

Blue Coat[®] Systems
ProxySG[™]

SGOS 3.2.x Upgrade Guide



Contact Information

Blue Coat Systems Inc.

420 North Mary Ave

Sunnyvale, CA 94085-4121

<http://www.bluecoat.com/support/index.html>

bcs.info@bluecoat.com

support@bluecoat.com

<http://www.bluecoat.com>

For concerns or feedback about the documentation: documentation@bluecoat.com

Copyright© 1999-2006 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxySG™, ProxyAV™, CacheOS™, SGOS™, Spyware Interceptor™, Scope™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, and The Ultimate Internet Sharing Solution® are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT SYSTEMS, INC., ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Number: 231-02672

Document Revision: 3.2.7—02/15/06

Contents

Contact Information

Chapter 1: About Upgrading to SGOS 3.2.x

About This Document	11
About Saved Configurations	11
Upgrade Path	12
Configuration Upgrade or Downgrade	12
Re-Upgrade Commands.....	13
Changing Between SGOS 3.x Versions	14

Chapter 2: Feature-Specific Upgrade Behavior

Chapter Conventions	16
Licensing	16
Management Services	16
Networking	18
Proxy Services	19
Authentication	23
Policy	26
Forwarding	30
Content Filtering.....	32
External Services.....	34
Access Logging	35
Monitoring and Maintenance	36
Content Management	37
System Level and Core Operating System Features	37
Securing the Serial Port	37

Chapter 1: *About Upgrading to SGOS 3.2.x*

This chapter discusses high-level behavior when upgrading the Blue Coat® Systems ProxySG™ operating system to SGOS 3.2.x.

About This Document

Blue Coat strongly recommends that you read this document before attempting to upgrade to SGOS 3.2.x from previous ProxySG operating systems.

SGOS 3.2.x provides substantial new features and existing feature enhancements, plus a new GUI and a more comprehensive Visual Policy Manager (VPM). Existing features and policies might not perform as with previous versions; therefore, upgrading to this version might require some additional configuration tuning. Likewise, as this SGOS version is designed to provide high security for the network, when downgrading to previous versions from SGOS 3.2.x, not all configurations and policies are retained, as they are not compatible with versions not designed to provide the level of security SGOS 3.2.x provides.

This document describes what information is maintained and retained during an upgrade or downgrade of SGOS versions, describes what configurations change or are obsolete after an upgrade, and provides critical high-level and feature-specific information and procedures.

About Saved Configurations

When upgrading to SGOS 3.2.x from a previous major release, the ProxySG saves a copy of the original configurations. These configurations remain unaffected when configuring features going forward. If you downgrade to a previous SGOS version, the saved configuration is used and the ProxySG is restored to that state.

The introduction of the SGOS 3.x operating system combines the previously separate Blue Coat Server Accelerator and Client Accelerator product functionalities. It does not matter which version is running on the appliance when you upgrade to SGOS 3.2.x; the ProxySG retains separate copies for each OS version. However, if you downgrade, only the configurations of the most recent version that was installed on this appliance are applied. For example, if the appliance was running CacheOS CA 4.2 just before upgrading to SGOS 3.2.x, but has also run SGOS 2.1.06, the SGOS 2.1.06 configurations are restored.

Following the upgrade path provided in the next section maintains most of the current settings, the exceptions being those features that have been substantially enhanced in SGOS 3.x.

Upgrade Path

Directly upgrading to SGOS 3.2.4 is only supported with specific CacheOS and SGOS versions. All other versions require one or more upgrades before upgrading to SGOS 3.2.4. The following table provides the upgrade paths.

Table 1.1: Upgrade Paths

Current OS	Direct Upgrade to SGOS 3.2.4?	Next OS version required	Comments
CA 1.0.00-CA3.1.15	No	CA 3.1.16	
CA 3.1.16	No	CA 4.1.10	
CA 3.5.00-CA3.5.07	No	CA 3.5.08	
CA 3.5.08	No	CA 4.1.10	
CA 4.0.00-CA4.1.09	No	CA 4.1.10	
CA 4.1.10 or greater	No	SG 2.1.07	
CA 4.2.00	No	CA 4.2.01	
CA 4.2.1 or greater	Yes	None	Can directly upgrade to SGOS 3.2.4
SA 1.0.00-SA2.0.x	No	SA 2.0.x	
SA 2.0.x	No	SA 4.1.10	
SA 4.0.00-SA4.1.09	No	SA 4.1.10	
SA 4.1.10 or greater	Yes	None	Can directly upgrade to SGOS 3.2.4.
SG 2.0.00-SG 2.1.06	No	SG 2.1.07	
SG 2.1.07 or greater	Yes	None	Can directly upgrade to SGOS 3.2.4.

Beginning in SGOS 3.2.3, you cannot upgrade to a system that is:

- Two or more major revisions higher than the current system. The reason is that if the new system were booted (and downloading it makes it the next boot system by default), you would have skipped a major release version in which policy syntax was deprecated, without seeing any deprecation warnings. Policy would fail to compile and the box would become unusable.
- A major revision higher, if there are deprecation warnings for the current policy.

Configuration Upgrade or Downgrade

After upgrading to SGOS 3.2.4, any changes made to the appliance configuration are saved in the SGOS 3.2.4 copy of the internal configuration registry. If for some reason you reboot the appliance back into an earlier major OS version, such as SGOS 2.x or CacheOS CA/SA 4, the configuration changes that you made under SGOS 3.2.4 are not reflected under the older OS. Instead, the configuration falls back to what was available before you first upgraded to SGOS 3.2.4.

