Changes

New Defaults

On an initial upgrade to version 6.7.x, TLS 1.1 and 1.2 are the default protocol selections for the Management Console and the SSL device profiles. TLS 1.1 will be used if 1.2 is not available. TLS 1.0 has been disabled by default. The default ciphers suites have been correspondingly updated as well.

If the default protocols (TLS 1.0, 1.1, and 1.2) for the SSL device profile (as with the HTTPS Console service) were selected previously, only TLS 1.1 and 1.2 are selected by default now. If the SSL device profile protocols were changed from the defaults previously, the selections do not change.

- The predefined SSL passive-attack-protection device profile can be used by many services, such as Authentication, Access-log, ICAP, Secure ADN, and OCSP.
- Interoperability issues may arise if a default or user-configured device profile is used to connect to a remote service that does not understand TLS 1.1 or 1.2.
- Management Console will no longer connect to browsers that do not support TLS 1.1 or 1.2 (Chrome before v21, Firefox before v23, Internet Explorer 8 and 9).
- If an SSL device profile uses a custom cipher suite, that cipher suite will be overwritten on upgrade.
- BCAAA may or may not support TLS 1.1. or 1.2. If the BCAAA connection fails, enable TLS 1.0 on the default SSL device profile.
  Notes:
  - Windows XP and Windows Server 2003 do not support TLS 1.1 or TLS 1.2.
  - Windows Vista and Windows Server 2008 do not support TLS 1.1 or TLS 1.2.
  - If you are using a Windows version later than those listed here, do not edit the default SSL device profile.
- User-configured SSL device profiles and Management Console settings retain their previous settings. Symantec strongly recommends updating the settings as soon as possible. If Management Center attempts to copy a configuration containing these older protocols to a different device, the operation will fail, as the client device treats copied device profiles as new profiles.
- The reverse proxy is unchanged. The defaults are TLS 1.0, 1.1, and 1.2 enabled. SSLv3 and SSLv3 are options.
- For the forward proxy, SSLv2 and v3 are disabled by default.
- SSLv2 and SSLv3 have been removed from the CLI for the Management Console and SSL device protocol; attempting to use them will generate errors.
- On a downgrade from version 6.7.x , your selections do not change (whether you kept the default selections or changed them).

Any subsequent upgrades to 6.7.x, for example after a downgrade, do not change the protocol selections; the protocols selected prior to the subsequent upgrade are retained.

AES-GCM and SHA384 Ciphers Support

The appliance now supports the following cipher suites for SSL forward proxy, reverse proxy, Management Console, SSL device profiles, and the SSL client as well as the existing forward proxy support:

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-GCM-SHA384

ECDSA Signed Certificate Support

The appliance can now verify ECDSA certificates during the SSL handshake, as well as DSA and RSA.

Increased Key Sizes for Emulated Server Certificates

The key size supported for emulated DSA and ECDSA server certificates has been increased to 2048 bits. The key size for emulated RSA server certificates is now matched up to a maximum of 4096 bits. For example, when the appliance intercepts a 4k RSA server certificate, it will emulate a 4k certificate.

On downgrade, the previous RSA 2k and DSA/ECDSA 1k limits will be enforced.

> **Caution:** High volumes of intercepting web sites with 4K RSA keys might affect performance on smaller-scale models such as the SG-S200 series. For details and a workaround for this issue, refer to TECH253498: https://www.symantec.com/docs/TECH253498

- Full information:
  ***SGOS Administration Guide* — Configuring Management Services, Authenticating a ProxySG Appliance, Managing SSL Traffic, Managing the SSL Proxy**

  ***SGOS Command Line Interface Guide* — Privileged Mode Configure Commands**

Authenticate Outbound SSH Connections

You can add host keys, select ciphers, and select HMACs to use for outbound SSH connections, such as the SCP upload client for access logs. See "Configure SCP Upload Client " on the next page for details.

To configure host keys, ciphers, and HMACs in the Management Console, select **Configuration > Authentication > SSH Outbound Connections** in the Proxy module.

To obtain a host key from a remote host, use the Management Console (**Configuration > Authentication > SSH Outbound Connections > Known Hosts** in the Proxy module).

The following CLI commands were added to support this feature:

```
#(config ssh-client)ciphers
#(config ssh-client)hmacs
#(config ssh-client)known-hosts
```

- Full information:

  ***SGOS Administration Guide* — Controlling Access to the Internet and Intranet**

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

Configure SCP Upload Client

SGOS supports the secure copy protocol (SCP) upload client for access log uploads. To configure SCP for access log upload, select **Proxy > Configuration > Access Logging > Logs > Upload Client**. Select **SCP** for the Client type.

The following commands were added to support this feature:

```
#(config log log_name)client-type scp
#(config log log_name)scp-client
```

> **Note:** Before you can configure the SCP upload client, you must add host keys and select ciphers and HMACs for outbound SSH connections, as described in " Authenticate Outbound SSH Connections " on the previous page.

Kerberos Constrained Delegation

In deployments where the User Principal Name (UPN) is not included in client certificates, configure Kerberos Constrained Delegation (KCD) to use the authorization username for authentication. Use the following CLI command:

```
#(config)security iwa-direct edit-realm realm_name
#(config iwa-direct realm_name)kcd-use-authz-name enable
```

where *realm_name* is your IWA realm name.

- Full information:

  Using Kerberos Authentication in a Reverse Proxy Environment

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

Support for Application Groups

This release introduces CASB policy that organizes similar web applications into named groups. This feature improves ease of use by providing you with the ability to write policy for groups of similar applications instead of writing multiple rules for individual applications. In addition, note that:

- Applications can belong to more than one group.
- As new application are added, removed, or modified, the group information automatically reflects the change. Application group policy and reporting are also updated.

