

Blue Coat® Systems SG™ Appliance

Volume 9: Managing the Blue Coat SG Appliance

SGOS Version 5.2.2



Contact Information

Blue Coat Systems Inc.
420 North Mary Ave
Sunnyvale, CA 94085-4121

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

bcs.info@bluecoat.com
<http://www.bluecoat.com>

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

Copyright© 1999-2007 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. ProxyAV™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, RA Connector™, RA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos 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: 231-02846

Document Revision: SGOS 5.2.2—09/2007

Contents

Contact Information

Chapter 1: About Managing the SG Appliance

| | |
|---------------------------|---|
| Document Conventions..... | 7 |
|---------------------------|---|

Chapter 2: Monitoring the SG Appliance

| | |
|--|----|
| Using Director to Manage SG Systems | 9 |
| Setting up Director and SG Appliance Communication | 11 |
| Monitoring the System and Disks..... | 12 |
| System Summary..... | 12 |
| Viewing System Environment Sensors | 13 |
| Viewing Disk Status..... | 14 |
| Viewing SSL Accelerator Card Information..... | 15 |
| Setting Up Event Logging and Notification | 15 |
| Configuring Which Events to Log..... | 15 |
| Setting Event Log Size | 16 |
| Enabling Event Notification | 16 |
| Syslog Event Monitoring..... | 17 |
| Viewing Event Log Configuration and Content..... | 18 |
| Configuring SNMP | 20 |
| Enabling SNMP | 20 |
| Configuring SNMP Community Strings | 21 |
| Configuring SNMP Traps | 22 |
| Configuring Health Monitoring..... | 23 |
| Health Monitoring Requirements..... | 23 |
| About the Health Monitoring Metric Types | 24 |
| About Health Monitoring | 24 |
| About Health Monitoring Notification..... | 26 |
| About the General Metrics..... | 26 |
| About the Licensing Metrics..... | 26 |
| About the Status Metrics..... | 27 |
| Changing Threshold and Notification Properties | 28 |
| Getting A Quick View of the SG Appliance Health..... | 29 |
| Viewing Health Monitoring Statistics..... | 30 |
| Troubleshooting | 31 |

Chapter 3: Maintaining the SG Appliance

| | |
|---|----|
| Restarting the SG Appliance..... | 33 |
| Hardware and Software Restart Options | 33 |
| Restoring System Defaults | 34 |

| | |
|---|----|
| Restore-Defaults..... | 34 |
| Factory-Defaults..... | 35 |
| Keep-Console..... | 35 |
| Clearing the DNS Cache | 36 |
| Clearing the Object Cache..... | 36 |
| Clearing the Byte Cache | 37 |
| Troubleshooting Tip..... | 37 |
| Clearing Trend Statistics | 37 |
| Upgrading the SG Appliance | 37 |
| The SG Appliance 5.x Version Upgrade..... | 38 |
| Troubleshooting Tip..... | 40 |
| Managing SG Appliance Systems..... | 40 |
| Setting the Default Boot System | 41 |
| Locking and Unlocking SG Appliance Systems..... | 42 |
| Replacing an SG Appliance System | 42 |
| Deleting an SG Appliance System..... | 43 |
| Disk Reinitialization | 43 |
| Multi-Disk SG Appliances..... | 43 |
| Single-Disk SG Appliance..... | 44 |
| Deleting Objects from the SG Appliance..... | 44 |

Chapter 4: Diagnostics

| | |
|---|----|
| Diagnostic Reporting (Service Information)..... | 46 |
| Sending Service Information Automatically..... | 46 |
| Managing the Bandwidth for Service Information..... | 47 |
| Configure Service Information Settings | 48 |
| Creating and Editing Snapshot Jobs | 50 |
| Packet Capturing (the Job Utility) | 52 |
| PCAP File Name Format..... | 52 |
| Common PCAP Filter Expressions | 52 |
| Configuring Packet Capturing..... | 53 |
| Core Image Restart Options | 57 |
| Diagnostic Reporting (Heartbeats)..... | 58 |
| Diagnostic Reporting (CPU Monitoring)..... | 59 |

Chapter 5: Statistics

| | |
|--|----|
| Selecting the Graph Scale..... | 61 |
| Viewing Traffic Distribution Statistics..... | 62 |
| Understanding Chart Data | 63 |
| Refreshing the Data | 63 |
| About Bypassed Bytes..... | 63 |
| About the Default Service Statistics | 64 |
| Viewing Bandwidth Usage or Gain | 64 |
| Viewing Client Byte and Server Byte Traffic Distribution | 65 |

| | |
|--|----|
| Viewing Traffic History | 65 |
| Understanding Chart Data | 67 |
| Refreshing the Data | 67 |
| About Bypassed Bytes..... | 68 |
| Viewing Bandwidth Usage or Gain or Client Byte and Server Byte Traffic History | 68 |
| Viewing the ADN History | 68 |
| Viewing Bandwidth Management Statistics..... | 68 |
| Viewing Protocol Statistics | 68 |
| Viewing System Statistics | 70 |
| Resources Statistics | 70 |
| Contents Statistics | 74 |
| Event Logging Statistics..... | 75 |
| Failover Statistics | 76 |
| Active Sessions—Viewing Per-Connection Statistics | 76 |
| Analyzing Proxied Sessions | 77 |
| Filtering the Display | 83 |
| Viewing HTML and XML Views of Proxied Sessions Data | 84 |
| Analyzing Bypassed Connections Statistics | 84 |
| Filtering the Display | 86 |
| Viewing HTML and XML Views of Bypassed Connections Data..... | 87 |
| Viewing Health Monitoring Statistics..... | 87 |
| Viewing Health Check Statistics..... | 87 |
| Viewing the Access Log..... | 87 |
| Viewing Advanced Statistics..... | 87 |
| Using the CLI show Command to View Statistics | 88 |

Appendix A: Glossary

Index

Chapter 1: About Managing the SG Appliance

Volume 9: Managing the Blue Coat SG Appliance describes how to monitor the SG appliance with SNMP (a brief introduction to Director is provided), event logging, or health monitoring. It also describes common maintenance and troubleshooting tasks.

Discussed in this volume:

- ❑ Chapter 2: "Monitoring the SG Appliance"
- ❑ Chapter 3: "Maintaining the SG Appliance"
- ❑ Chapter 4: "Diagnostics"
- ❑ Chapter 5: "Statistics"
- ❑ Appendix A: "Glossary"

Document Conventions

The following section lists the typographical and Command Line Interface (CLI) syntax conventions used in this manual.

Table 1-1. Document Conventions

| Conventions | Definition |
|-------------------------|--|
| <i>Italics</i> | The first use of a new or Blue Coat-proprietary term. |
| Courier font | Command line text that appears on your administrator workstation. |
| <i>Courier Italics</i> | A command line variable that is to be substituted with a literal name or value pertaining to the appropriate facet of your network system. |
| Courier Boldface | A Blue Coat literal to be entered as shown. |
| { } | One of the parameters enclosed within the braces must be supplied |
| [] | An optional parameter or parameters. |
| | Either the parameter before or after the pipe character can or must be selected, but not both. |

Chapter 2: Monitoring the SG Appliance

This chapter describes the methods you can use to monitor your SG appliances, including event logging, SNMP, and health monitoring. A brief introduction to Director is also provided.

This chapter contains the following sections:

- ❑ “Using Director to Manage SG Systems” on page 9
- ❑ “Monitoring the System and Disks” on page 12
- ❑ “Setting Up Event Logging and Notification” on page 15
- ❑ “Configuring SNMP” on page 20
- ❑ “Configuring Health Monitoring” on page 23

Using Director to Manage SG Systems

Blue Coat Director allows you to manage multiple SG appliances, eliminating the need to configure and control the appliances individually.

Director allows you to configure an SG appliance and then push that configuration out to as many appliances as required. Director also allows you to delegate network and content control to multiple administrators and distribute user and content policy across a Content Delivery Network (CDN). With Director, you can:

- ❑ Reduce management costs by centrally managing all Blue Coat appliances.
- ❑ Eliminate the need to manually configure each remote SG appliance.
- ❑ Recover from system problems with configuration snapshots and recovery.

Automatically Registering the SG Appliance with Director

You can use the Blue Coat Director registration feature to automatically register the SG appliance with a Blue Coat Director, thus enabling that Director to establish a secure administrative session with the appliance. During the registration process, Director can “lock out” all other administrative access to the appliance so that all configuration changes are controlled and initiated by Director. This is useful if you want to control access to the appliance or if you want to ensure that appliances receive the same configuration.

The registration process is fully authenticated; the devices use their Blue Coat appliance certificate or a *shared secret* (a registration password configured on Director) to confirm identities before exchanging public keys. If the SG appliance has an appliance certificate, that certificate is used to authenticate the SG appliance to Director as an SSL client. If the SG appliance does not have an appliance certificate, you must configure a registration secret on Director and specify that secret on the SG appliance. Refer to the *Blue Coat Director Configuration and Management Guide* for more information about specifying the shared secret.

Note: The Blue Coat appliance certificate is an X.509 certificate that contains the hardware serial number of a specific SG device as the Common Name (CN) in the subject field. Refer to the device authentication information in *Volume 5: Advanced Networking* for more information about appliance certificates.

Director Registration Requirements

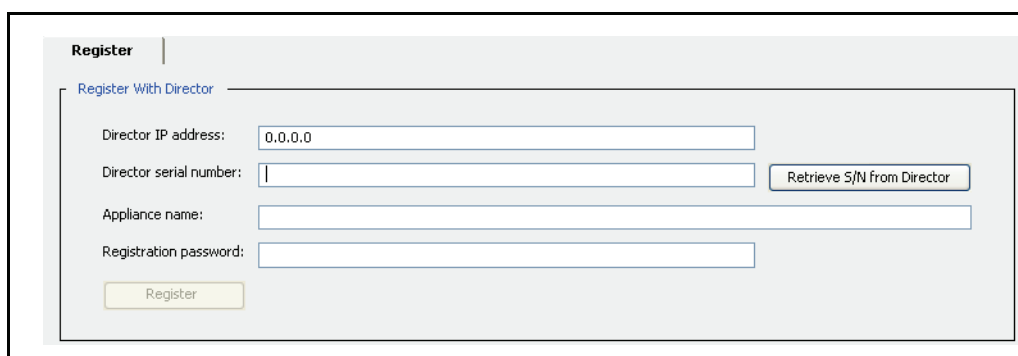
To register the appliance with Director, the SSH-Console service must be enabled. Director registration will fail if the ssh-console has been disabled or deleted, or if the SSHv2 host key has been removed.