If you upgrade to 3.2.4, make changes to your configuration, and then downgrade, your configuration changes apply to 3.1.x. The exceptions:

- On an upgrade from 3.1.x to 3.2.4, the ProxySG will send patience-text messages with progress information (instead of a hardcoded message with no progress information). On a downgrade to 3.1.x, the ProxySG sends hardcoded patience-text message with no progress information.
- Any new policy language constructs added in 3.2.4 that are not supported in 3.1.x will result in a policy compilation error on downgrade. Remove these new elements before downgrading from 3.2.4 to 3.1.x.
- If you select SmartFilter v4 in 3.2.4 and then downgrade, you will have a v4 database and be unable to load it under 3.1.x (since 3.1.x only understands SmartFilter v3). You must download a new database. Until you do (or until the next auto-download), you will get content-filter-unavailable.
- Any changes to the services configuration (additions, deletions, modifications) done in 3.2.4 will not be available on a downgrade to 3.1.x. The 3.1.x settings will be unchanged from the original upgrade.
- Force-NTLM support in VPM on downgrade: In the actions in VPM where the force NTLM object was used, the rule shows up as a normal authentication object.
- If you downgrade when you have a Netegrity SiteMinder realm defined, the Management Console reports an error, and you will be unable to edit realms with the Management Console. You can still edit realms with the CLI, but you cannot remove Netegrity realms in SGOS 3.1.3 or earlier. The best practice is to remove any Netegrity realms prior to downgrading.
- A new Telnet service was introduced as part of the Shell proxy. If you downgrade to 3.1.x, this service will show up as "unknown." You cannot delete this service in 3.1.x. You must delete the service before downgrading.
- If you enable encrypted access logs and downgrade from 3.2.4 to 3.1.x (where $x \leq 4$), you will see a registry warning printed on the console. This does not affect normal operation.

Re-Upgrade Commands

Two CLI commands (from the `enable` prompt) can be used to force the upgrade process to occur again:

- `restore-cacheos4-config`—Verifies if a saved CA or SA 4.2 configuration exists on the ProxySG. If one does not exist, the administrator receives a message and exits the command. If a configuration exists, the SGOS 3.x configuration is cleared, as well as any SGOS 2.x configurations, and a reboot occurs. The reboot triggers the upgrade process, and the CA or SA 4.2 configurations are converted to SGOS 3.x.
- `restore-sgos2-config`—Verifies if a saved SGOS 2.x configuration exists on the ProxySG. If one does not exist, the administrator receives a message and exits the command. If a configuration exists, the SGOS 3.x configuration is cleared, and a reboot occurs. The reboot triggers the upgrade process, and the SGOS 2.x configurations are converted to SGOS 3.x.

Invoking these commands is useful for the following scenarios:

- When the initial SGOS 3.x upgrade occurs, any compatible configurations are converted. This only happens once; therefore, if you downgrade to a pre-SGOS 3.x version, perform configuration

changes, and re-install SGOS 3.x, those changes are not propagated. These commands force an upgrade that includes the new changes.

- Because the SGOS 3.x configurations are converted from the latest version of SGOS installed on the ProxySG, the `restore-cacheos4-config` command can be used to force an upgrade based on the existing CA or SA 4.2 version if an SGOS 2.x version exists on the ProxySG.

Changing Between SGOS 3.x Versions

When upgrading or downgrading between versions of SGOS 3.x, copies of version-specific configurations are not retained. Instead, all configurations created in an upgrade are retained if the configuration is relevant to the downgrade version.

Chapter 2: *Feature-Specific Upgrade Behavior*

This chapter provides critical information concerning how specific features are affected by upgrading to SGOS 3.x (and, if relevant, downgrading from) and provides actions administrators must or are recommended to take as a result of upgrading.

This chapter contains the following sections:

- "Chapter Conventions"—Describes the method this chapter uses to describe each feature.
- "Licensing"—Discusses the new global licensing scheme.
- "Management Services"—Discusses the Management Console, Telnet console, SSH console, and serial console.
- "Networking"—Discusses interfaces and adapters.
- "Proxy Services"—Discusses HTTP, SSL, FTP, Windows Media, Real Media, and QuickTime proxies.
- "Authentication"—Discusses realms and each authentication protocol.
- "Policy"—Discusses the behavior of the enhanced Content Policy Language, the Visual Policy Manager, and policy files upon upgrading.
- "Forwarding"—Discusses forwarding host issues.
- "Content Filtering"—Discusses the behavior of on-box content filtering configurations and third-party vendor issues.
- "External Services"—Discusses the behavior of ICAP and Websense4 off-box.
- "Access Logging"—Discusses the new access logging facilities.
- "Monitoring and Maintenance"—Discusses SNMP and Heartbeats.
- "Content Management"—Discusses a CLI change.
- "System Level and Core Operating System Features"—Discusses the merge of client accelerator and server accelerator features and system resources.
- "Securing the Serial Port"—Discusses upgrade behavior of new functionality designed to protect the serial and setup consoles.

Chapter Conventions

In discussing how upgrading or downgrading affects specific features, each feature contains up to four categories:

- **Upgrade Behavior**—describes upgrade behavior regardless of upgrade path and specific version information as necessary. This section might also provide brief functionality of new or enhanced features.
- **Administrator Actions**—provides steps you can take before and after an upgrade to assure a smooth transition.
- **CLI Compatibility Issues**—describes changed, additional, or deleted CLI commands.
- **Documentation Reference**—provides references to other relevant topics in the *Blue Coat ProxySG Configuration and Management Guide* or where otherwise noted.

Licensing

The method the ProxySG applies licenses for features has been redesigned to a global SGOS 3.x licensing scheme that does not use the Product Authorization Key (PAK) as in previous versions. In SGOS 3.x, all licensable features can be configured without a license; however, all activity relating to those features is denied until a valid license is entered.

Upgrade Behavior—All Upgrade Paths

- The PAKs are not converted to new licensing keys.
- Blue Coat provides a grace period of 60 days during which all licensable features are enabled.

Administrator Actions

The Blue Coat Web pages provides instructions for obtaining new product licenses.

CLI Compatibility Issues

The former licensing commands under the `streaming windows-media` and `streaming real-media` do not exist. New commands `set` and `show` global licenses for features.

Documentation References

Chapter 2: “Licensing”

Management Services

This section discusses the Management Console, Telnet console, SSH console, and serial console.

Management Console

The Management Console features a new skin, rearranged menu items, and new menu items relating to new features.

Upgrade Behavior—All Upgrade Paths

- In SGOS 3.x, the default listening port on all interfaces is 8082 (secure HTTPS-Console), which is automatically created if not used before the upgrade. It uses a keyring with a default self-signed certificate. Also, a non-secure Management Console listening port, 8081, is created and enabled if a non-secure Management Console existed before the upgrade; otherwise, it is created but disabled.
- Before SGOS 3.x, only one HTTP or HTTPS console could be configured at any given time. SGOS 3.x features a new services configuration option. Upon upgrade, a new service is created based on the pre-upgrade Management Console type (HTTP or HTTPS) and the port number.
- If the Management Console was configured as a secure service before the upgrade, the corresponding console map and all attributes (such as keyring and protocol version) are upgraded to a new service. The new service is enabled or disabled dependent on whether Web management was enabled or disabled.