To use this feature:

- Ensure that the appliance has a valid subscription for the CASB Audit AppFeed for SG. Modifications to CASB data are automatically provided in database updates via the subscription feed.
- Enable the Application Classification service.
- Select Intelligence Services as the content filtering data source.

The following were added to support this feature:

- The ability to look up application groups for a URL and display the list of groups (in the Management Console, **Proxy > Configuration > Application Classification > General**).
- In the `bcreportermain_v1` and `bcsecurityanalytics_v1` access log formats, an `x-bluecoat-application-groups` field.
- An **Application Group** VPM object used to apply policy actions to a specified application group.
- A CPL condition `request.application.group=` to test the specified application group for a URL
- A CLI subcommand that displays supported application groups or the groups to which the specified application belongs:

  `#(config application-classification)`**`view groups`** `[`**`application`** `<`*`application_name`*`>]`

- Full information:

  ***SGOS Administration Guide* — Filtering Web Content, Creating Custom Access Log Formats, *and* Access Log Formats**

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

  ***Content Policy Language Reference* — Condition Reference**

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

Possible Values of Application Attributes

> **Note:** The data feed for this feature will be in Advanced Secure Gateway 6.7.4. To use this feature, upgrade to 6.7.4 when that release is available.

This release introduces a CLI subcommand to display possible values for a specified application attribute:

- `#(config application-attributes)`**`view possible-values`** `<`*`attribute_name`*`>`

  If an attribute name contains spaces, enclose it in double quotation marks ("). When writing policy that includes the `request.application.<`*`attribute_name`*`>=` condition, use this subcommand to ensure that the CPL parameters are valid.

To use this feature:

- Ensure that the appliance has a valid subscription for CASB Audit AppFeed for SG. Modifications to CASB data are automatically provided in database updates via the subscription feed.
- Enable the Application Classification and Application Attributes services.
- Select Intelligence Services as the content filtering data source.
- Full information:

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

Enhancements and Changes in Advanced Secure Gateway 6.7.2.1

Advanced Secure Gateway 6.7.2.1 introduces the following enhancements and changes:

Pipelining Disabled by Default for Better Network Performance

Due to recent advances in web browsers, pipelining provides limited benefits and can increase CPU utilization in certain workloads. Thus, in a new installation of 6.7.x, or upon an upgrade to this release, pipelining is disabled by default.

Ability to Add Kafka `MessageSet` Headers to Access Logs

If an access log has Kafka client and gzip file type selected, you can configure the appliance to add a `MessageSet` header to the compressed log files so that the Kafka broker processes the data correctly as gzip-compressed data.

Use the following command to enable/disable the header (by default, the setting is disabled):

```
#(config log log_name)kafka-client [no] message-set-codec
```

Refer to the *Command Line Interface Reference* for details on this command.

Making any change to an access log's upload client configuration that reverses the previous `MessageSet` header state (that is, the header's presence or absence in the log files) can cause future log uploads to fail. You must take additional steps to ensure that logs are processed correctly; for details, refer to the *SGOS Administration Guide*.

Cipher and HMAC Support in FIPS Mode

After booting the appliance in FIPS mode, issue the following CLI commands to view the default cipher/HMAC lists, current selections, and available ciphers/HMACs:

```
#(config ssh-console)view ciphers
#(config ssh-console)view hmacs
#(config ssh-client ciphers)view
#(config ssh-client hmacs)view
```

Enhanced CCL Policy

This release adds support for configuring the CA Certificate List (CCL) to use for a specific IP address or hostname. When this object is not used, the default server certificate validation CCL is applied.

- Full information:

- ***SGOS Administration Guide* - Specifying an Issuer Keyring and CCL Lists for SSL Interception**
- ***Visual Policy Manager Reference* - The Visual Policy Manager**
- ***Content Policy Language Reference* - Properties Reference**

Skype for Business Support

In previous versions of SGOS, some Skype For Business and Microsoft Lync application connections failed when the appliance intercepted SSL traffic on port 443 and UDP port 5061 was firewall-restricted. Some issues occurred with logging in, joining meetings, meeting audio, and starting presentations. Issues occurred due to the following limitations:

- Lack of OCSP stapling/Certificate Revocation List (CRL) distribution point support
- Partial support for Session Initiation Protocol (SIP)
- Lack of support for Microsoft Traversal Using Relay NAT (MS-TURN) protocol

To restore chat client communications, this SGOS release supports:

- CRL distribution points on emulated certificates, which you configure in the SSL proxy service
- SIP and MS-TURN protocol detection and policy control, which you configure in the <ssl-access> layer
- Full information:
- ***Office 365 Integration & Best Practices WebGuide* - Skype/Lync Fix: SGOS Configuration**
- ***SGOS Administration Guide* - Managing Outlook 365 Applications**
- ***Visual Policy Manager Reference* - The Visual Policy Manager**
- ***Content Policy Language Reference* - Conditions Reference *and* Properties Reference**
- ***Command Line Interface Reference* - Privileged Mode Configure Commands**

Fixes in Advanced Secure Gateway 6.7.2.1

Advanced Secure Gateway 6.7.2.1 includes the following security advisory fixes and bug fixes.

Security Advisory Fixes in this Release

Advanced Secure Gateway 6.7.2.1 includes security advisory fixes. This update:

B#	Issue
N/A	Patches vulnerable code. For details, refer to the Advisory Details section in SA117.
N/A	Patches vulnerable code.For details, refer to the Advisory Details section in SA105.
N/A	Patches vulnerable code. For details, refer to the Advisory Details section in SA132.