Registering the SG Appliance with Director

Though usually initiated at startup (with the serial console setup), you can also configure Director registration from the Management Console, as described in the following procedure.

To register the appliance with a Director:

1. Select **Maintenance > Director Registration**.



The screenshot shows a web form titled "Register" with a sub-section "Register With Director". The form contains the following fields and buttons:

- Director IP address:** A text input field with the value "0.0.0.0".
- Director serial number:** A text input field with a vertical cursor. To its right is a button labeled "Retrieve S/N from Director".
- Appliance name:** A text input field.
- Registration password:** A text input field.
- Register:** A yellow button at the bottom left of the form.

2. In the **Director IP address** field, enter the Director IP address.
3. In the **Director serial number** field, enter the Director serial number or click **Retrieve S/N from Director**. If you retrieve the serial number from the Director, verify that the serial number matches the one specified for your Director.
4. Optional—In the **Appliance name** field, enter the SG appliance name.
5. If your appliance does not have an appliance certificate, enter the Director shared secret in the **Registration password** field.

Note: Refer to the *Blue Coat Director Configuration and Management Guide* for more information about configuring the shared secret. For information about appliance certificates, refer to *Volume 5: Advanced Networking*.

6. Click **Register**.

Related CLI Commands for Director Registration

```
SGOS# register-with-director dir_ip_address [appliance_name  
dir_serial_number]
```

Setting up Director and SG Appliance Communication

Director and the SG appliance use SSHv2 as the default communication mode. SSHv1 is not supported.

For Director to successfully manage multiple appliances, it must be able to communicate with an appliance using SSH/RSA and the Director's public key must be configured on each system that Director manages.

When doing initial setup of the SG appliance from Director, Director connects to the device using the authentication method established on the device: SSH with simple authentication or SSH/RSA. SSH/RSA is preferred, and must also be set up on Director before connecting to the SG appliance.

Director can create an RSA keypair for an SG appliance to allow connections. However, for full functionality, Director's public key must be configured on each appliance. You can configure the key on the system using the following two methods:

- ❑ Use Director to create and push the key.
- ❑ Use the `import-director-client-key` CLI command from the SG appliance.

Using Director to create and push client keys is the recommended method. The CLI command is provided for reference.

Complete the following steps to put Director's public key on the SG appliance using the CLI of the appliance. You must complete this procedure from the CLI. The Management Console is not available.

Note: For information on creating and pushing a SSH keypair on Director, refer to the *Blue Coat Director Installation Guide*.

Log in to the SG appliance you want to manage from Director.

1. From the `(config)` prompt, enter the `ssh-console` submode:

```
SGOS#(config) ssh-console
SGOS#(config ssh-console)
```

2. Import Director's key that was previously created on Director and copied to the clipboard.

Important: You must add the Director identification at the end of the client key. The example shows the username, IP address, and MAC address of Director. "Director" (without quotes) must be the username, allowing you access to passwords in clear text.

```
SGOS#(config services ssh-console) inline director-client-key
Paste client key here, end with "..." (three periods)
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvJIXt1ZausE9qrcXem2IK/mC4dY8Cxxo1/
B8th4KvedFY33OByO/pvwcuchPZz+b1LETTY/zc3SL7jdVffq00KBN/
ir4zu7L2XT68ML2ORWa9tXFedNmKl/iagI3/QZJ8T8zQM6o7WnBzTvMC/
ZElMZZddAE3yPCv9+s2TR/Ipk=director@10.25.36.47-2.00e0.8105.d46b
...
ok
```

To view the fingerprint of the key:

```
SGOS#(config sshd) view director-client-key clientID
jsmith@granite.example.com
83:C0:0D:57:CC:24:36:09:C3:42:B7:86:35:AC:D6:47
```

To delete a key:

```
SGOS#(config sshd) delete director-client-key clientID
```

Monitoring the System and Disks

The **System and disks** page in the Management Console has the following tabs:

❑ **Summary**

Provides configuration information and a general status information about the device.

❑ **Tasks**

Enables you to perform systems tasks, such as restarting the system and clearing the DNS or object cache. See [Chapter 3: "Maintaining the SG Appliance"](#) for information about these tasks.

❑ **Environment**

Displays hardware statistics.

❑ **Disks**

Displays details about the installed disks and enables you take them offline.

❑ **SSL Cards**

Displays details about any installed SSL cards.

These statistics are also available in the CLI.

Note: The SG 400 appliances do not have an Environment tab.

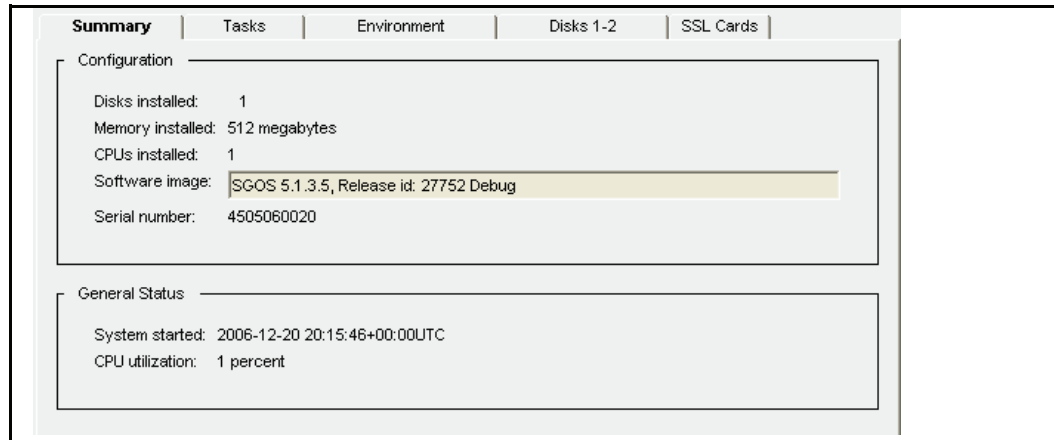
System Summary

The device provides a variety of information on its status. The fields on the Summary tab are described below:

- ❑ **Disks Installed**—the number of disk drives installed in the device. The Disks tab displays the status of each drive.
- ❑ **Memory installed**—the amount of RAM installed in the device.
- ❑ **CPUs installed**—the number of CPUs installed in the device.
- ❑ **Software image**—the version and release number of the device image.
- ❑ **Serial number**—the serial number of the machine, if available.
- ❑ **System started**—the time and date the device was started.
- ❑ **CPU utilization**—the current percent utilization of the device CPU.

To view the system summary statistics:

Select **Maintenance > System and disks > Summary**.



Viewing System Environment Sensors

The icons on the Environment tab are green when the related hardware environment is within acceptable parameters, and red when an out-of-tolerance condition exists. If an icon is red, click **View Sensors** to view detailed sensor statistics to learn more about the out-of-tolerance condition.

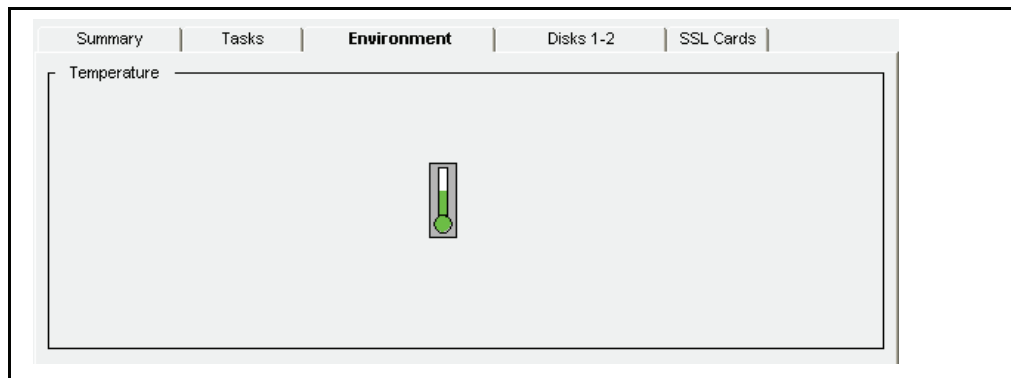
Note: The health monitoring metrics on the Statistics > Health page also show the state of environmental sensors. See [“Configuring Health Monitoring”](#) on page 23 for more information.

Note: You cannot view environment statistics on an SG 400 appliance.

To view the system environment statistics:

1. Select **Maintenance > System and disks > Environment**.

Note: This tab varies depending on the type of SG appliance that you are using.



2. Click **View Sensors** to see detailed sensor values; close the window when you are finished.

| Sensor statistics | | |
|-------------------|---------|--------|
| Sensor Name | Reading | Status |
| MB Temperature | 31.0 C | OK |
| CPU Temperature | 31.0 C | OK |

Viewing Disk Status

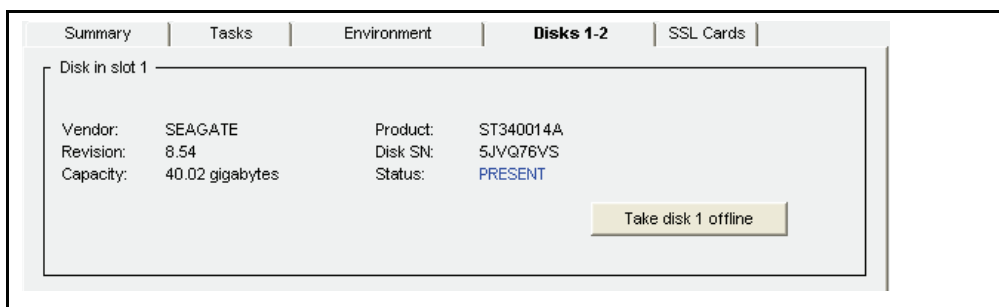
You can view the status of each of the disks in the system and take a disk offline if needed.