Upgrade Behavior—CA 4.2 and SA 4.1

Passwords configured for archive configuration, access log upload, and LDAP backend are lost. You must redefine these passwords on the ProxySG.

CLI Compatibility Issues

Removed commands

- The commands to configure the Management Console.
- The `(config) https console-map` commands.

New commands

- The `(config services) http-console` and `(config services) https-console` commands are used to configure the Management Console.
- The Management Console HTTPS keyring is configured with the `(config services) https-console` command.
- Two new software restoration commands have been added:
 - ❑ `restore-cacheos4-config`—restores the ProxySG to the most recent version of CacheOS.
 - ❑ `restore-sgos-config`—restores the ProxySG to the most recent version of SGOS 2.x.

Documentation References

Chapter 5: “Managing Port Services”

Telnet Console

Upgrade Behavior—All Upgrade Paths

- Existing Telnet services are maintained on the same port upon upgrading.
- If a Telnet service was not configured before the upgrade, a new one is created on port 23, but is disabled.

CLI Compatibility Issues

None.

Documentation References

Chapter 5: “Managing Port Services”

SSH Console

The SSH Console replaces Telnet as the default remote access method.

Upgrade Behavior—All Upgrade Paths

- SSH v2 is automatically enabled with an automatically generated SSH v2 host key.
- SSH v1 is enabled only if the previous SSH configuration was enabled.
- SSH v1 host keys and RSA client keys are copied.

CLI Compatibility Issues

- The SSH CLI commands are now located in the `(config services) ssh-console` submode (previously existed in `sshd` submode).

Setup Console

CLI Compatibility Issues

The setup console now allows you to create a software bridge using available Ethernet ports.

Documentation References

Chapter 4: “Configuring the System”—“About Bridging”

Networking

This section discusses the Pass-Through Card and interfaces.

Upgrade Behavior—All Upgrade Paths

The network interface number scheme has changed to accommodate multi-interface adapters for bridging functionality. The new numbering scheme is $n:m$, where n is the adapter number and m is the interface number on the adapter. The upgrade to SGOS 3.x automatically updates the old format to the new.

Administrator Actions

None.

CLI Compatibility Issues

The interface CLI commands now accept the `n:m` convention; however, if only a single value is entered, SGOS 3.x by default assumes you are providing an adapter number and the interface is 0.

Documentation References

Chapter 4: “Configuring the System”

Proxy Services

This section discusses HTTP, SSL, FTP, Windows Media, Real Media, and QuickTime proxies.

HTTP

As ProxySG functionality combines the features of the previous Server Accelerator and Client Accelerator OS versions, SGOS 3.x contains a profile feature that allows you to select a default Blue Coat HTTP option configuration set for forward proxy (the former CA deployment), reverse proxy (the former SA deployment), and bandwidth gain deployments. These default option configurations are not derived from previous OS settings. For more information about these default configurations, refer to Chapter 6, Configuring Proxies, in the *Blue Coat ProxySG Configuration and Management Guide*.

Upgrade Behavior—All Upgrade Paths

- Caching Authenticated Data (CAD) is now enabled by default.
- In pre-SGOS 3.x versions, HTTP services with NAP and explicit attributes suppressed access logging and caching. In SGOS 3.x, NAP was dropped.
- In SGOS 3.x, the default maximum cacheable size increases from 50MB to 1024MB. During the upgrade to SGOS 3.x, if the value is defined as 50MB, it is changed to 1024MB.
- A new HTTP or TCP-Tunnel service is created. This replaces the HTTP services (NAP) attribute. The type of service created depends on the combination of attributes, as defined in the following table.

Table 2.2: HTTP Attributes

Pre-SGOS 3.x Attributes	SGOS 3.x HTTP or TCP-Tunnel Service
HTTP service: NAP, explicit	HTTP service: explicit
HTTP service: NAP, transparent	TCP-Tunnel service: transparent
HTTP service: NAP, explicit, transparent	HTTP service: explicit, transparent

Administrator Actions

- If you previously had HTTP services with NAP and explicit attributes, you must add a CPL policy rule to continue to suppress access logging and caching (if such behavior is required).
- If you plan to run SGOS 3.x on a series 7xx or 7xxx platform and plan to deploy the appliance as both a forward and reverse caching proxy, Blue Coat recommends thoroughly understanding the new profile feature.

CLI Compatibility Issues

The `nap` attribute no longer exists in the `services http` mode.

Documentation References

- Chapter 6: “Configuring Proxies”
- *The Blue Coat Content Policy Language Reference*.

SSL

Upgrade Behavior—All Upgrade Paths

- Console maps are not used in SGOS 3.x. Equivalent attributes must now be configured as an HTTPS-Console service.
- Server maps and client maps are not used in SGOS 3.x.
- The upstream server certificate is verified by default. In previous versions, the upstream certificate was ignored unless explicitly configured to verify.
- Previously, an explicitly-proxied HTTP connection to a secure server registered in the Access Log as `https://www.site.com`. In SGOS 3.x, such transactions are registered as `tcp://www.site.com`.

Upgrade Behavior—CacheOS SA 4.1 Upgrade Path

- HTTPS server maps are converted to HTTPS services. A new HTTPS service is created on the same port as the previous version.
- Upon upgrading from CacheOS SA 4.1 to SGOS 3.1.0, server maps on non-local IP addresses are *not* converted to HTTPS services.
- Upon upgrading from CacheOS SA 4.1 to SGOS 3.1.1, server maps on non-local IP addresses are converted to HTTPS services and function just as in CacheOS SA 4.1.
- If you upgrade from CacheOS SA 4.1 to SGOS 3.1.0, and then from SGOS 3.1.0 to SGOS 3.1.1, server maps on non-local addresses are not available to be converted.
- HTTPS tunnel maps are converted to TCP-Tunnel services. A new TCP-Tunnel service is created on the same port as the previous version.
- In SGOS 3.1.x, the `ssl-verify-server` option is enabled by default, which can cause upstream HTTPS connections to fail.

Administrator Actions

- If upgrading from a CacheOS SA 4.1 path, disable the `http ssl-verify-server` option if the upstream server does not present a proper certificate to preserve HTTPS server connection integrity.

Alternately, perform the following:

- Verify that the certificate of the certificate authority that signed the upstream server certificate is imported on the ProxySG.