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

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

Bug Fixes in this Release

Advanced Secure Gateway 6.7.2.1 includes bug fixes. This update:

Security

B#	Issue
235633	Fixes an issue where auto-complete was not disabled on password fields in forms on policy exception pages. After an upgrade to version 6.7.x, the system does not pick up the changes automatically; you must edit your current exceptions manually to get the changes. Refer to the "Update Exceptions Manually" topic in the *SGOS Upgrade/Downgrade WebGuide* for instructions.
242427	Fixes an issue where a specially-crafted HTTP message could cause the appliance to stop responding when certain policy gestures were used.

HTTP Proxy

B#	Issue
244110	Fixes an issue where HTTP(S) proxy upstream requests didn't have `Host` header canonicalized per RFC7230.

Management Console

B#	Issue
249339	Fixes an issue where using links (for example, from your site's internal webpages) to ProxySG advanced URLs could result in "400 Bad Request" errors.

Advanced Secure Gateway 6.7.x Reference Information

The following sections provide reference and compatibility information for the Advanced Secure Gateway 6.6.x software series.

Advanced Secure Gateway 6.7.x Limitations

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

Authentication

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

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

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

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

CASB AppFeed Uses Default BRR

When writing policy rules based on Business Readiness Rating (BRR), note that the CASB AppFeed applies its own Default BRR; it does not apply tenants' BRR modified from Symantec CloudSOC. TECH247736 describes this behavior: http://www.symantec.com/docs/TECH247736

Dynamic Categorization in Secure Mode

The CLI command to enable secure mode for dynamic categorization is not available in verson 6.7.x.

Before upgrading, enable secure mode in 6.5.x. If you have already upgraded, downgrade to version 6.5.x, enable secure mode, and upgrade again.

This deprecation was previously documented as B#237090.

Front Panel Configuration

The appliance supports only a static message on the LCD display on the front bezel. Configuration, status, or other details typically available on the front panel display are not available.

Use the serial console to perform initial configuration steps, use SSH or the serial console to view current status and appliance information.

Limited Signed Image Support

Installing images from HTTPS servers with a certificate signed by private CAs or with self-signed certificates is not possible.

Install upgrade images using the link provided by the download page at MySymantec, from an HTTP-based server, or from an HTTPS server with a certificate signed by a public CA.

Non-Functional Application Attributes Command

Advanced Secure Gateway 6.7.2.1 added the following CLI:

```
#(config application-attributes)view groups [attribute <attribute_name>]
```

This subcommand is visible in CLI output if you issue the **?** help parameter; however, this CLI is non-functional. Do not use this subcommand.

> **Note:** This CLI was removed in version 6.7.4.

Advanced Secure Gateway 6.7.x Known Issues

Symantec is aware of the following issues in Advanced Secure Gateway 6.7.x.

Access Logging

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#250158	The output for **#show config** does not indicate that SCP is set as the upload client (through either the CLI or the Management Console).	"Fixes in Advanced Secure Gateway 6.7.3.1" on page 155
B#250180	The log tail for a selected log in the Management Console (**Statistics > Access Logging > Log Tail**) displays the same entries multiple times when new entries do not appear. This issue occurs when there is a burst of traffic through the appliance, followed by no traffic or very slow traffic. This issue does not occur if traffic through the appliance is continuous.	"Fixes in Advanced Secure Gateway 6.7.3.1" on page 155
B#253658	Continuous access log upload stops after logging directory slots run out.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112 "Fixes in Advanced Secure Gateway 6.7.3.6" on page 141
SG-5340 B#267383	Access log objects are not created when the name includes a period (".")	

Authentication

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-9435	Admin authentication does not work when a BCSI-AC cookie is present in the browser.	
B#261934 SG-5812	When testing Windows SSO authentication from the CLI and when nested groups are enabled, the appliance might restart.	Fixes in 6.7.4.140

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#253544	A fix for a previous issue (B#246848) was implemented to prevent latency/firewall-related issues while contacting domain controllers (DCs) in remote geographical locations. The fix introduced an issue where the appliance can contact only DCs in the local Active Directory (AD) site to which the appliance belongs. As a result, because an appliance requires a read-write domain controller to join a domain, appliances with only local access to a read-only DC are unable to join the AD domain.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#256029	Kerberos authentication fails after the appliance's machine account password is changed in Active Directory and the machine account is enabled for AES-256 bit encryption.	"Fixes in Advanced Secure Gateway 6.7.3.6" on page 141
B#252851	The SNMP Schannel configuration stores incorrect CLI commands in the configuration archive, which prevents the configuration from being restored.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#255299	The proxy experiences a page fault restart in process "HTTP CW F95FD4B90" in "libc.so" related to the timing of actions when using the auth/debug log URL	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#253745	The domain controller (DC) resets the connection when the appliance sends an SMB1 Echo Request in an SMB2 environment.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#254717	AES authentication with Kerberos fails if the Kerberos load balancer username contains an upper-case letter.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112

Boot

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#262122 SG-5971	**Issue:** Downgrading from Advanced Secure Gateway 6.7.4.x to 6.6.x fails in the following cases: - The `restore-defaults` command was performed on version 6.7.4.x - The appliance was manufactured with version 6.7.4.x **Workaround:** Downgrade to version 6.7.3.x before downgrading to version 6.6.x.	