To view disk status or take a disk offline:

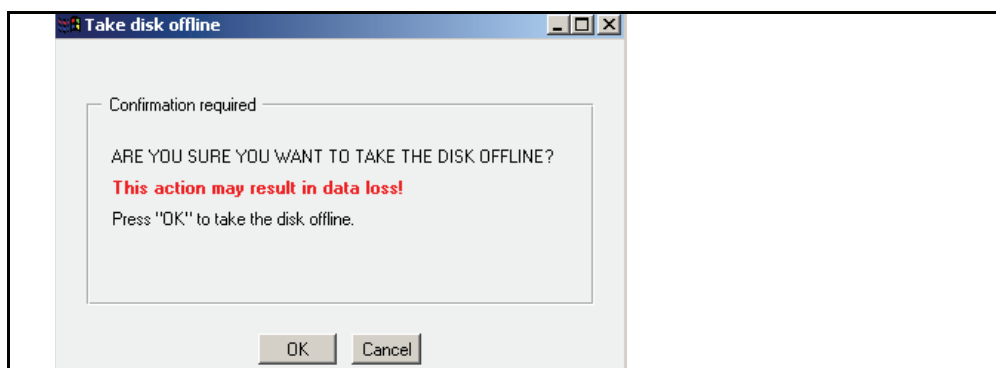
1. Select **Maintenance > System and disks > Environment**.

The default view provides information about the disk in slot 1.

Note: The name and appearance of this tab differs, depending on the range of disks available to the SG appliance model you use.



2. Select the disk to view or to take offline by clicking the appropriate disk icon.
3. (Optional) To take the selected disk offline, click the **Take disk x offline** button (where x is the number of the disk you have selected); click **OK** in the Take disk offline dialog that displays.



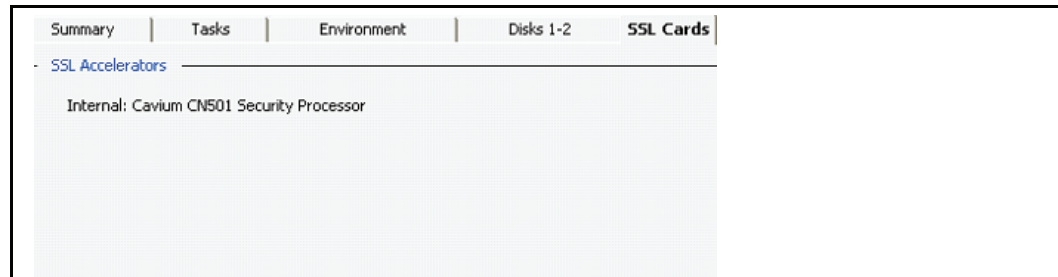
Viewing SSL Accelerator Card Information

Selecting the **Maintenance > System and disks > SSL Cards** tab allows you to view information about any SSL accelerator cards in the system. If no accelerator cards are installed, that information is stated on the pane.

To view SSL accelerator cards:

Note: You cannot view statistics about SSL accelerator cards through the CLI.

Select **Maintenance > System and disks > SSL Cards**.



Setting Up Event Logging and Notification

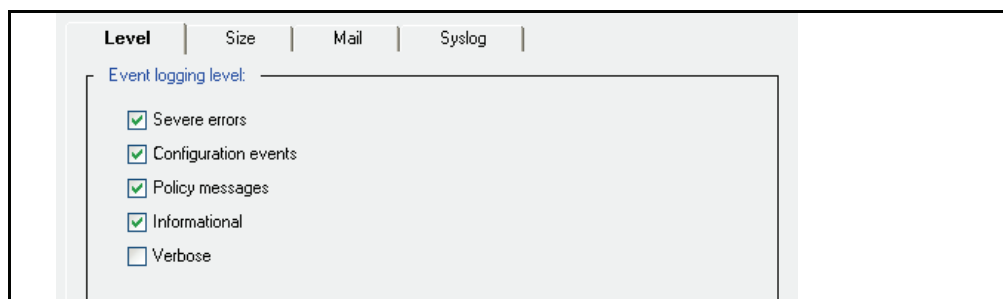
You can configure the SG appliance to log system events as they occur. *Event logging* allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The appliance can also notify you by e-mail if an event is logged.

Configuring Which Events to Log

The event level options are listed from the most to least important events. Because each event requires some disk space, setting the event logging to log all events fills the event log more quickly.

To set the event logging level:

1. Select **Maintenance > Event Logging > Level**.



2. Select the events you want to log.

When you select an event level, all levels above the selection are included. For example, if you select **Verbose**, all event levels are included.

3. Click **Apply**.

Related CLI Commands for Setting the Event Logging Level

```
SGOS#(config event-log) level {severe | configuration | policy |
informational | verbose}
```

Table 2-1. Event Logging Level Options

| | |
|---------------|---|
| severe | Writes only severe error messages to the event log. |
| configuration | Writes severe and configuration change error messages to the event log. |
| policy | Writes severe, configuration change, and policy event error messages to the event log. |
| informational | Writes severe, configuration change, policy event, and information error messages to the event log. |
| verbose | Writes all error messages to the event log. |

Setting Event Log Size

You can limit the size of the appliances’s event log and specify what the appliance should do if the log size limit is reached.

To set event log size:

1. Select **Maintenance > Event Logging > Size**.

2. In the **Event log size** field, enter the maximum size of the event log in megabytes.
3. Select either **Overwrite earlier events** or **Stop logging new events** to specify the desired behavior when the event log reaches maximum size.
4. Click **Apply**.

Related CLI Commands to Set the Event Log Size

```
SSGOS#(config event-log) log-size megabytes
SSGOS#(config event-log) when-full {overwrite | stop}
```

Enabling Event Notification

The SG appliance can send event notifications to Internet e-mail addresses using SMTP. You can also send event notifications directly to Blue Coat for support purposes. For information on configuring diagnostic reporting, see [Chapter 4: "Diagnostics"](#).

Note: The SG appliance must know the host name or IP address of your SMTP mail gateway to mail event messages to the e-mail address(es) you have entered. If you do not have access to an SMTP gateway, you can use the Blue Coat default SMTP gateway to send event messages directly to Blue Coat.

The Blue Coat SMTP gateway only sends mail to Blue Coat. It will not forward mail to other domains.

To enable event notifications:

1. Select **Maintenance > Event Logging > Mail**.

The screenshot shows the 'Mail' configuration page. At the top, there are tabs for 'Level', 'Size', 'Mail', and 'Syslog'. Below the tabs, there is a section titled 'Mail notifications to:'. Inside this section, there is a table with a header 'Names' and an empty body. Below the table, there are three buttons: 'New', 'Edit', and 'Delete'. Below the buttons, there are three radio buttons: 'SMTP gateway name:' (selected), 'SMTP gateway IP:', and 'Clear SMTP gateway settings'. The 'SMTP gateway name:' field contains the text 'mail.heartbeat.bluecoat.com'. The 'SMTP gateway IP:' field is empty.

2. Click **New** to add a new e-mail address; click **OK** in the Add list item dialog that appears.
3. In the **SMTP gateway name** field, enter the host name of your mail server; or in the **SMTP gateway IP** field, enter the IP address of your mail server.
4. (Optional) If you want to clear one of the above settings, select the radio button of the setting you want to clear. You can clear only one setting at a time.
5. Click **Apply**.

Related CLI Commands to Enable Event Notifications

```
SGOS#(config event-log) mail add email_address
```

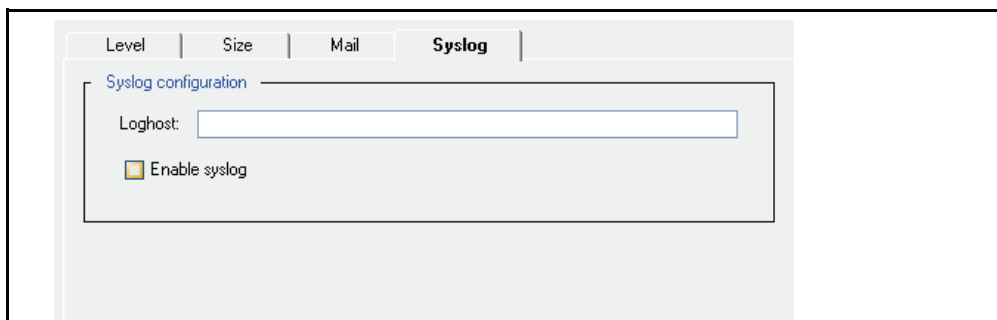
Syslog Event Monitoring

Syslog is an event-monitoring scheme that is especially popular in UNIX environments. Sites that use syslog typically have a log host node, which acts as a sink (repository) for several devices on the network. You must have a syslog daemon operating in your network to use syslog monitoring. The syslog format is: Date Time Hostname Event.

Most clients using syslog have multiple devices sending messages to a single syslog daemon. This allows viewing a single chronological event log of all of the devices assigned to the syslog daemon. An event on one network device might trigger an event on other network devices, which, on occasion, can point out faulty equipment.

To enable syslog monitoring:

1. Select **Maintenance > Event Logging > Syslog**.



2. In the **Loghost** field, enter the domain name or IP address of your loghost server.
3. Select **Enable Syslog**.
4. Click **Apply**.

Related CLI Commands to Enable Syslog Monitoring

```
SGOS#(config event-log) syslog {disable | enable}
```

Viewing Event Log Configuration and Content

You can view the system event log, either in its entirety or selected portions of it.

Viewing the Event Log Configuration

You can view the event log configuration, from `show` or from `view` in the `event-log` configuration mode.

To view the event log configuration:

At the prompt, enter the following command:

- ❑ From anywhere in the CLI

```
SGOS> show event-log configuration
Settings:
  Event level: severe + configuration + policy + informational
  Event log size: 10 megabytes
  If log reaches maximum size, overwrite earlier events
  Syslog loghost: <none>
  Syslog notification: disabled
  Syslog facility: daemon
Event recipients:
SMTP gateway:
  mail.heartbeat.bluecoat.com
```

-or-

- ❑ From the `(config)` prompt:

```
SGOS#(config) event-log
SGOS#(config event-log) view configuration
Settings:
  Event level: severe + configuration + policy + informational
  Event log size: 10 megabytes
  If log reaches maximum size, overwrite earlier events
  Syslog loghost: <none>
```

```
Syslog notification: disabled
Syslog facility: daemon
Event recipients:
SMTP gateway:
mail.heartbeat.bluecoat.com
```

Viewing the Event Log Contents

Again, you can view the event log contents from the `show` command or from the event-log configuration mode.

The syntax for viewing the event log contents is

```
SGOS# show event-log
```

```
-or-
```

```
SGOS# (config event-log) view
```

```
[start [YYYY-mm-dd] [HH:MM:SS]] [end [YYYY-mm-dd] [HH:MM:SS]] [regex
regex | substring string]
```

Pressing `<Enter>` shows the entire event log without filters.

The order of the filters is unimportant. If `start` is omitted, the start of the recorded event log is used. If `end` is omitted, the end of the recorded event log is used.

If the date is omitted in either `start` or `end`, it must be omitted in the other one (that is, if you supply just times, you must supply just times for both `start` and `end`, and all times refer to today). The time is interpreted in the current timezone of the appliance.