- Verify that the common name in the upstream server certificate matches the hostname of the upstream server.
- If you have policy rules for matching transactions and changing `https://www.site.com` log entries, you must rewrite these rules to adhere to the new format: `tcp://www.site.com`.

CLI Compatibility Issues

- The `https` command sub-mode is now the `ssl` sub-mode.
- The `https client-map` attribute is replaced by `(config) ssl client {create | edit | delete}`.
- Under `services`, `https` and `tcp-tunnel` are new.
- The `services https-console` commands replace the `https console-map` commands.
- The `services https` commands replace the `https server-map` commands.
- The `verify-https` attribute for a forwarding host is now `ssl-verify-server`.
- A new option, `http ssl-verify-server`, enables SSL certificate verification of an upstream server. The option is enabled by default.

Documentation References

- Chapter 5: “Managing Port Services”
- Chapter 6: “Configuring Proxies”

FTP

Upgrade Behavior—All Upgrade Paths

- Native explicit FTP proxy is a new feature. Upon upgrading, all previous FTP proxy services are configured as explicit and transparent.
- The global maximum cacheable size encompasses both FTP and HTTP; you cannot specify the maximum cacheable size for just FTP.

Documentation References

Chapter 6: “Configuring Proxies”—“Configuring the FTP Proxy”

Windows Media

Upgrade Behavior—All Upgrade Paths

- Previously, the ProxySG was limited to one transparent MMS listener on port 1755 and one explicit listener on a user-specified port. SGOS 3.x supports multiple listeners, which are configured through the services GUI component or CLI commands. Upon upgrading, the transparent and explicit listeners are converted to new MMS services, each with its respective attribute.

- If the pre-upgrade explicit listener resided on port 1755 (which is transparent), an MMS service is created on this port with the explicit attribute, and transparent is also enabled if it was previously enabled.
- Windows Media proxy routing rules are now processed through the Forwarding feature. Upon upgrading, the proxy routing rules are converted to forwarding host configurations and appropriate CPL forwarding rules that are written to the CPL forward policy file.
- The PAK licensing scheme has been replaced with a global license scheme. See "Licensing" on page 16 for more information.

CLI Compatibility Issues

- The commands associated with creating a service that were under `streaming windows-media` are now under `(config) services mms`.
- The `license pak` option in the `(config) streaming windows-media` command are removed.
- The `proxy-route` option in the `(config) streaming windows-media` command are removed.
- The ability to manage Windows Media access logging with CLI commands has been replaced with an enhanced Access Logging feature on the ProxySG.

Documentation References

- Chapter 19: "Access Logging"
- Chapter 18: "Configuring the Upstream Networking Environment"
- Chapter 2: "Licensing"
- Chapter 15: "Streaming Media"

Real Media and QuickTime

Rather than porting RealProxy software as in previous versions, SGOS 3.x features a native RTSP proxy that supports Real Media and QuickTime traffic. This provides the following differences:

- The RTSP proxy only caches and splits Real Media content types `rm`, `rv`, and `ra`.
- Caching is accomplished with the RTSP and RDT protocols; the proprietary MEI-MII protocol to talk to the origin RealServer is no longer used.
- Splitting is accomplished with the RTSP and RDT protocols; the proprietary splitter protocol is not used to talk to the origin RealServer.
- QuickTime content is not cached or split, but supported in pass-through mode.

Upgrade Behavior—All Upgrade Paths

- As the native RTSP proxy differs vastly from the ported RealProxy software, *no configurations are converted upon upgrading to SGOS 3.x*.
- Because the RTSP proxy is now native to the ProxySG, all supported access log formats can be logged; however, the previous RealNetworks proprietary access log formats are not supported.
- The PAK licensing scheme has been replaced with a global license scheme. See "Licensing" on page 16 for more information.

Administrator Actions

- Blue Coat recommends documenting the RealProxy configurations (use the Management Console or CLI to view the existing services) before performing the upgrade. After upgrading to SGOS 3.x, you can then easily create the new services.
- In previous versions, the RealProxy by default listened on port 554 for transparent and explicit connections, and could be specified to listen on another port (commonly 1091) for explicit connections. Upon upgrading, a new RTSP service on port 554 is created but disabled. To maintain this, enable this service and, optionally, create an explicit service on port 1091.
- Proxy routing rules are not converted to forwarding host configurations or CPL forwarding rules. After upgrading to SGOS 3.x, you must configure new forwarding rules.

CLI Compatibility Issues

- The `streaming real-media` commands now resemble the `windows-media` commands.
- QuickTime streaming is configured through the new `streaming quicktime` commands.

Documentation References

- Chapter 2: “Licensing”
- Chapter 5: “Managing Port Services”
- Chapter 15: “Streaming Media”

Authentication

Realms

Upgrade Behavior—All Upgrade Paths

Two CPL attributes have been added to all authentication realm types:

- Virtual URL—Provides the ability to specify a virtual URL to redirect per realm.
- Display name—Specifies the string to display in the authentication challenge.

CLI Compatibility Issues

The following command:

```
(config realm_type realm_name) {spooof-authentication | no spooof-authentication}
```

is replaced with:

```
(config realm_type realm_name) spooof-authentication {enable | disable}
```

The `realm_type` applies to BASIC types (LDAP, RADIUS, and Local).

Documentation References

Chapter 9: “Using Authentication Services”

LDAP

Upgrade Behavior—All Upgrade Paths

- LDAP v.3 features the following new options:
 - Protocol version—The ability to specify the LDAP version, 2 or 3. The default is 2.
 - Referrals—Allows referrals returned from the LDAP server to be followed. The default is disabled.
 - SSL—Provides SSL support. The default is disabled.
- LDAP realms now features the ability to specify the level of dereference. In SGOS 2.x, this value was hardcoded to `ALWAYS`; upon upgrading, the value defaults to `ALWAYS`. In CacheOS 4.x, this value was hardcoded to `NEVER`; upon upgrading; the value defaults to `NEVER`.
- To support VPM browsing, LDAP realms now feature the ability to specify the objectclass values to use when searching for containers, groups and users during a VPM LDAP browse session. The default objectclass values for a particular LDAP realm depend on the server type of the LDAP realm. The ability to specify a server type was introduced in SGOS 2.x; upon upgrading, the objectclass values for the specified server type are added to the LDAP realm. If upgrading from CacheOS 4.x, the server type defaults to `OTHER`, and the objectclass values for type `OTHER` are added to the LDAP realm.