CLI Consoles

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255576 SG-6637	Issuing the `#show config` command might cause the appliance to restart if the URL set using `#(config)`**`statistics-export config-path`** is invalid.	"Fixes in Advanced Secure Gateway 6.7.3.6" on page 141

Content Analysis

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-16338	If multiple Java Management Consoles are accessed at the same time, the sandboxing link cannot be accessed.	
SG-14222	The Advanced Secure Gateway appliance can experience one or more silent host side restarts when a mini context is saved. This affects Advanced Secure Gateway 6.7.4.9 and later, which uses Content Analysis 2.4.x. There is no impact on the operation of the appliance.	
CAS-6281	**Issue:** Kaspersky anti-virus patterns in version 6.7.4.141 are not compatible with older Advanced Secure Gateway releases. **Workaround:** After a downgrade from version 6.7.4.141, force an update of the Kaspersky pattern files. In **Services > AV Patterns**, click **Force Update Now**.	
CAS-3156	When Content Analysis is integrated with Security Analytics, and SNMP trap alerts are enabled for the Sandboxing Threat Admin Alert (Asynchronous), the Security Analytics report URL does not show in the trap message.	
CAS-3190	Historical connections do not persist and are cleared upon shutdown.	
CAS-2813	Content Analysis is able to decompress/extract files from archives that have been compressed with gzip, bzip2, xz, lzip, and several other popular compression algorithms. If the archive uses a supported compression algorithm, Content Analysis is able to decompress the archive and send files within the archive to configured sandboxes for analysis. For zip and tar files with alternate compression algorithms (Lzma, ppmd, deflate), Content Analysis is unable to decompress the file but sends the archive to the sandbox if Content Analysis is configured to send this file type. Whether the sandbox application or service can decompress the archive and analyze its contents depends on the capabilities of the program. In the case of Symantec Malware Analysis, archives bypass sandbox analysis.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#222291 SG-2903	In very rare instances, the appliance does not detect the file system in a timely manner during bootup. When this issue occurs, the appliance reboots. The subsequent bootup sequence is successful.	
B#222104 B#249720 SG-2900	**Issue**: In rare cases, the Content Analysis configuration can be cleared during reboot. The frequency of occurrence is very low. If this issue does happen, the Content Analysis configuration must be restored. **Workaround**: As a preventative measure, save the Content Analysis configuration in a secure location and ensure it is available.	
B#231967 B#256510 SG-2897	The "cas-audit" log feature available in standalone Content Analysis 1.3.6.1 is not available in Content Analysis on the appliance.	
B#215932 SG-5382	Content Analysis doesn't send email notifications when it's restarted, even if E-mail is configured for the Reboot notification type.	

B#237010	OWA and Office Online (Office 365) URLs are treated as streaming traffic.	This issue is resolved.
		
		Install the following policy to bypass scanning of long-lived HTTP requests:
		
		`<Cache>`
		`server_url.path=/owa/ev.owa2`
		`server_url.query.regex="`
		`(.*)ns=PendingRequest`
		`(.*)ev=PendingNotificationRequest`
		`(.*)"`
		`response.icap_service(no)`
		`response.icap_service(proxyav, fail_closed)`
		
		Note: You can specify `outlook.office365.com` or `outlook.office.com`.

B#238672 SG-5427	Email notifications for Content Analysis statistics are not working correctly: ■ Attachments are omitted. ■ If using Java Web Start, the report title does not display the Content Analysis appliance name.	
B#254218	Virus definition count isn't displayed for the Symantec AV engine. This graphical issue has no impact on the AV engine's performance.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255006	Kaspersky might fail with an antivirus_engine_error (26:0x80070057) if the OCS sends non-RFC2616 characters in file names.	Fixes in 6.7.4.140

Documentation

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#253226	The *SGOS Administration Guide* and **Proxy** online help incorrectly state that you can specify a hostname for the custom access log upload client. In both the Management Console and the CLI, only an IP address is supported.	Fixed in February 2018.

Event Logging

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#215932 SG-5382	Content Analysis fails to send email notifications after a restart, even if E-mail is configured for Reboot notification type.	

FTP Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#258715 SG-4623	When ICAP REQMOD mirroring is enabled for the FTP proxy, the `s-action` access log field is occasionally not populated.	

HTTP Proxy

B#	Issue Workaround (if available)	Fixed In (when applicable)
247731	Pipelined requests do not follow routing domain rules.	"Fixes in Advanced Secure Gateway 6.7.3.1" on page 155
258588	HTTP debug log filters do not work unless both client and server IP filters are set.	"Fixes in Advanced Secure Gateway 6.7.4.3" on page 83

ICAP

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#219269 SG-2750	**Issue:** Adding an ICAP server to or removing an ICAP server from a load balancing group can, under some circumstances, cause the ProxySG appliance to stop responding. **Workaround:** Temporarily disable the health check for the ICAP object to reduce the chances of this issue occurring. Symantec recommends that you do the following: 1. In the Management Console, select **Configuration > Health Checks > General**. 2. Select the health check for the ICAP object and click **Edit**. The console displays an Edit Health Check dialog. 3. For Enabled state, select **Disabled: Unhealthy**. 4. Click **OK > Apply** to save your changes. 5. Add or remove the ICAP server to/from the load balancing group. 6. Repeat steps 1 -2. Then, re-enable the health check and save your changes.	
B#257787	Restoring defaults resets the Advanced Secure Gateway internal ICAP max connections to 25. Refer to ALERT2558 for details: http://www.symantec.com/docs/ALERT2558	"Fixes in Advanced Secure Gateway 6.7.3.6" on page 141
SG-5657 263858	The configuration file or SysInfo records do not reflect changes made successfully to internal ICAP settings.	Fixes in 6.7.4.4
SG-8038	The exception page from the DLP server (request modifier) is not displayed when the ICAP service is configured to use the vendor's 'virus found' page.	Fixes in 6.7.4.4

Initialization

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#263609 SG-5650	**Issue**: On the Advanced Secure Gateway, the birth certificate does not persist when the appliance is reinitialized from the bootloader. **Workaround**: Use the CLI command “request-appliance-certificate” to request a birth certificate.	