Understanding the Time Filter

The entire event log can be displayed, or either a starting date/time or ending date/time can be specified. A date/time value is specified using the notation ([YYYY-MM-DD] [HH:MM:SS]). Parts of this string can be omitted as follows:

- ❑ If the date is omitted, today's date is used.
- ❑ If the time is omitted for the starting time, it is 00:00:00
- ❑ If the time is omitted for the ending time, it is 23:59:59

At least one of the date or the time must be provided. The date/time range is inclusive of events that occur at the start time as well as dates that occur at the end time.

Note: If the notation includes a space, such as between the start date and the start time, the argument in the CLI should be quoted.

Understanding the Regex and Substring Filters

A regular expression can be supplied, and only event log records that match the regular expression are considered for display. The regular expression is applied to the text of the event log record not including the date and time. It is case-sensitive and not anchored. You should quote the regular expression.

Since regular expressions can be difficult to write properly, you can use a substring filter instead to search the text of the event log record, not including the date and time. The search is case sensitive.

Regular expressions use the standard regular expression syntax as defined by policy. If both `regex` and `substring` are omitted, then all records are assumed to match.

Example

```

SGOS# show event-log start "2004-10-22 9:00:00" end "2004-10-22
9:15:00"

2004-10-22 09:00:02+00:00UTC "Snapshot sysinfo_stats has fetched /
sysinfo-stats " 0 2D0006:96 ../Snapshot_worker.cpp:183

2004-10-22 09:05:49+00:00UTC "NTP: Periodic query of server
ntp.bluecoat.com, system clock is 0 seconds 682 ms fast compared to NTP
time. Updated system clock. " 0 90000:1 ../ntp.cpp:631

```

Configuring SNMP

You can view an SG appliance using a Simple Network Management Protocol (SNMP) management station. The appliance supports MIB-2 (RFC 1213), Proxy MIB, and the RFC2594 MIB, and can be downloaded at the following URL: <https://download.bluecoat.com/release/SGOS5/index.html> (The SNMP link is in the lower right-hand corner).

Enabling SNMP

To view an SG appliance from an SNMP management station, you must enable and configure SNMP support on the appliance.

To enable and configure SNMP:

1. Select **Maintenance > SNMP > SNMP General**.

2. Select **Enable SNMP**.
3. (Optional) To reset the SNMP configuration to the defaults, click **Reset SNMP settings**. This erases any trap settings that were set as well as any community strings that had been created. You do not need to reboot the system after making configuration changes to SNMP.
4. In the **sysLocation** field, enter a string that describes the appliance's physical location.
5. In the **sysContact** field, enter a string that identifies the person responsible for administering the appliance.

Related CLI Commands to Enable and Configure SNMP

```

SGOS#(config snmp) {disable | enable}
SGOS #(config snmp) sys-contact string
SGOS#(config snmp) sys-location string

```

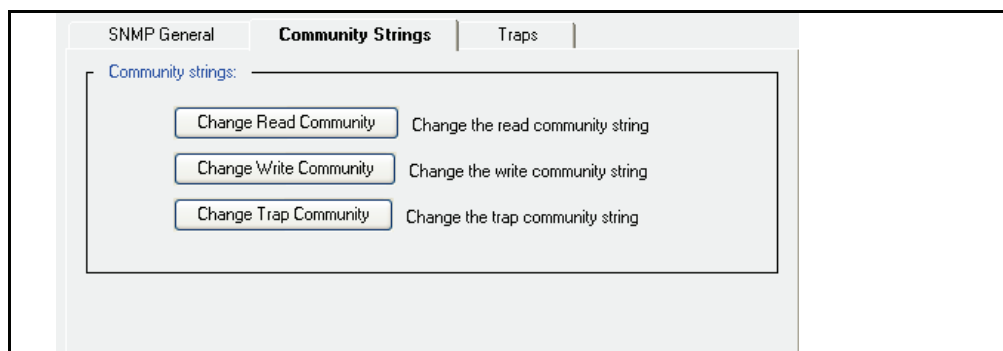
Configuring SNMP Community Strings

Use *community strings* to restrict access to SNMP data. To read SNMP data on the SG appliance, specify a *read community string*. To write SNMP data to the appliance, specify a *write community string*. To receive traps, specify a *trap community string*. By default, all community string passwords are set to public.

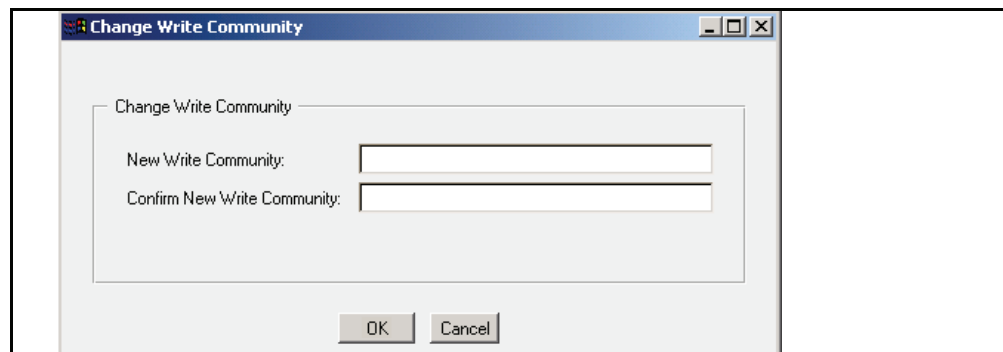
Note: If you enable SNMP, make sure to change all three community-string passwords to values that are difficult to guess. Use a combination of uppercase, lowercase, and numeric characters. An easily-guessed community-string password makes it easier to gain unauthorized access to the SG appliance and network.

To set or change community strings:

1. Select **Maintenance > SNMP > Community Strings**.



2. Click the community string button you want to change.
The Change Read/Write/Trap Community dialog displays.



3. Enter and confirm the community string; click **OK**.
4. Click **Apply**.

To set or change community strings:

You can set the community strings in either cleartext or encrypted form.

To set them in cleartext:

```
SGOS#(config) snmp
SGOS#(config snmp) enable
SGOS#(config snmp) read-community password
SGOS#(config snmp) write-community password
```

```
SGOS#(config snmp) trap-community password
```

To set them as encrypted:

```
SGOS#(config) snmp
SGOS#(config snmp) enable
SGOS#(config snmp) encrypted-read-community encrypted-password
SGOS#(config snmp) encrypted-write-community encrypted-password
SGOS#(config snmp) encrypted-trap-community encrypted-password
```

Configuring SNMP Traps

The SG appliance can send SNMP traps to a management station as they occur. By default, all system-level traps are sent to the address specified. You can also enable authorization traps to send notification of attempts to access the Management Console. Also, if the system crashes for whatever reason, a cold start SNMP trap is issued on power up. No configuration is required.

Note: The SNMP trap for CPU utilization is sent only if the CPU continues to stay up for 32 or more seconds.

To enable SNMP traps:

Note: You cannot configure SNMP traps to go out through a particular interface. The interface that is configured first is used until it fails and is used to identify the device.

1. Select **Maintenance > SNMP > Traps**.

2. In the **Send traps to** fields, enter the IP address(es) of the workstation(s) where traps are to be sent.
3. To receive authorization traps, select **Enable authorization traps**.
4. Select **Apply** to commit the changes to the SG appliance.

Related CLI Commands for Enabling SNMP Traps

```
SGOS#(config snmp) trap-address {1 | 2 | 3} ip_address
```

Indicates which IP address(es) can receive traps and in which priority.

```
SGOS#(config snmp) authorize-traps
```

Configuring Health Monitoring

The health monitoring feature tracks key hardware and software metrics so that you can quickly discover and diagnose potential problems. Director (and other third-party network management tools) also use these metrics to remotely display the current state of the SG appliance. By monitoring these key hardware and software metrics, Director can display a variety of health-related statistics—and trigger notification if action is required.

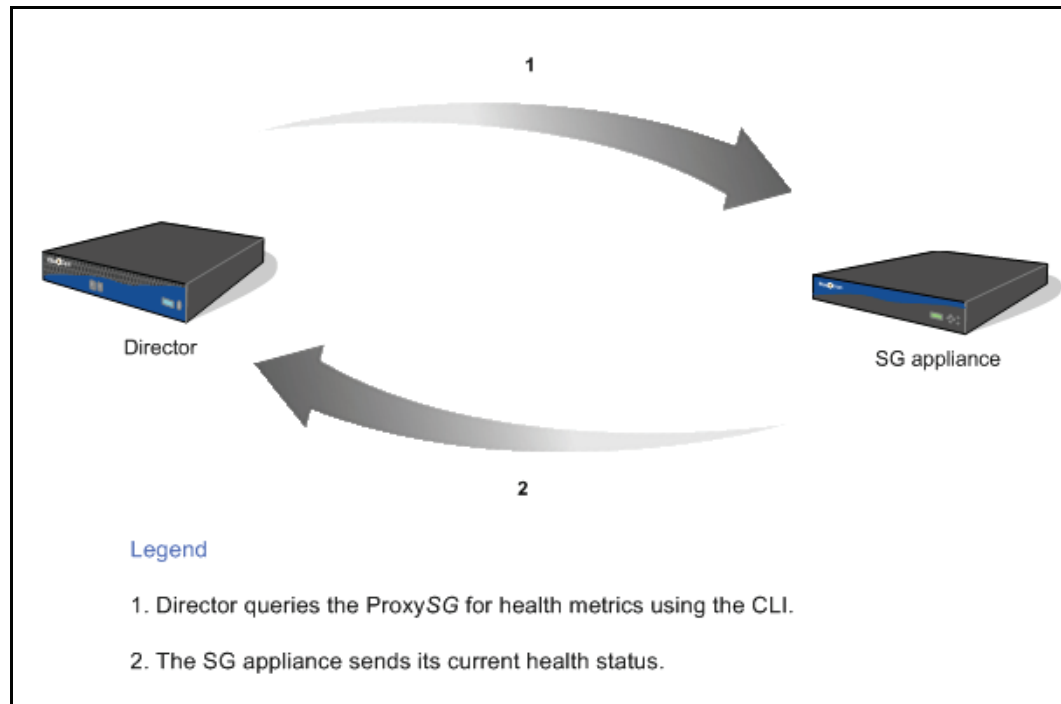


Figure 2-1. Health Monitoring Configuration and Notification Process

As shown in the preceding figure, health monitoring metrics can be remotely configured and queried from Director. The metrics are also configurable on the SG appliance itself.