CLI Compatibility Issues

- The `security ldap all` command has been removed.
- The previous `distinguished-name` command and its sub-commands have been replaced with:

```
(config ldap realm) distinguished-name base-dn {add | remove | promote | demote | clear} base-dn
```

Documentation References

Chapter 9: “Using Authentication Services”

NTLM

Upgrade Behavior—All Upgrade Paths

SGOS 3.x provides:

- SSL support for CAASNT. For a new NTLM realm and any existing realm upon upgrading, the default is disabled.
- The ability to disable support for BASIC or NTLM credentials in an NTLM realm. For a new NTLM and any existing realm upon upgrading, both types are supported.
- CAASNT version compatibility with previous SGOS releases. Note that previous versions are not compatible with SGOS 3.x.

SGOS 3.2.x provides:

- A new authentication agent called Blue Coat Authentication and Authorization Agent (BCAAA) service that replaces CAASNT.

Administrator Actions

- SGOS 3.1.x: The new CAASNT version must be installed. If SSL support is required, CAASNT must be installed on Windows 2000, as Windows NT v4 is not supported.
- SGOS 3.2.x and higher: You must use the 3.2 release of the BCAA service with SGOS 3.2 and higher. You can also use the BCAA service in place of the deprecated CAASNT application for SGOS 2.x and SGOS 3.1.x. You cannot use CAASNT with SGOS 3.2 and higher.

CLI Compatibility Issues

- The `security ntlm all` command has been removed.
- The `(config ntlm realm) server-retry` command has been removed; the server retry count is not used in SGOS 3.x.

Documentation References

- Appendix A: “Using the Authentication/Authorization Agent”
- Chapter 9: “Using Authentication Services”

Local Realm

Upgrade Behavior—All Upgrade Paths

- The SGOS 2.x UNIX realms are renamed to Local realms.
- A Local realm references the Local User List for authentication and authorization. Upon upgrading, the list associated with an existing Local realm is the default list.

CLI Compatibility Issues

- The `security unix` sub-command is replaced by `security local`.

Documentation References

Chapter 9: “Using Authentication Services”

Local User Lists

Upgrade Behavior—All Upgrade Paths

- SGOS 3.x allows you to create, edit, view, and delete local users.
- A default local user list is created upon upgrading. A UNIX realm converted to a Local User realm is configured to use the default local user list.

CLI Compatibility Issues

- The `local-user-list` command manages the local user list.
- The `set_auth.pl` script for loading users onto the ProxySG is still valid.

Documentation References

Chapter 9: “Using Authentication Services”

General Authentication

Upgrade Behavior—CacheOS CA 4.2 Upgrade Path

If console credentials are null, upon upgrade they default to `admin, admin`.

CLI Compatibility Issues

- The following command:

```
security {allowed-access | no allowed-access} ip_address [mask]
```

is replaced with:

```
security allowed-access {add | remove} ip_address [mask]
```
- The following command:

```
security {enforce-acl | no enforce-acl}
```

is replaced with:

```
security enforce-acl {enable | disable}
```

Documentation References

Chapter 9: “Using Authentication Services”

Policy

Two new properties and service objects have been added for 3.2.4:

- `icap_error_code` (used with ICAP in VPM)
- `virus_detected` (used with ICAP in VPM)

CPL

SGSOS 3.x features new CPL forwarding policy file for forwarding rules.

Upgrade Behavior—SGOS 2.1.x Upgrade Path

- Forwarding and MMS proxy routing files are converted to CPL and copied to the forward policy file.
- The central policy and central bypass list paths changed from:

`http://www.bluecoat.com/support/subscriptions/CentralPolicy.txt`
`http://www.bluecoat.com/support/subscriptions/CentralBypassList.txt`

to:

`https://www.bluecoat.com/support/subscriptions/CentralPolicy.txt`
`https://www.bluecoat.com/support/subscriptions/CentralBypassList.txt`

However, the default upon upgrade remains `http://`; you must manually change the paths.

Upgrade Behavior—CacheOS CA 4.2 Upgrade Path

- Forwarding and MMS proxy routing files are converted to CPL and copied to a new forward policy file. Also, the path for the default central policy file is updated to `https://`.
- The filter and central policy files are copied to the SGOS 3.x local and central files, respectively. These copied files run in CPL backward-compatibility mode, which causes syntax deprecation warnings to be generated by the CPL compiler. These files must be converted to current CPL syntax before upgrading to the next major release of ProxySG. The *Blue Coat Content Policy Language Guide* contains an appendix that discusses upgrading from CacheOS in more detail.
- CPL and XML files are created that are explicitly used by the Visual Policy Manager. Pre-upgrade configurations are translated into policy and inserted in both files.
- MMS and Real Media host alias rules are converted to CPL rewrite rules and inserted into the VPM policy file.
- If a requirement for administrators to log in existed, a default `admin` authentication challenge policy is installed to the appropriate realm. If the enable console ACL was configured, it is installed as a subnet restriction.
- If a requirement for users to log in existed, a user authentication challenge policy is installed to the appropriate realm.
- The default path for downloading the central policy file (filter file to policy file) is updated if it was set to the default.

Upgrade Behavior—CacheOS SA 4.1 Upgrade Path

- Forwarding and MMS proxy routing files are converted to CPL and copied to the forward policy file. Also, the path for the default central policy file is updated to `https://`.
- The filter file is copied to the SGOS 3.x local file. This copied file runs in CPL backward-compatibility mode, which causes syntax deprecation warnings to be generated by the CPL compiler. This file must be converted to current CPL syntax before upgrading to the next major release of ProxySG. The *Blue Coat Content Policy Language Guide* contains an appendix that discusses upgrading from CacheOS in more detail.
- The path to the central policy file is created.
- CPL and XML files are created that are explicitly used by the Visual Policy Manager. Pre-upgrade configurations are translated into policy and inserted in both files
- MMS and Real Media host alias rules are converted to CPL rewrite rules and inserted into the VPM policy file.

- If a requirement for administrators to log in existed, a default *admin* authentication challenge policy is installed to the appropriate realm. If the enable console ACL was configured, it is installed as a subnet restriction.
- If a requirement for users to log in existed, a user authentication challenge policy is installed to the appropriate realm.
- While the SGOS 3.x CPL allows policy control of the features available in previous Server Accelerators, they are not automatically added to existing policy. Rather, the HTTP acceleration profile is set to *portal* mode.