Management Console

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#260464	**Issue:** In the GUI, the bandwidth stats displays incorrect statistics for the parent class. **Workaround:**To view bandwidth management statistics, view the CLI output (show bandwitdh-management statistics) or access the JavaMC via the HTTP-Console.	
B#217492 SG-2794	When you manually configure link settings for a link aggregation member interface, the dialog provides an option to select **Half** under **Link Settings**. Half-duplex is not available for aggregate interfaces.	
B#217732 SG-2804	**Issue:** A link aggregation member interface might display an incorrect state after you delete an aggregate link. **Workaround:** To display the correct link state, refresh the Management Console page in the browser.	
B#249339	Using links (for example, from your site's internal webpages) to ProxySG advanced URLs might result in "400 Bad Request" errors.	"Fixes in Advanced Secure Gateway 6.7.2.1" on page 177
B#222815 SG-2923	The Threats count on the **ASG Overview** tab shows -1 before any threats are detected.	
B#222816 SG-2924	The Files Blocked, Websites Blocked, and Blocked by Sandboxing metrics on the **Overview** tab sometimes show -1 until they are populated with observed values.	
B#222887 SG-5389	The web browser used to load the Management Console can occasionally restart if the Management Console window is idle for a prolonged period of time.	
B#223044 SG-2928	The value of Files Blocked by Policy on the **Overview** tab does not reflect the number of files blocked by type when policy that uses free form entry rather than radio button list is used.	
B#250440 SG-5853	The **Overview**, **Content Analysis**, and **Sandboxing** tabs display an "Access Denied" message when you are logged in as a read-only user.	"Fixes in Advanced Secure Gateway 6.7.4.3" on page 83
B#254660	The Management Console does not accept system image download URLs consisting of more than 227 characters.	"Fixes in Advanced Secure Gateway 6.7.3.6" on page 141
B#260464	**Statistics > Bandwidth Mgmt** shows incorrect statistics for parent class.	Fixes in 6.7.4.140
B#261869 SG-7026	Adding an existing CA certificate whose name contains spaces to a CCL fails when using the Management Console.	Fixes in 6.7.4.140

MAPI Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#249746	Email attachment scan results are cached, but subsequent attachment downloads are sent to the ICAP server again instead of using previously cached data.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112

Performance

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#242394 SG-3672	The appliance experiences performance degradation if CPU usage is greater than 70% and the appliance is in transparent bridging mode with a significant portion of traffic being bridged.	
B#234568 SG-3252	Higher DNS utilization occurs under heavy load conditions. This was discovered in some internal performance tests.	

Policy

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#262506	If changing malware scanning from an internal to an external content analysis service and tenant policy is used or pushed from Management Center, you must manually install a VPM policy.	Fixes in 6.7.4.140
B#262197	In a transparent deployment, if authentication policy allows access for specific users/groups, users might not be able to join a meeting or log-in with Skype for Business.	Fixes in 6.7.4.140
B#236676 SG-3349	**Issue:** Disabling multi-tenant policy without first clearing tenant policy causes the appliance to stop logging the request body although `http.request.log_details (header,body)` exists in policy. **Workaround:** Re-enable multi-tenancy, clear the tenant and landlord policy files, and disable multi-tenancy again.	
B#242737 SG-2969	**Issue:** Users on mobile devices receive an Invalid Certificate Authority error when connecting to Google +. The issue occurs when using Google Chrome, Mozilla Firefox, Internet Explorer, and the device's default web browser. **Workaround:** Install the ProxySG appliance's SSL certificate on the mobile device.	

ID	Issue Workaround (if available)	Fixed In (when applicable)

B#231634
 	
SG-2852
	When multitenant policy exists, the `http.request.body.inspection_size()` property setting for the default tenant is always in effect, even if non-default tenants have different settings for the property. For example, if tenant A's body inspection size is 12 KB and the default tenant's is 10 KB, a request body size of 11 KB triggers an inspection even if tenant A's policy applies to the transaction. When this issue occurs, however, tenant A's `http.request.detection.other.threshold_exceeded()` setting is respected and applies correctly to the transaction.
	
	Consider the following example:
	
	`; default tenant policy`
	`; inspect up to 10 KB of the HTTP request body`
	`; monitor requests larger than 10 KB`
	`<proxy>`
	`http.request.body.inspection_size(10000) \`
	`http.request.detection.other.threshold_exceeded(monitor)`
	
	`; tenant A policy`
	`; inspect up to 12 KB of the HTTP request body`
	`; block requests larger than 12 KB`
	`<proxy>`
	`http.request.body.inspection_size(12000) \`
	`http.request.detection.other.threshold_exceeded(block)`
	
	Given these rules:
	
	■ A request that is subject to tenant A policy and with body size of 11 KB should be inspected in its entirety and not blocked. The request body's first 10 KB are inspected and the request is blocked.
	
	■ A request that is subject to tenant A policy and with body size of 13 KB should be inspected up to the first 12 KB and blocked. The request body's first 10 KB are inspected and the request is blocked.	

ID	Issue Workaround (if available)	Fixed In (when applicable)

B#249884
 	
SG-4058
	Issue: When policy includes multiple forms of county names (such as short names, ISO codes, and full names), IP addresses in geographical regions are allowed or denied as intended, but policy traces show regions with an incorrect verdict. For example, consider the following CPL:
	
	`<proxy>`
	`supplier.allowed_countries[uS, US, "Us", Ca, "United States"] (deny)`
	
	This policy results in denials of IP addresses in Canada and the United States, but a policy trace shows that "United States" is denied whereas "uS" is allowed.
	