To facilitate prompt corrective action, notification can be configured for threshold “events.” For example, an administrator can configure a threshold so that an e-mail or SNMP trap is generated when the threshold state changes. Additionally, many of the threshold levels are configurable so that you can adjust the thresholds to meet your specific requirements.

Health Monitoring Requirements

Before using the health monitoring feature you must ensure that the e-mail addresses of all persons that should be notified of health monitoring alerts are listed in the Event log properties. See “[Setting Up Event Logging and Notification](#)” on page 15 for more information.

About the Health Monitoring Metric Types

The SG appliance monitors the following types of health metrics:

- ❑ Hardware
- ❑ Environmental
- ❑ ADN
- ❑ System resource
- ❑ Licensing metrics

The system resource and licensing thresholds are user-configurable, meaning that you can specify the threshold level that will trigger an alert.

The hardware, environmental, and ADN metrics are *not* configurable and are preset to optimal values. For example, on some platforms, a Warning is triggered when the CPU temperature reaches 55 degrees Celsius.

These health monitoring metrics are logically grouped as General, Licensing, or Status metrics.

About Health Monitoring

Health Monitoring allows you to set notification thresholds on various internal metrics that track the health of a monitored system or device. Each metric has a *value* and a *state*.

The *value* is obtained by periodically measuring the monitored system or device. In some cases, the value is a percentage or a temperature measurement; in other cases, it is a status like "Disk Present" or "Awaiting Approval".

The *state* indicates the severity of the metric as a health issue:

- ❑ OK—The monitored system or device is behaving normally.
- ❑ WARNING—The monitored system or device is outside typical operating parameters and may require attention.
- ❑ CRITICAL—The monitored system or device is either failing, or is far outside normal parameters, and requires immediate attention.

The current state of a metric is determined by the relationship between the value and its monitoring *thresholds*. The Warning and Critical states have thresholds, and each threshold has a corresponding *interval*.

All metrics begin in the OK state. If the value crosses the Warning threshold and remains there for the threshold's specified interval, the metric transitions to the Warning state. Similarly, if the Critical threshold is exceeded for the specified interval, the metric transitions to the Critical state. Later (for example, if the problem is resolved), the value may drop back down below the Warning threshold. If the value stays below the Warning threshold longer than the specified interval, the state returns to OK.

Every time the state changes, a notification occurs. If the value fluctuates above and below a threshold, no state change occurs until the value stays above or below the threshold for the specified interval.

This behavior helps to ensure that unwarranted notifications are avoided when values vary widely without having any definite trend. You can experiment with the thresholds and intervals until you are comfortable with the sensitivity of the notification settings.

Health Monitoring Example

The following picture shows an example. The lower horizontal line represents the Warning threshold; the upper horizontal line is the Critical threshold. Note how they divide the graph into bands associated with each of the three possible states. Assume both thresholds have intervals of 20 seconds, and that the metric is currently in the OK state.

1. At time 0, the monitored value crosses the Warning threshold. No transition occurs yet. Later, at time 10, it crosses the critical threshold. Still, no state change occurs, because the threshold interval has not elapsed.
2. At time 20, the value has been above the warning threshold for 20 seconds--the specified interval. The state of the metric now changes to Warning, and a notification is sent. Note that even though the metric is currently in the critical range, the State is still Warning, because the value has not exceeded the Critical threshold long enough to trigger a transition to Critical.
3. At time 25, the value drops below the Critical threshold, having been above it for only 15 seconds. The state remains at Warning.
4. At time 30, it drops below the Warning threshold. Again the state does not change. If the value remains below the warning threshold until time 50, then the state will change back to OK.

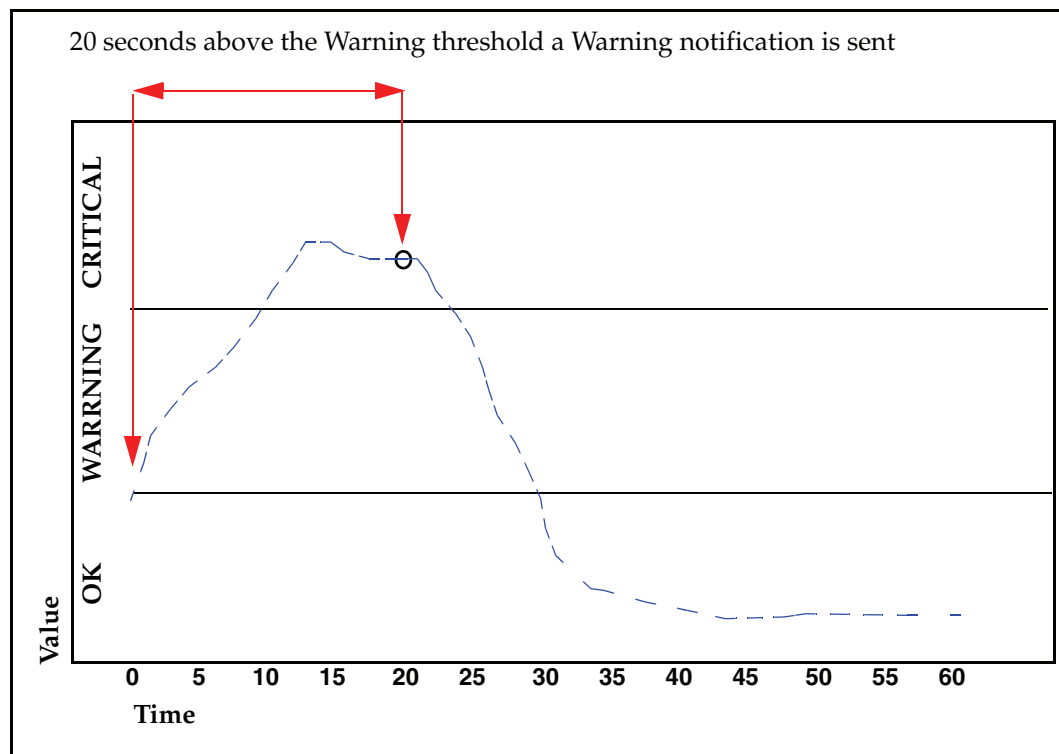


Figure 2-2. Relationship between the threshold value and threshold interval

About License Expiration Metrics

The threshold values for license expiration metrics are set in days until expiration. In this context, a "critical" threshold indicates that license expiration is imminent. This is the only configurable metric in which the Critical threshold value should be smaller than the Warning threshold value. For example, if you set the Warning threshold to 45, an alert is sent when there are 45 days remaining in the license period. The Critical threshold would be less than 45 days, for example 5 days.

For the license expiration metrics, the threshold interval is irrelevant and is set by default to 0. You should set the Warning Threshold to a value that will give you ample time to renew your license. By default, all license expiration metrics have a Warning Threshold of 30 days. By default, the Critical Threshold is configured to 0, which means that a trap is immediately sent upon license expiration.

About Health Monitoring Notification

By default, the Director polls the SG appliances to determine their current state. If the state has changed, Director updates the device status. Other types of notification are also available. Any or all of the following types of notification can be set:

- ❑ SNMP trap: Sends an SNMP trap to all configured management stations.
- ❑ E-mail: Sends e-mail to all persons listed in the Event log properties.
- ❑ Log: Inserts an entry into the Event log. See “Setting Up Event Logging and Notification” on page 15 for more information.

About the General Metrics

The following table lists the metrics displayed in the **Maintenance > Health Monitoring > General** page. The thresholds for these metrics are user-configurable. See “About Health Monitoring” on page 24 for information about thresholds and alert notification.

All threshold intervals are in seconds.

Table 2-2. General Health Monitoring Metrics

| Metric | Units | Default Thresholds/Intervals | Notes |
|-----------------------|------------|---|---|
| CPU Utilization | Percentage | Critical: 95%/120 seconds Warning: 80%/120 seconds | Measures the value of CPU 0 on multi-processor systems-- <i>not</i> the average of all CPU activity. |
| Memory Pressure | Percentage | Critical: 95%/120 seconds Warning: 90%/120 seconds | Memory pressure occurs when memory resources become limited, causing new connections to be delayed. |
| Interface Utilization | Percentage | Critical: 90%/120 seconds Warning: 60%/120 seconds | Measures the traffic (in and out) on the interface to determine if it is approaching the bandwidth maximum. |

About the Licensing Metrics

The following table lists the metrics displayed in the **Maintenance > Health Monitoring > Licensing** page. You can monitor User License utilization metrics and the following license expiration metrics:

- ❑ SGOS Base License: Licenses not listed here are part of the SGOS base license.
- ❑ SSL Proxy
- ❑ SG Client

See [“About License Expiration Metrics”](#) on page 25 for information licensing thresholds.

| Metric | Units | Default Thresholds/Intervals | Notes |
|---------------------|------------|--|---|
| License Utilization | Percentage | Critical: 100%/0 Warning: 90%/0 | For licenses that have user limits, monitors the number of users. |
| License Expiration | Days | Critical: 0 days/0 Warning: 30 days/0 | Warns of impending license expiration. For license expiration metrics, intervals are ignored. See “About the Licensing Metrics” on page 26 for more information. |

About the Status Metrics

The following table lists the metrics displayed in the **Maintenance > Health Monitoring > Status** page. The thresholds for these metrics are *not* user-configurable.

Table 2-3. Status Health Monitoring Metrics

| Metric | Threshold States and Corresponding Values |
|--|---|
| Disk status | Critical: Bad Warning: Removed Offline OK: Not Present Present |
| Temperature Bus temperature CPU temperature | Critical: High-critical Warning: High-warning |
| Fan (The fan metric differs by hardware model, for example, CPU fan, chassis fan) | Critical: Low-critical Warning: Low-warning |

Table 2-3. Status Health Monitoring Metrics (Continued)

| | |
|---|---|
| Voltage Bus Voltage CPU voltage Power Supply voltage | Critical: Critical High-critical Low-critical Warning: High-warning Low-warning |
| ADN Connection Status | OK: Connected Connecting Connection Approved Disabled Not Operational Warning: Approval Pending Mismatching Approval Status Partially Connected Critical: Not Connected Connection Rejected See <i>Volume 5: Advanced Networking</i> for more information about the ADN metrics. |
| ADN Manager Status | OK: No Approvals Pending Not Applicable Warning: Approvals Pending |

Changing Threshold and Notification Properties

The health monitoring threshold and notification properties are set by default. Use the following procedure to modify the current settings.