Administrator Actions

Upon upgrading and installing new policy, Blue Coat strongly recommends reviewing the policy compilation for CPL deprecation warnings. CPL syntax deprecations must be resolved before upgrading to any post-SGOS (not including 3.x.x release) future releases because these syntaxes will be obsolete.

CLI Compatibility Issues

None.

Documentation References

- Chapter 9: “Using Authentication Services”
- The *Blue Coat Content Policy Language Reference*

VPM

Upgrade Behavior—SGOS 2.1.x Upgrade Path

- The first time the SGOS 3.x version of the VPM is launched, the VPM XML and CPL files are updated to support the new functionality.
- The following VPM objects are rewritten (as required) as Combined Objects, with no impact to functionality:
 - ❑ URL lists
 - ❑ IP Address lists
 - ❑ Source Objects
 - ❑ Destination Objects
 - ❑ Time lists
 - ❑ Protocol lists
- Block Categories are rewritten as content filtering *exceptions* and use the Deny option.
- The following objects have changed or moved to a new column:
 - ❑ User Agent has moved from the Service column to the Source column.
 - ❑ Override Authentication and Override Content Filter have been removed.

- ❑ The Time column has been repositioned to before the Action column.
- ❑ Proxy IP Port has moved from the Destination column to the Source column.
- ❑ The Destination column has been removed from the Administration Authentication policy layer.

Administrator Actions

After upgrading to SGOS 3.x, start the current version of VPM and re-install the policy. This refreshes the stored policy files. Until this is performed, the VPM policy remains in the SGOS 2.x format.

Documentation References

Chapter 13: “The Visual Policy Manager”

Exception Pages

Exception pages replace the Error Pages (Response Message Generator) in CacheOS CA 4.2/SA 4.1 and SGOS 2.1.x.

Upgrade Behavior—All Upgrade Paths

Exception pages are new for SGOS 3.x, and the previous Error Pages are ignored upon upgrading.

Administrator Actions

This section provides two methods to configure Exception Pages. Review the options and use the method that best fits your requirements. Also, refer to the *Blue Coat Systems ProxySG Configuration and Management Guide* for detailed information and Exception Page editing tips.

Method 1

Use the `(config) exceptions` CLI command and sub-commands to create and customize Exception Pages. Refer to the *Blue Coat Systems ProxySG CLI Reference* for detailed information about this command.

Method 2

Upgrade the former Error Pages. Perform the following steps:

1. To provide a reference of the previous Error Pages, access them with the following URL:

```
https://Pre-SGOS3.x_IP_address:console_port/error_pages.txt
```

Note: This URL remains valid upon upgrading from SGOS 2.x or CacheOS, but is for reference only. It cannot be edited, nor is it used in any configuration.

2. Access the default Exceptions stored in the Installable List:

```
https://Updated_ProxySG_IP_address:console_port/exceptions/default.txt
```

3. Customize the default Installable List based on the previous Error Pages.
4. Install the new list.

CLI Compatibility Issues

The following Error Pages commands:

```
inline error-pages
load error-pages
error-pages path
```

are replaced with:

```
inline exceptions
load exceptions
(config) exceptions
```

Documentation References

Chapter 14: “Advanced Policy”—“Defining Exceptions”

Forwarding

Upgrade Behavior—All Upgrade Paths

In SGOS 3.x, default and backup hosts are replaced with a *default sequence*, or forwarding host list. Upon upgrading, a system that had defined default and backup hosts now has a default sequence of the default host followed by the backup host. If only a default *or* a backup host was defined, that host becomes the default host. If neither were defined, the sequence remains empty. After the upgrade is complete, you can use the CLI to add or remove hosts from the sequence and promote or demote existing hosts in the sequence.

During the upgrade, all existing forwarding rules are rewritten to include the keyword `default` to preserve the previous behavior of attempting to contact a particular host, using the default and backup hosts as fallbacks.

Upgrade Behavior—SGOS 2.1 Upgrade Path

- SGOS 3.x introduces a new forwarding policy file for forwarding-related rules. This new file is generated during the upgrade and contains CPL translations from previous policy.
 - ❑ The forwarding policy file always follows the local policy file in the file order.
 - ❑ If the `restore-defaults` CLI command is invoked, the forwarding policy file is emptied.
 - ❑ Blue Coat recommends not inserting forwarding policy in other files.
- SGOS 3.x introduces a new CPL `<forward>` policy layer type.
 - ❑ Created during the upgrade, the new forwarding policy file for forwarding rules contains only `<forward>` layers.
 - ❑ Time-based triggers are allowed in a `<forward>` layer.
 - ❑ The `trace_rules()` and `trace_request()` are allowed in a `<forward>` layer.
 - ❑ Notification actions are available from a `<forward>` layer.
 - ❑ Policy in `<forward>` layers can be executed by both proxy and cache transactions.

- Forwarding and MMS proxy route configurations are converted into forwarding hosts and groups and SOCKS gateways under a `<forward>` layer in the forwarding policy file.
- During the upgrade, regular expression-based forwarding rule URLs are converted using `server_url.regex` triggers, not `server_url.host.regex` triggers (does not apply to MMS proxy routing rules).
- Performing a re-upgrade (for example, invoking the `restore-sgos2-config` command) overwrites the forwarding file with fresh upgrade information and replaces the Forwarding and SOCKS gateway configurations.
- Upon upgrade from SGOS 2.x to SGOS 3.x, all of the forwarding host configuration is migrated. In addition, a forwarding policy and a default forwarding sequence is created. In order to delete any or all of the hosts in the configuration, the forwarding policy and the default forwarding sequence must first be cleared. Otherwise an error is displayed, stating that the host is referenced by policy.

Upgrade Behavior—CacheOS CA 4.2 Upgrade Path

The upgrade occurs in two stages. First, the relevant Forwarding configurations are filtered out of the ICP configuration file and copied to the SGOS 2.1 forwarding configuration file. All rules are translated into a `hostname:port` format. If applicable, the direct/deny list is also copied into the forwarding configuration file. The upgrade then follows the SGOS 2.1 path as described above.

Upgrade Behavior—CacheOS SA 4.1 Upgrade Path

- The upgrade occurs in two stages. First, the relevant Forwarding configurations are filtered out of the advanced forwarding configuration file and copied to the SGOS 2.1 forwarding configuration file, filtering out obsolete entries. The upgrade then follows the SGOS 2.1 path as described above.
- HTTP requests sent to a forwarding server that has no HTTP port but does have an HTTPS port are *coerced* to be an HTTPS request; the same occurs in reverse.