	Workaround: Do not use multiple formats for country names in policy. Use a consistent format for all instances of country names, as follows:
	
	`<proxy>`
	`supplier.allowed_countries["United States", Canada] (deny)`	

B#250179	The exceptions file (**Configuration > Exceptions > View > Exceptions Configuration**) does not show currently-defined exceptions. Clicking any link of a known exception displays the message "No exception found called '<*exception_name*>'".	"Fixes in Advanced Secure Gateway 6.7.3.1" on page 155
B#251992 SG-4129	Policy performance is adversely affected when policy includes a large number of categories assigned to a single URL.	Fixes in 6.7.4.140
B#252806 SG-4248	Changing base user-defined exception fields does not update a policy-defined exception.	
B#252541	Rules with a **BlockPopupAds** object result in a 'Warning: Unreachable statement' error when installing VPM policy.	"Fixes Included from SGOS 6.7.4.130" on page 100
SG-7926	The `$(cs-categories)` and `$(cs-category)` substitutions do not display the correct URL rating on the coaching (NotifyUser) page.	Fixes in 6.7.4.4
SG-5359 B#267518	Coaching policy does not work when tenant policy is installed.	

Serviceability

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-8213	Enabling monitor also unexpectedly enables periodic uploads.	Fixes in 6.7.4.4

Services

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#261499	You might not be able to remove the default TCP Port 514 listener.	Fixes in 6.7.4.140
B#262653	When using HTTPS, ADN attributes might appear on the HTTPS proxy service. Note that attributes can be ignored, except when restoring the configuration archive.	Fixes in 6.7.4.140

SSL Proxy

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-13361	HTTPS sites the were denied by policy appear under Sessions > Errored Sessions.	
SG-18488	If tunnel-on-error is enabled, SSLv2 traffic is blocked, which might cause an outage.	
SG-18488	SSLv2 traffic cannot interpret the CH and tunnel-on-error cannot tunnel the session.	
SG-9211	**Issue:** SSL intercept policy set to `on_exception` does not work when policy includes any of the following: ▪ `server.certificate.hostname.category=` ▪ malware scanning policy The issue occurs because these policies involve server certificate category lookups. **Workaround:** Use full SSL interception for URLs or categories that should be blocked.	
B#252087	The appliance does not use the SNI extension in the server-side connection, which is required by some servers to respond with the correct server certificate in the TLS handshake.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#220528 SG-2866	**Issue:** If you remove external certificates from the external certificate list (ECL) and then delete those external certificates through the Management Console, the ECL state becomes inconsistent on the appliance. **Workaround:** Remove the external certificates from the ECL and apply the changes. Then, delete the external certificates.	
B#225793 SG-2985	**Issue:** **`#show config`** output does not enclose the `issuer-keyring` name in quotation marks. When the name includes spaces, subsequent attempts to apply the saved configuration fail. **Workaround:** Copy and paste the relevant sections of **`#show config`** output into a text editor. In the text editor, add the quotation marks around the keyring name manually, and re-apply the inline configuration.	
B#225611 SG-2970	When you change the SSL protocol version for a SSL device profile, the appliance selects compatible ciphers from the list of previously selected ciphers instead of selecting all the available ciphers for the new SSL protocol version.	
B#248792	Threshold monitor restarts occur with high memory usage by SSL connections.	Partial fix available in version 6.7.3. The behavior is improved in this release. "Fixes in Advanced Secure Gateway 6.7.3.1" on page 155

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#227420	Some versions of Management Center cannot connect to an appliance running in FIPS mode. **Note:** Advanced Secure Gateway 6.7.x introduces changes to how the appliance handles ciphers upon upgrade. Refer to the security fix for B#241332 to learn about this behavior change.	This issue is resolved. Add one of the following ciphers to the managed device: ■ aes256-ctr ■ aes192-ctr ■ aes128-ctr
B#252450 SG-4320	In STunnel and Bypass modes, the `x-cs-session-id` and `x-cs-server-certificate-key-size` access log fields are not populated.	
B#253905 SG-3605	The appliance stops responding when the **CRL distribution point** host name field (**Proxy > Configuration > Proxy Settings > SSL Proxy**) includes special characters.	
B#253926 SG-4323	In some cases, the appliance creates a certificate with the OCS IP address in the SAN **DNS Name** field when providing the client with a server-side TCP error message.	
B#255423 SG-4373	On a resumed connection, the `x-cs-server-certificate-key-size` access log field always displays `RSA[1024]`.	
B#257012 SG-6902	In bypass mode, the `x-cs-server-certificate-key-size` access log field displays `RSA[1024]`. In bypass mode, this information is not available and the field should not be populated.	"Fixes Included from SGOS 6.7.4.130" on page 100
B#257835 SG-4574	When adding a keyring through the CLI, whitespaces in field values are not ignored. This issue does not occur when creating keyrings through the Management Console.	
B#258130	`http.request.apparent_data_type` and `http.request.data.N` policy are not enforced.	"Fixes Included from SGOS 6.7.4.130" on page 100

ID	Issue Workaround (if available)	Fixed In (when applicable)

B#258141
 	
SG-4598
	Issue: Setting the **Client Certificate Validation CCL** or **Server Certificate Validation CCL** object in the **SSL Intercept Layer** in the VPM results in the error "Invalid action for <ssl-intercept> layer", and policy does not compile.
	
	Workaround: These gestures have been moved to the `<ssl>` layer. Write the policy in CPL instead, as follows:
	
	`<ssl>`
	`server.certificate.validate.ccl(CertList)`	

SG-6161 B#267269	After upgrading to ASG 6.7.4.2 , when SSL traffic is not intercepted by policy, SSL attributes (such as negotiated cipher or TLS version) are not available for use in policy conditions and access log fields. Refer to TECH253316 for more information on this issue.	"Fixes in Advanced Secure Gateway 6.7.5.1" on page 25