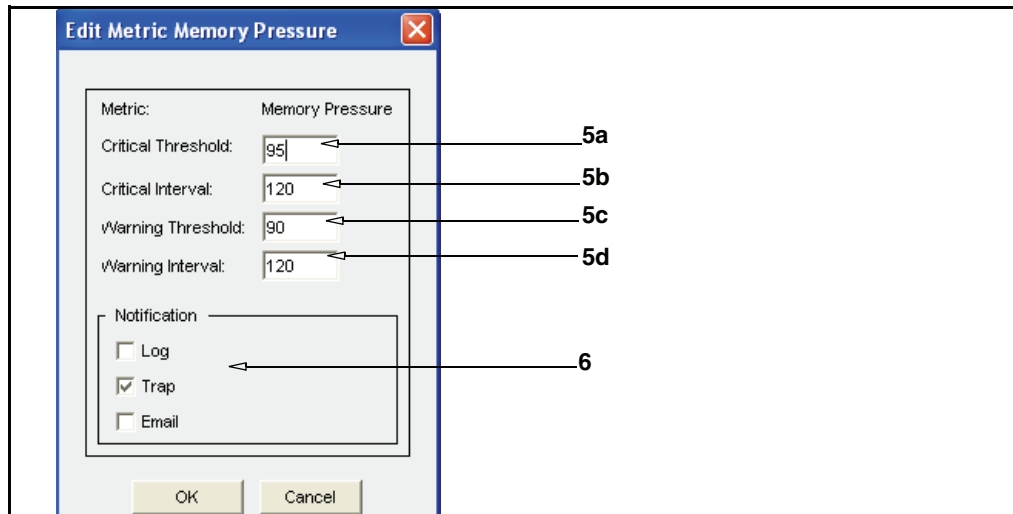
To change the threshold and notification properties:

1. Select **Maintenance > Health Monitoring**.
2. Do one of the following:
 - To change the system resource metrics, select **General**.
 - To change the hardware/environmental/ADN metrics, select **Status**.

Note: You cannot change the threshold values for metrics in the Status tab.

- To change the licensing metrics, select **Licensing**.
3. Select the metric you want to modify.

4. Click **Edit** to modify the threshold and notification settings. The **Edit Health Monitor Setting** dialog displays. (hardware, environmental, and ADN thresholds cannot be modified.)



5. Modify the threshold values:
 - a. To change the critical threshold, enter a new value in the Critical Threshold field.
 - b. To change the critical interval, enter a new value in the Critical Interval field.
 - c. To change the warning threshold, enter a new value in the Warning Threshold field.
 - d. To change the warning interval, enter a new value in the Warning Interval field.
6. Modify the notification settings.
 - **Log** adds an entry to the Event log.
 - **Trap** sends an SNMP trap to all configured management stations.
 - **Email** sends an e-mail to the addresses listed in the Event log properties. See [“Setting Up Event Logging and Notification”](#) on page 15 for more information.
7. Click **OK** to close the Edit Metric dialog.
8. Click **Apply**.

Related CLI Syntax to Modify Threshold and Notification Properties

```
#(config) alert threshold metric_name warning_threshold
warning_interval critical_threshold critical_interval
#(config) alert notification metric_name notification_method
```

where *metric_name* refers to `cpu-utilization`, `license-utilization`, `license-expiration`, `memory-pressure`, or `network-utilization`.

Getting A Quick View of the SG Appliance Health

The Management Console uses the health monitoring metrics to display a visual representation of the overall health state of the SG appliance. The health icon is located in the upper right corner of the Management Console and is always visible.

System health is determined by calculating the “aggregate” health status of the following metrics:

- ❑ CPU Utilization
- ❑ Memory Pressure
- ❑ Network interface utilization
- ❑ Disk status (for all disks)
- ❑ License expiration
- ❑ License “user count” utilization (when applicable)
- ❑ ADN status

The possible health states are **OK**, **Warning**, or **Critical**.

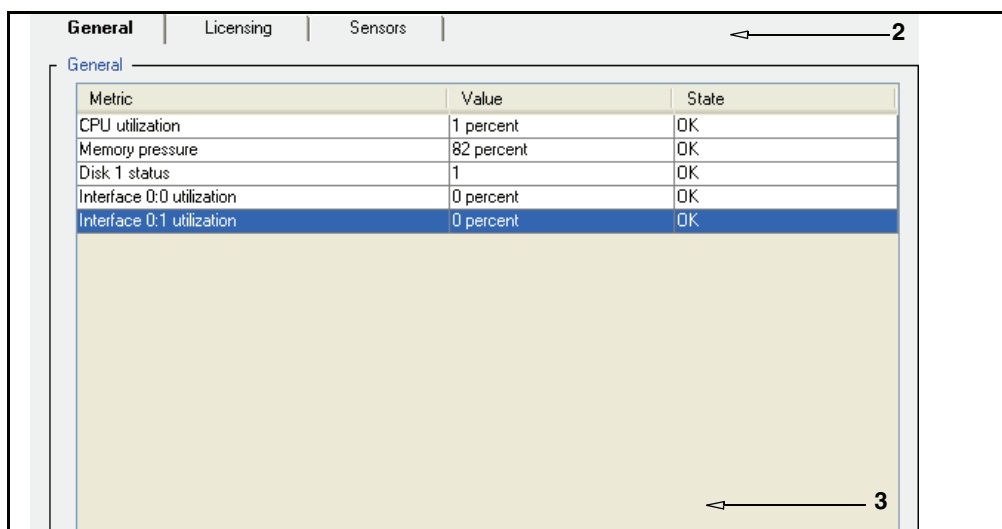
Clicking the health icon displays the **Statistics > Health** page, which lists the current condition of the system’s health monitoring metrics, as described in the next section.

Viewing Health Monitoring Statistics

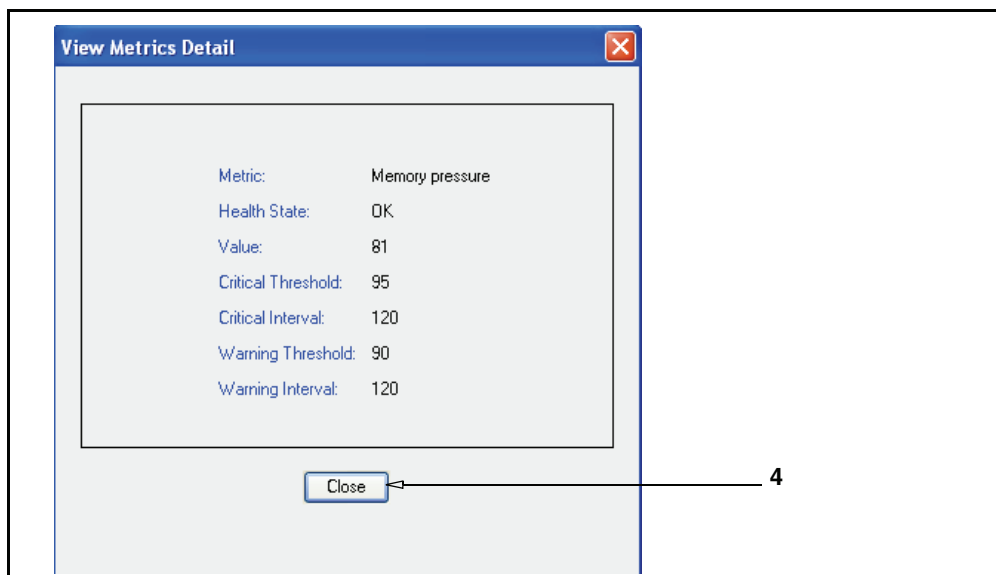
While the health icon presents a quick view of the appliance health, the **Statistics > Health Monitoring** page enables you to get more details about the current state of the health monitoring metrics.

To review the health monitoring statistics:

1. From the Management Console, select **Statistics > Health Monitoring**.



2. Select a health monitoring statistics tab:
 - **General:** Lists the current state of CPU utilization, interface utilization, memory pressure, and disk status metrics.
 - **Licensing:** Lists the current state of license utilization and expiration metrics.
 - **Status:** Lists the current state of all metrics.
3. To get more details about a metric, highlight the metric and click **View**. The **View Metrics Detail** dialog displays.



4. Click Close to close the **View Metrics Detail** dialog.
5. Optional—If you want to modify a metric, highlight the metric and click **Set Thresholds**. The **Maintenance > Health Monitoring** page displays. To modify the metric, follow the procedure describe in “[Changing Threshold and Notification Properties](#)” on page 28.

Related CLI Syntax to View Health Monitoring Statistics

```
SGOS#(config) show system-resource-metrics
```

The show system-resource-metrics command lists the state of the current system resource metrics.

Notification varies by platform. If you try to set notification for a metric that does not support notification, you will see the following error message:

```
Sensor not supported on this platform
```

Depending on the platform, the metrics displayed by the show system-resource-metrics command might differ from the metric names listed in the alert command output. For example, the bus-temperature metric can be shown as motherboard temperature in the show system-resources-metrics output. If you are setting notification from the Management Console, you can verify the category by clicking the Preview button to view the CLI output.

Troubleshooting

If you continue to receive alerts, contact Blue Coat Technical Support. For licensing questions, contact Blue Coat Support Services. It is helpful to obtain a packet capture for CPU, memory pressure, and network interface issues, before calling Technical Support.

Table 2-4. Technical Support and Support Services Contact Information

| | |
|-----------------------------|---|
| Blue Coat Technical Support | http://www.bluecoat.com/support/contact.html |
| Blue Coat Support Services | http://www.bluecoat.com/support/services/index.html |

Chapter 3: Maintaining the SG Appliance

This chapter describes how to maintain the SG appliance; for example, restarting the appliance, restoring system defaults, upgrading the appliance, and reinitializing disks.

This chapter contains the following sections:

- ❑ “Restarting the SG Appliance” on page 33
- ❑ “Restoring System Defaults” on page 34
- ❑ “Clearing the DNS Cache” on page 36
- ❑ “Clearing the Object Cache” on page 36
- ❑ “Clearing the Byte Cache” on page 37
- ❑ “Clearing Trend Statistics” on page 37
- ❑ “Upgrading the SG Appliance” on page 37
- ❑ “Managing SG Appliance Systems” on page 40
- ❑ “Disk Reinitialization” on page 43
- ❑ “Deleting Objects from the SG Appliance” on page 44

Restarting the SG Appliance

The restart options control the restart attributes of the SG appliance if a restart is required because of a system fault.