Administrator Actions

- Two-way URL rewrite rules in the policy might require modification. If URL rewrite rules exist that convert `https://` original URLs to `http://` server URLs, you must also have rules to rewrite embedded links in the response of the form `http://` to `https://` to complete the conversion of a non-secure site to a secure site.
- Examine forwarding hosts, SOCKS gateways, and the policy files. While the upgrade conversions are automatic, they involve complex transformations. If necessary, restructure forwarding policies from machine-generated strings to easily identifiable aliases.
- Blue Coat recommends using the VPM to manage the forwarding rules and immediately moving forwarding rules from the forward CPL file to the VPM.
- SGOS 3.x allows you to uniformly apply forwarding rules to all supported protocols. Consider this when examining and fine-tuning the forwarding policy.
- Some unexpected upgrade behavior can occur. For example, with CacheOS SA 4.1, you can define an HTTPS port on an upstream host of type *proxy*. This is not allowed in SGOS 3.x; the type is converted to type *server* (but it is logged in the Event Log). Again, reviewing all upgraded configurations is recommended to discover such conversions.

CLI Compatibility Issues

- As a result of merging Client Accelerator and Server Accelerator functionality into one OS, the forwarding sub-commands now include `host-affinity`, `load-balancing`, and `failure-mode`.
- Forwarding and SOCKS gateway health checks are now configured with the `health-check` command and sub-commands. A health check service can be created for a specific forwarding host, or the ProxySG can be configured to perform global health checks.

Documentation References

- Chapter 18: “Configuring the Upstream Networking Environment”
- Chapter 12: “Managing Policy Files”
- Chapter 13: “The Visual Policy Manager”
- The *Blue Coat Content Policy Language Reference*

Content Filtering

Content filtering functionality is categorized as *on-box* services, or services the ProxySG performs itself using third-party resources, and as *off-box* services, where the ProxySG forwards requests to and receives responses from other third-party servers that perform content scanning and filtering tasks. On-box services are provided with features labeled as Content Filtering, and off-box services are configured as External Services. This section refers to on-box services; see “External Services” on page 34 for more content filtering information.

Note: Consider this new organization of content filtering functionality on the ProxySG when resolving policy deprecation errors; policy once configured under Content Filtering might now be configured under External Services.

Websense3 off-box is no longer supported; Websense4 off-box is supported, but resides in External Services. SurfControl is now supported.

Upgrade Behavior—SGOS 3.1 Upgrade Path

The Websense log protocol changed from version 1 to version 3 in SGOS 3.2.x.

Upgrade Behavior—SGOS 2.1 Upgrade Path

- SmartFilter—Since the release of SGOS 2.x, SmartFilter has modified some category names. SGOS 3.x uses names that are approved by SmartFilter.
- Websense (v4 and v5)—Websense v3 featured 29 categories with defined names. In SGOS 3.x, Websense supports nearly 100 categories and the category names are specified in the database. These names change frequently. Upon upgrading, substantial category renaming occurs.
- Use of obsolete category names can still exist in policies, but a deprecation warning is displayed. Failure to resolve these category names can result in the blocking of future SGOS versions upgrades.
- As a ProxySG can only use one content filter vendor, only the obsolete names for the vendor configured at the time of the upgrade are retained.

Upgrade Behavior—CacheOS CA 4.2 Upgrade Path

The content filtering configuration is not preserved or translated to current CPL. Upon upgrading, Content Filtering is configured with defaults defined by a newly-manufactured appliance.

Administrator Actions

- Once SGOS 3.x is installed, you *must* re-download the content filtering database from each vendor you have a contract with. At a minimum, configure the automatic filter download feature to do so as soon as possible.
- Update the relevant policy file to resolve obsolete category names. Consider that the Visual Policy Manager automatically updates the policy file with current names at the next policy installation.

Applies to CacheOS CA 4.2 Deployments Only:

The following procedure assumes that you want to reapply a very similar policy as before.

1. Before upgrading, record the content filter vendor configuration and the list of all blocked categories. For example: SmartFilter; downloaded from default location; username is foo, password is bar; auto-download occurs every day at 2 am UTC; blocked categories: Sex, Sports, and Gambling.
2. After the upgrade, select Content Filtering>Automatic Download; configure the time.
3. Select Content Filtering>SmartFilter; enter the password; click Download now.

Note: The download URL is the default SmartFilter URL that applies to the version used by SGOS 3.x, not any previous versions.

4. Edit the local policy file. For example:

```
<cache>
  Category=(Sex, Sports, Gambling) exception(content_filter_denied)
```

5. View the compiled policy and resolve any obsolete category names.

CLI Compatibility Issues

- As mentioned before, the Content Filtering features were split into two main sections. The CLI commands reflect this change. The `content-filter` command and sub-commands related to the features discussed in this section.
- Selecting a provider is immediate and does not require a reboot.
- Previously, the `disable` option halted a vendor; now the vendor is set to `none`.
- A vendor configuration can be completely configured before selecting it. Blue Coat recommends this action so the transition between vendors is seamless.

Documentation References

- Chapter 17: “Content Filtering”
- Chapter 10: “External Services”
- Chapter 12: “Managing Policy Files”

- Chapter 13: “The Visual Policy Manager”

External Services

As discussed in “Content Filtering”, all off-box content filtering services are labeled as External Services. This includes ICAP and Websense v4.

ICAP

Upgrade Behavior—SGOS 2.1 Upgrade Path

- Clusters are now called *service groups*.
- All previously configured ICAP services and clusters are migrated.
- Upon upgrading, ICAP v0.95 services become inactive.

Administrator Actions

Create new ICAP v1.0 services to replace the obsolete services. If you only have ICAP v0.95 servers, you must upgrade to v1.0 servers.

Note: Patience pages display regardless of any pop-up blocking policy that is in effect.

CLI Compatibility Issues

- The commands to create v0.95 services do not exist in SGOS 3.x.
- All `(config icap)` commands are now `(config external-services)`.

Documentation References

Chapter 10: “External Services”—“Section A: ICAP”

Websense v4 (off-box)

Upgrade Behavior—SGOS 2.1 Upgrade Path

If the SGOS 2.1 configuration contains a Websense v4 off-box IP address, a new External Service named `websense` is created and the previous configuration, including the host and port, whether to send client information, and whether to fail open, is copied. Furthermore, if Websense v4 was the selected content filter provider, the new service is designated as the default.