SSL/TLS and PKI

ID	Issue Workaround (if available)	Fixed In (when applicable)
SG-18246	**Issue:** If you are running Advanced Secure Gateway 6.7.4.9 and later, and the appliance is configured as a reverse proxy, the server persistence does not work. **Workaround:** Use Advanced Secure Gateway 6.7.4.8 or earlier until this issue is fixed.	
SG-18196	If the appliance is running Advanced Secure Gateway 6.7.5.1, the memory footprint increases by 3-5% due to the fix for SG-14742. If the footprint is around 70-75%, memory consumption can easily be pushed into memory regulation.	
B#250120	You cannot create a new HTTPS Reverse Proxy service in the Management Console (**Configuration > Services > Proxy Services > New Service**).	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#221218 SG-2885	A newly-created certificate displays "Not yet valid" for **Certificate expiry** (**Proxy > Configuration > SSL> Keyrings**). This issue occurs when the appliance's clock is ahead of the clock on the client running the Management Console.	
B#220453 SG-2861	If you issue the `#(config ssl)create signing-request` command and the certificate signing request fails, issuing the command again causes CLI to stop responding.	
B#225612 SG-2971	When changing the SSL protocol version for an SSL device profile, the appliance selects compatible ciphers from the list of previously-selected ciphers instead of the list of all available ciphers.	
B#248731 SG-3988	In the access log for the SSL reverse proxy service, `client-side negotiated-cipher` fields are populated incorrectly when GCM or SHA384 ciphers are used.	

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#253377	Random HTTPS pages do not load when SSL Proxy is used. Refer to TECH248154 for details: http://www.symantec.com/docs/TECH248154	6.7.2.3 PR
B#256750 SG-4462	In Skype for Business, video calling and screen sharing do not work.	Fixes in 6.7.4.1
B#257920 SG-4583	You receive the following error when uploading a signed configuration file that was just downloaded: **% Attempt to load configuration failed: signature verification failed: The message did not match the PKCS7 signature.** The error occurs when any signing keyrings are set on the appliance.	
B#256750 SG-4462	Skype for Business Video calling and screen sharing do not work.	Fixes in 6.7.4.1

SSLV Integration

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#242864 SG-3692	When SSL connections are denied using a server-negotiated cipher policy, access log values for negotiated cipher, negotiated cipher strength, and negotiated cipher size are not populated.	
B#256905 SG-4482	In SSLV offload mode, the `x-cs-session-id` access log field displays incorrect session ID values and the `x-cs-server-certificate-key-size` field always returns `RSA[1024]` for key size.	
B#258272 SG-4612	With SSLV offload enabled and policy enforcing cipher based properties, some SSL cipher access log fields present SSLV values instead of ProxySG appliance values. For example, instead of displaying `AES256-SHA` a field shows `RSA-AES256-CBC-SHA`.	
B#256791	In SSLV offload mode, Symantec recommends using the default TCP window size of 65535. Increasing the TCP window size might result in stalled connections.	"Fixes Included from SGOS 6.7.4.130" on page 100

System Statistics

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#262919 SG-4890	When the appliance is experiencing a heavy load, running the `clear-statistics persistent` CLI command might cause the appliance to stop passing traffic.	Fixes in 6.7.4.140

TCP/IP and General Networking

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#258974 SG-4633	When booting up the appliance, if the first DNS server in the primary group is unreachable, the appliance might stop booting.	Fixes in 6.7.4.140
B#263272 SG-7127	The appliance might return a false attack in progress status from an SNMP walk.	Fixes in 6.7.4.140
B#257272	Downloads of large files via SOCKS proxy on high-speed networks (2Mbps+ speed) time out.	"Fixes Included from SGOS 6.7.4.130" on page 100 "Fixes in Advanced Secure Gateway 6.7.3.7" on page 136
B#244784	Packets might exit an incorrect interface in IPv6 configuration when static routes are configured.	"Fixes in Advanced Secure Gateway 6.7.3.1" on page 155
B#253548 SG-4155	Restart occurs due to high volume of IPv6 network traffic.	
B#250616	The appliance might have restarted in Process group: "PG_TCPIP", Process: "stack-bnd-2:0-rxq-0" in "libstack.exe.so". This issue occurred when delayed intercept was enabled.	6.7.2.3 PR
B#250637	The appliance might have restarted in Process group: "PG_TCPIP" in Process: "stack-api-worker-0" in "libmemory.so". This issue occurred when dynamic bypass was enabled.	6.7.2.3 PR
B#255319 SG-6805	The appliance might experience a restart in process "HTTP SW 40047170A40 for 30F29CC2A40" in "libstack.exe.so".	"Fixes in Advanced Secure Gateway 6.7.3.11" on page 122

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#249425 SG-4032	The default gateway cannot be removed unless it is reachable from a configured interface's IP address.	
B#255291 SG-4333	Enabling and disabling EDNS support is not reflected in the event log.	
B#255453	After the appliance is set as Master in a failover configuration, it sends gratuitous ARPs showing a Sender MAC Address containing only zeroes (`00:00:00:00:00:00`). This occurs when both aggregate interfaces and VLAN are configured.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112 "Fixes in Advanced Secure Gateway 6.7.3.6" on page 141
B#252086	The appliance might experience a restart in PG_TCPIP when Virtual IP is configured in failover mode.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#255057	You cannot delete auto-linklocal IPv6 addresses when the interface has link-aggregation set.	"Fixes Included from SGOS 6.7.4.130" on page 100
B#259669 B#256543	The proxy does not fail over when the DNS server fails in a custom DNS group.	"Fixes in Advanced Secure Gateway 6.7.3.7" on page 136