Important: The default settings of the Restart option suits most systems. Changing them without assistance from Blue Coat Systems Technical Support is not recommended.

Hardware and Software Restart Options

The Restart settings determine if the SG appliance does a faster software-only restart, or a more comprehensive hardware and software restart. The latter can take several minutes longer, depending upon the amount of memory and number of disk drives in the appliance.

The default setting of **Software only** suits most situations. Restarting both the hardware and software is recommended in situations where a hardware fault is suspected.

For information about the Core Image settings, see “[Core Image Restart Options](#)” on page 57.

Note: If you change restart option settings and you want them to apply to the next SG appliance restart, click **Apply**.

To restart the SG appliance:

1. Select **Maintenance > System and disks > Tasks**.

2. In the **Restart** field, select either **Software only** or **Hardware and software**.
3. If you select the **Hardware and software** option, select a system from the **System to run** drop-down list.
The default system is pre-selected.
4. Click **Apply**.
5. Click **Restart now**.
6. Click **OK** to confirm and restart the SG appliance.

Related CLI Syntax to Configure the Hardware/Software Restart Settings

```
SGOS# (config) restart mode {hardware | software}
SGOS# restart abrupt
SGOS# restart regular
SGOS# restart upgrade
```

Restoring System Defaults

SGOS allows you to restore some or all of the system defaults. Use these commands with caution. The `restore-defaults` command deletes most, but not all, system defaults:

- ❑ The `restore-defaults` command with the `factory-defaults` option reinitializes the SG appliance to the original settings it had when it was shipped from the factory.
- ❑ The `restore-defaults` command with the `keep-console` option allows you to restore default settings without losing all IP addresses on the system.

Restore-Defaults

Settings that are deleted when you use the `restore-defaults` command include:

- ❑ All IP addresses (these must be restored before you can access the Management Console again).
- ❑ DNS server addresses (these must be restored through the CLI before you can access the Management Console again).
- ❑ Installable lists.
- ❑ All customized configurations.

- ❑ Third-party vendor licenses, such as SmartFilter or Websense. If you use the `restore-defaults` command after you have installed licenses, and the serial number of your system is configurable (older boxes only), the licenses fails to install and the SG appliance returns to the trial period (if any time is left). To correct the problem, you must configure your serial number and install your license-key again.
 - ❑ Blue Coat trusted certificates.
 - ❑ Original SSH (v1 and v2) host keys (new host keys are regenerated).
- You can use the `force` option to restore defaults without confirmation.

Factory-Defaults

All system settings are deleted when you use the `restore-defaults` command with the `factory-defaults` option.

The only settings that are kept when you use the `restore-defaults` command with the `factory-defaults` option are:

- ❑ Trial period information.
- ❑ The last five installed appliance systems, from which you can pick one for rebooting.

The Setup Console password is also deleted if you use `restore-defaults factory-defaults`. For information on the Setup Console password, refer to *Volume 4: Securing the Blue Coat SG Appliance*.

You can use the `force` option to restore defaults without confirmation.

Keep-Console

Settings that are retained when you use the `restore-defaults` command with the `keep-console` option include:

- ❑ IP interface settings, including VLAN configuration.
- ❑ Default gateway and static routing configuration.
- ❑ Virtual IP address configuration.
- ❑ TCP round trip time settings.
- ❑ Bridging settings.
- ❑ Failover group settings.

Using the `keep-console` option retains the settings for all consoles (Telnet, SSH, HTTP, and HTTPS), whether they are enabled, disabled, or deleted. Administrative access settings retained using the `restore-defaults` command with the `keep-console` option include:

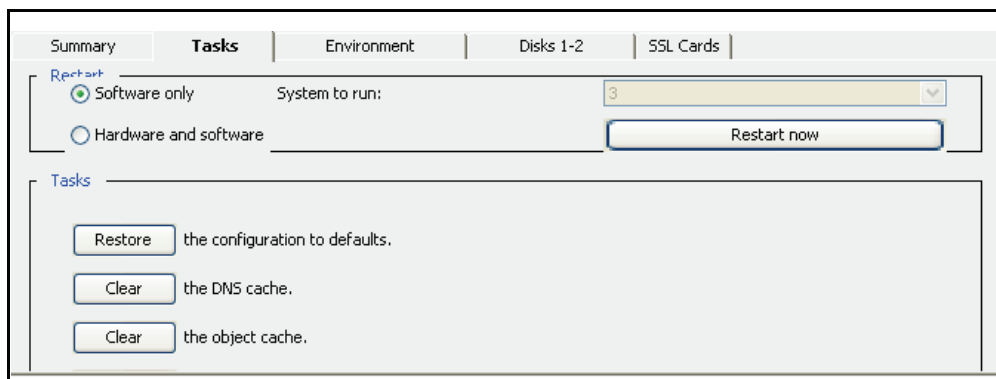
- ❑ Console username and password.
- ❑ Front panel pin number.
- ❑ Console enable password.
- ❑ SSH (v1 and v2) host keys.
- ❑ Keyrings used by secure console services.
- ❑ RIP configurations.

You can also use the `force` option to restore defaults without confirmation.

To restore system defaults:

Note: The `keep-console` and `factory-defaults` options are not available through the Management Console.

1. Select **Maintenance > System and disks > Tasks**.



2. From the **Tasks** field, click **Restore the configuration to defaults**. If you restore the configuration from the Management Console, most settings are lost because you cannot use the `keep-console` option.

The Restore Configuration dialog appears.

3. Click **OK**.

Related CLI Syntax to Restore System Defaults

```
SGOS# restore-defaults [keep-console]
SGOS# restore-defaults [keep-console] force
SGOS# restore-defaults factory-defaults
```

Clearing the DNS Cache

You can clear the DNS cache at any time. You might need to do so if you have experienced a problem with your DNS server or if you have changed your DNS configuration.

To clear the DNS cache:

1. Select **Maintenance > System and disks > Tasks**.
2. In the **Tasks** field, click **Clear** next to “the DNS cache.”
3. Click **OK** to confirm in the Clear system DNS cache dialog that appears.

Related CLI Syntax to Clear the DNS Cache

```
SGOS# clear-cache dns-cache
```

Clearing the Object Cache

You can clear the object cache at any time.

When you clear the cache, all objects in the cache are set to *expired*. The objects are not immediately removed from memory or disk, but a subsequent request for any object requested is retrieved from the source before it is served.

To clear the object cache:

1. Select **Maintenance > System and disks > Tasks**.
2. In the **Tasks** field, click **Clear next** to “the object cache.”
3. Click **OK** to confirm in the Clear cache dialog that appears.

Related CLI Syntax to Clear the Object Cache

```
SGOS# clear-cache object-cache
```

Clearing the Byte Cache

You can clear the byte cache at any time. You might want to do this for testing purposes.

To clear the byte cache:

1. Select **Maintenance > System and disks > Tasks**.
2. In the **Tasks** field, click **Clear** next to “the byte cache.”
3. Click **OK** to confirm in the **Clear Byte Cache** dialog that appears.

Related CLI Syntax to Clear the Byte Cache

```
SGOS# clear-cache byte-cache
```

Troubleshooting Tip

Occasionally, the Management Console might behave incorrectly because of browser caching, particularly if the browser was used to run different versions of the Management Console. This problem might be resolved by clearing the browser cache.

Clearing Trend Statistics

You can clear all persistent trend statistics at any time.

To clear all persistent statistics:

1. Select **Maintenance > System and disks > Tasks**.
2. In the **Tasks** field, click **Clear** next to “the trend statistics.”
3. Click **OK** to confirm in the **Clear Trend Statistics** dialog that appears.

Related CLI Syntax to Clear Trend Statistics

```
SGOS# clear-statistics persistent
```

Upgrading the SG Appliance

When an upgrade to the SGOS software becomes available, you can download it through the Internet and install it. You can also download it to your PC and install it from there.

Important: Enable the auto-detect encoding feature on your browser so that it uses the encoding specified in the console URLs. The browser does not use the auto-detect encoding feature by default. If auto-detect encoding is not enabled, the browser ignores the charset header and uses the native OS language encoding for its display.

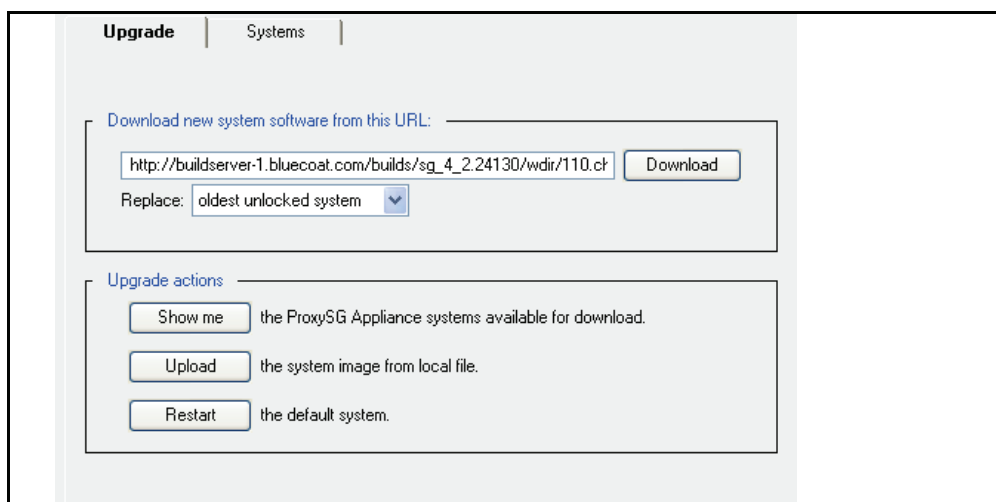
The SG Appliance 5.x Version Upgrade

The appliance must be running version SGOS 4.2.1.6 or later in order to upgrade to SGOS 5.x. You cannot directly upgrade from any previous version.

Note: At least one other system must be unlocked to do the upgrade. If all systems are locked, or all systems except the running system are locked, the **Download** button in the Management Console is disabled. Similarly, the `load upgrade` command in the CLI generates an error.