Upgrade Behavior—CacheOS CA 4.2/SA 4.1 Upgrade Path

The content filtering configuration is not upgraded in 4.x because the Websense 4 off-box version used in SGOS 3.1.1 is not compatible.

CLI Compatibility Issues

The following table lists the SGOS 2.1 commands and the SGOS 3.x equivalents.

Table 2.3: Equivalent CLI Commands

SGOS2.1 Command (content-filter)	SGOS3.x Command (external-services)
(config websense 4.x off-box) ip-address <i>ip_address</i>	(config websense service_name) host { <i>ip_address</i> <i>host_name</i> }
(config websense 4.x off-box) port <i>port</i>	(config websense service_name) port <i>port</i>
(config websense 4.x off-box) send-user-name	(config websense service_name) send-client-info
(config websense 4.x off-box) fail-open	(config websense service_name) fail-open
(config content-filter) select-provider websense4 off-box	(config websense service_name) apply-by-default

The following CacheOS CA 4.2 commands are obsolete and removed from SGOS 3.x:

```
(config websense 4.x off-box) default-domain domain
(config websense 4.x off-box) directory-service service
```

Documentation References

Chapter 10: “External Services”—“Section B: Websense”

Access Logging

The access logging feature has been enhanced to support multiple logs and policy-based logging.

Upgrade Behavior—All Upgrade Paths

- Upon upgrading to SGOS 3.x, all configurations based on the single log are converted as follows:
 - ❑ Three new logs are created by default: *main*, *streaming*, and *im*.
 - ❑ The upload and rotation configurations are inherited from the previous version.
 - ❑ Seven new formats are created by default: *main* (ELFF), *streaming* (ELFF), *im* (ELFF), *NCSA*, *Squid*, *SurfControl*, and *Websense*.
 - ❑ If the previous single log format used ELFF or a custom format, upon upgrading the main log uses the same format as previously defined.

Note: The SGOS 3.x ELFF format uses ELFF strings rather than % strings; this is converted during the upgrade. Custom strings retain the % strings.

- ❑ If the previous single log used NCSA or Squid formats, upon upgrading the main log uses pre-defined NCSA or Squid format.
- ❑ The streaming log facility employs the ELFF format similar to that used previously for just Windows Media. The streaming log inherits all other configurations, such as upload and rotation, from the previous version.

- ❑ If access logging was enabled before the upgrade, the HTTP, HTTPS, FTP, ICP, and TCP-Tunnel protocols are configured to send to the `main` log. If access logging was not enabled, the default logging policy for these protocols is defined as none.
- ❑ If Windows Media access logging was enabled before the upgrade, the Windows Media protocol logs are sent to the `streaming` log.
- ❑ The previous RealProxy access logging configuration is ignored.
- ❑ Access logging for all proxies new to SGOS 3.x (such as IM) default to none.
- Real Media access logging is supported; however, the proprietary RealNetworks format is not supported.
- Upon upgrading, existing log files from previous versions are not accessible; however, they remain on the ProxySG and are accessible upon a downgrade.

Administrator Actions

- Because pre-upgrade access logs are not accessible once the ProxySG is upgraded SGOS 3.x, save them off-box in case they need to be examined.
- If you previously had HTTP services with NAP and explicit attributes, you must add a CPL policy rule to continue to suppress access logging and caching (if such behavior is required).
- If required, configure the Real Media and QuickTime proxies to send logs to the `streaming` log or another log of choice.
- If you have policy rules for matching transactions and changing `https://www.site.com` log entries, you must rewrite these rules to adhere to the new format: `tcp://www.site.com`.

CLI Compatibility Issues

- The `access-logging` commands have been completely redesigned.
- The Access Logging console URLs have been changed. Most of the new console URLs end with the log name to distinguish the information provided.

Documentation References

- Chapter 19: “Access Logging”
- Chapter 5: “Managing Port Services”
- Chapter 6: “Configuring Proxies”

Monitoring and Maintenance

Heartbeats

Upgrade Behavior—All Upgrade Paths

The previous HTTP POST heartbeat method is replaced by HTTPS POST. Also, the fallback to SMTP is no longer supported; therefore, heartbeats now use only HTTPS, which is more secure as compared to HTTP and SMTP.

Administrator Actions

Blue Coat recommends enabling heartbeats, or Blue Coat monitoring; SGOS 3.x ensures the privacy of your ProxySG configuration.

Documentation References

Appendix F: “Diagnostics”—“Diagnostic Reporting (Heartbeats)”

Content Management

Upgrade Behavior—All Upgrade Paths

None.

Administrator Actions

None.

CLI Compatibility Issues

The `content distribute` command accepts `url entered_url` or just `entered_url`.

System Level and Core Operating System Features

Upgrade Behavior—All SGOS 2.1 and CacheOS CA 4.2 Upgrade Paths

The System Resource Allocation (%) feature does not exist in SGOS 3.x. This feature is not required in SGOS 3.x because resources are shared dynamically among protocols.

Upgrade Behavior—CacheOS SA 4.1 Upgrade Path

SGOS 3.x combines the features previously segregated by appliances running CacheOS CA 4.2 and CacheOS SA 4.2. The ProxySG can be used as both a forward proxy and a reverse proxy at the same time.

Administrator Actions

Refer to HTTP information and documentation to understand how the SGOS 3.x HTTP profile affects reverse proxy deployments.

CLI Compatibility Issues

The `system-resource-percent` command is removed.

Securing the Serial Port

This is a new feature in 3.2.4. When the secure serial port is enabled (recommended):

- A setup console password is required in order to access the setup console. If the setup console password is forgotten, the setup console is inaccessible and can no longer be used to manage network settings or recover from Management Console problems.
- A username and password is required in order to use the CLI through the serial console. If the setup console password is forgotten, you can still use the serial console to connect to the ProxySG CLI.

Upgrade/Downgrade Behavior

- If you are upgrading to 3.2.4, the secure serial port is disabled by default. If you subsequently use the setup console, you are asked if you want to enable the secure serial port at that time.
- On new installations, you are asked if you want to enable the secure serial port.
- Downgrades will ignore the secure serial port setting. If older systems are present on the machine, it can be possible for an attacker to force the downgrade and then access the serial port. For maximum security, older systems should be deleted.