URL Filtering

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#232047 SG-5404	**Issue:** Occasionally the WebPulse service is not able to recover automatically when it gets into a state where all of the services are reporting that they are sick. This results in the following event log message, "Dynamic categorization error: No service specified to use." **Workaround:** Disable and re-enable the WebPulse service.	
B#249253	The WebPulse tab (**Configuration > Threat Protection > WebPulse**) does not display database download status if Intelligence Services is enabled.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255954	**Issue:** Some SSL websites do not load, even if WebPulse is running in background mode. **Workaround:** Perform a drt.rating_servic service health check. In the Management Console (**Configuration > Health Checks > General**), select **drt.rating_service** and click **Perform health check**.	"Fixes Included from SGOS 6.7.4.130" on page 100
B#256515 SG-4437	When the content filtering categorization and Application Classification providers are both disabled, the **Statistics > Category Details** page does not load.	
B#256858	A specific URL takes a long time to load when DRTR is running in the background.	"Fixes Included from SGOS 6.7.4.130" on page 100
B#256952	After downloading an updated content filtering database with changed category names, previous category names are still visible when you view the categories list.	Fixes in 6.7.4.140
B#257351 SG-4536	The `#show system-resource-metrics` CLI output shows empty statistics for custom local databases that are not defined.	
B#257872	During an initial boot of the appliance, a page fault might occur in Process Group "PG_CFS" Process:"Subscription.download_worker" in "liburl_filter.exe.so". Rebooting the appliance usually resolves the issue.	"Fixes Included from SGOS 6.7.4.130" on page 100
B#256160	WebPulse is not categorizing websites in a child/parent configuration when a valid forwarding host is not supplied.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112 "Fixes in Advanced Secure Gateway 6.7.3.7" on page 136
B#259289 SG-4670	When using the **Configuration > Content Filtering > General > Test URL** function, URLs with Unicode characters do not match against local database-defined categories. Matching works with live traffic.	

Visual Policy Manager

ID	Issue Workaround (if available)	Fixed In (when applicable)
B#255321	The appliance sends an `invalid_request` exception error page if you log out of the Management Console and then try to access the consent banner URL again with same browser.	"Fixes in Advanced Secure Gateway 6.7.4.107" on page 112
B#258187	**Service Name** and **Service Group** objects are not visible in the Service column in the Web Request Layer.	"Fixes Included from SGOS 6.7.4.130" on page 100

Advanced Secure Gateway Appliance Resources

This page provides information about supported platforms for this release and where to go for additional hardware information and procedures. Advanced Secure Gateway 6.7.x is not supported on any platform not listed here.

Platforms	Resources	Comments
ASG-S500	https://support.symantec.com/content/unifiedweb/en_US/article.DOC10385.html	PDF version of the Quick Start Guide included in the package for all ASG appliances
ASG-S400	https://support.symantec.com/content/unifiedweb/en_US/article.DOC10136.html	
ASG-S200	https://support.symantec.com/content/unifiedweb/en_US/article.DOC10394.html	

Additional Resources

Subject	Resources	Comments
Diagnostics	http://www.symantec.com/docs/DOC9795	S-Series Maintenance and Upgrade Guide

About Security Certification

Advanced Secure Gateway 6.7.2.102 is designed for FIPS 140-2 validation. The following hardware platforms are FIPS-certified:

- ProxySG: S400-20/30/40 and S500-10/20/30
- Reverse Proxy: S400-20/30/40 and S500-10/20/30
- Advanced Secure Gateway: S400-20/30/40 and S500-10/20

To meet the security requirements of our customers, Symantec maintains Federal Information Processing Standard (FIPS) 140-2 and Common Criteria certifications on Symantec appliances. For more information about the current FIPS and Common Criteria certifications, refer to the *Using FIPS Mode on the ProxySG* document:

http://www.symantec.com/docs/DOC10145

Cryptographic Algorithms in FIPS Mode

In FIPS mode, the appliance can use only the cryptographic algorithms and functions listed below for security relevant and administrative actions (proxy operations are not limited):

- Advanced Encryption Standard (AES) 128-,192- and 256-bit key sizes
- Triple-DES
- Diffie-Hellman: SHA-1, SHA-256
- Rivest Shamir Adleman (RSA):
    - RSA sizes for keys created by the appliance: 2048-bit
    - RSA sizes for keys imported by the appliance: 1024-, 2048-, 3072-, 4096-, 8192-bit
- Secure Hash Algorithm (SHA-1):
    - SHA-1 is used where permitted for protocol and signature verification purposes.
    - SHA-224, SHA-256, SHA-384, SHA-512
- Keyed-Hash Message Authorization Code (HMAC):
    - HMAC with SHA-1
    - HMAC with SHA-2
- Random Number Generation
    - NIST SP 800-90A CTR Deterministic Random Bit Generator
    - ANSI x9.31 Appendix A.2.4 Pseudo Random Number Generator

Updated FIPS Mode Restrictions

- Windows domain configuration for IWA Direct is enabled in FIPS mode.
- Keyrings containing legacy RSA keys of less than 2048-bits may be imported and used.
- In the event a power up self test (software or hardware) fails, the appliance presents options to reboot and retry the self test, and to boot into the last successfully booted release.

Documentation and Other Self-Help Options

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

Product Documentation and Articles

- Search for articles and downloads at MySymantec:

  https://support.symantec.com/

- Refer to MySymantec for product documentation:

  ProxySG: https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145522

  Content Analysis: https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145459

- Access online help from within the Advanced Secure Gateway Management Console; however, note that documentation posted on MySymantec supersedes online help.

Security Advisory Fixes

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

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

Symantec Connect Forums

- Connect with other users at Symantec Connect Forums:

  https://www.symantec.com/connect/

Documentation Changes

Advanced Secure Gateway:

- Starting with this release, Symantec is discontinuing the Advanced Secure Gateway Proxy Administration documentation. For proxy-related information, refer to the equivalent version of SGOS documentation. For content analysis-related information, refer to the appropriate Content Analysis documentation:

For Advanced Secure Gateway version	Refer to Content Analysis documentation version
6.7.2.x	2.1.x
6.7.3.x	2.2.x
6.7.4.x	2.3.x

Provide Feedback

- Send any questions or comments about documentation:

  documentation_inbox@symantec.com

- For Customer Care requests, send email to:

  NP_customercare@symantec.com