To upgrade the SG appliance:

1. Select **Maintenance > Upgrade > Upgrade**.

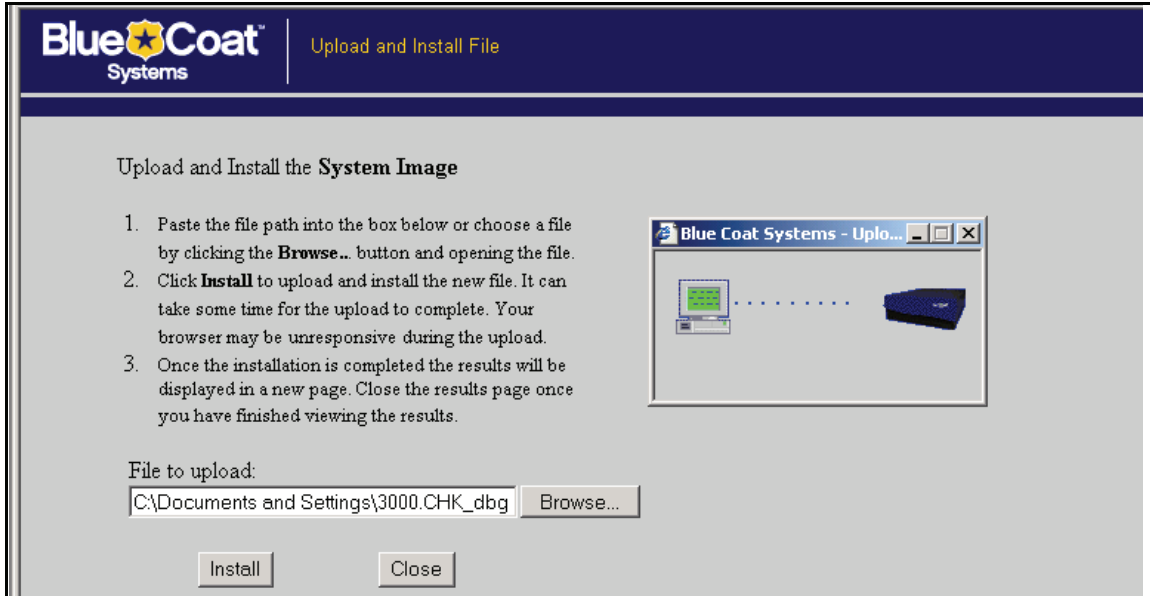


The screenshot shows the 'Upgrade' page in the Management Console. At the top, there are tabs for 'Upgrade' and 'Systems'. Below the tabs, there is a section titled 'Download new system software from this URL:'. This section contains a text input field with the URL 'http://buildserver-1.bluecoat.com/builds/sg_4_2.24130/wdir/110.cf', a 'Download' button, and a 'Replace:' dropdown menu set to 'oldest unlocked system'. Below this is a section titled 'Upgrade actions' with three buttons: 'Show me' (with the description 'the ProxySG Appliance systems available for download.'), 'Upload' (with the description 'the system image from local file.'), and 'Restart' (with the description 'the default system.').

2. Click **Show me** to connect to the Blue Coat download page, follow the instructions, and note the URL of the SGOS upgrade for your system model. Then enter the URL in the **Download new system software from this URL** field and click **Download**.

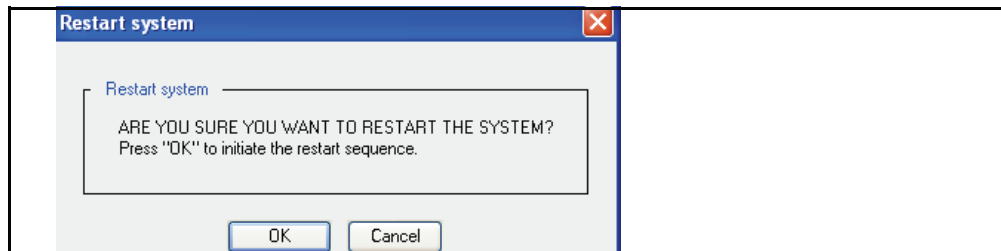
-or-

(Only if you previously downloaded a system image to your PC) Click **Upload** and **Browse** to the file location, then click **Install**. The upload might take several minutes.



3. (Optional) Select the system to replace in the **Replace** drop-down list. If you uploaded an image from your PC, refresh the Systems pane to see the new system image.
4. Click **Restart**.

The **Restart system** dialog displays.



5. Click **OK** to reboot the SG appliance to the default system.

Related CLI Syntax to Upgrade the SGOS Software

```
SGOS# (config) upgrade-path url
```

where *url* is the location of the SGOS upgrade image.

```
SGOS# (config) exit
```

```
SGOS# load upgrade [ignore-warnings]
```

where *ignore-warnings* allows you to force an upgrade even if you receive policy deprecation warnings. Using the `load upgrade ignore-warnings` command to force an upgrade while the system emits deprecation warnings results in a policy load failure; all traffic is allowed or denied according to default policy.

```
SGOS# restart upgrade
```

Troubleshooting Tip

If the SG appliance does not come up after rebooting and the serial port is connected to a terminal server (terminal concentrator), try the following:

- ❑ Have an active session open on the terminal server, noting any traffic (characters) being output.
- ❑ Unplug the terminal server from the appliance in case it is causing a problem (such as bad cabling).

Managing SG Appliance Systems

The SG appliance **Systems** tab displays the five available systems. Empty systems are indicated by the word **Empty**.

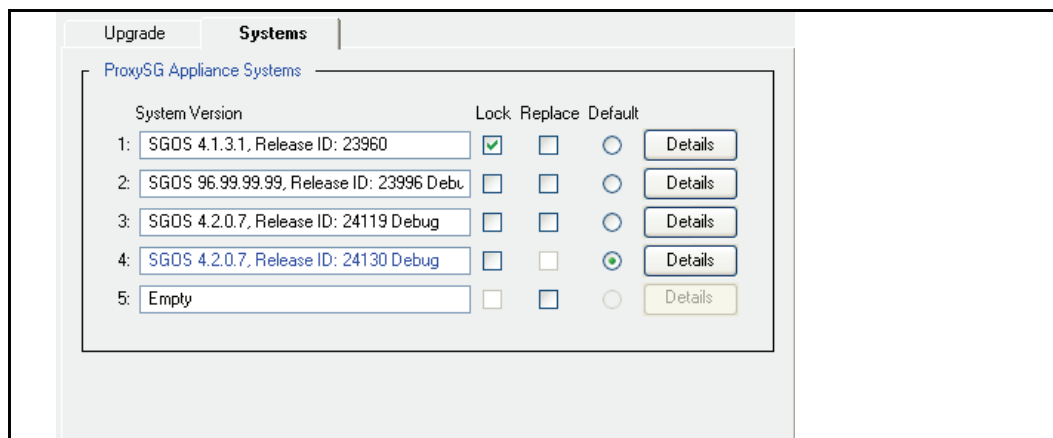
The system currently running is highlighted in blue and cannot be replaced or deleted.

From this screen, you can:

- ❑ Select the SGOS system version to boot.
- ❑ Lock one or more of the available SGOS system versions.
- ❑ Select the SGOS system version to be replaced.
- ❑ Delete one or more of the available SGOS system versions (CLI only).
- ❑ View details of the available SGOS system versions.

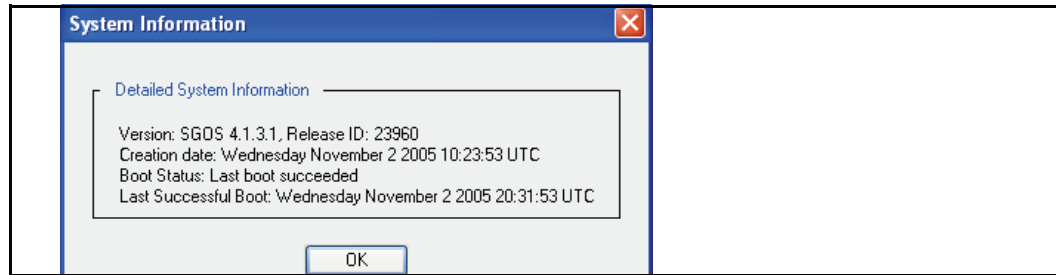
To view SGOS system replacement options:

Select **Maintenance > Upgrade > Systems**.



To view details for an SGOS system version:

1. Select **Maintenance > Upgrade > Systems**.
2. Click **Details** next to the system for which you want to view detailed information; click **OK** when you are finished.



To view details for an SGOS system version:

At the command prompt:

```
SGOS> show installed-systems
```

Example Session

```
SGOS> show installed-systems
```

SG Appliance Systems

1. Version: SGOS 4.2.1.1, Release ID: 25460
Thursday April 6 2006 08:49:55 UTC, Lock Status: Locked
Boot Status: Last boot succeeded, Last Successful Boot: Thursday
April 6 2006 17:33:19 UTC
2. Version: SGOS 4.2.1.1, Release ID: 25552 Debug
Friday April 14 2006 08:56:55 UTC, Lock Status: Unlocked
Boot Status: Last boot succeeded, Last Successful Boot: Friday April
14 2006 16:57:18 UTC
3. Version: N/A, Release ID: N/A (EMPTY)
No Timestamp, Lock Status: Unlocked
Boot Status: Unknown, Last Successful Boot: Unknown
4. Version: N/A, Release ID: N/A (EMPTY)
No Timestamp, Lock Status: Unlocked
Boot Status: Unknown, Last Successful Boot: Unknown
5. Version: N/A, Release ID: N/A (EMPTY)
No Timestamp, Lock Status: Unlocked
Boot Status: Unknown, Last Successful Boot: Unknown
Default system to run on next hardware restart: 2
Default replacement being used. (oldest unlocked system)
Current running system: 2

When a new system is loaded, only the system number that was replaced is changed.

The ordering of the rest of the systems remains unchanged.

Setting the Default Boot System

This setting allows you to select the system to be booted on the next hardware restart. If a system starts successfully, it is set as the default boot system. If a system fails to boot, the next most recent system that booted successfully becomes the default boot system.

To set the SG appliance to run on the next hardware restart:

1. Select **Maintenance > Upgrade > Systems**.
2. Select the preferred System version in the **Default** column.
3. Click **Apply**.

Note: An empty system cannot be specified as default, and only one system can be specified as the default system.

Related CLI Syntax to Set the Default Boot System

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) default system_number
```

Locking and Unlocking SG Appliance Systems

Any system can be locked, except a system that has been selected for replacement. If all systems, or all systems except the current system, are locked, the SG appliance cannot load a new system.

If a system is locked, it cannot be replaced or deleted.

To lock a system:

1. Select **Maintenance > Upgrade > Systems**.
2. Select the system(s) to lock in the **Lock** column.
3. Click **Apply**.

To unlock a system:

1. Select **Maintenance > Upgrade > Systems**.
2. Deselect the system(s) to unlock in the **Lock** column.
3. Click **Apply**.

To unlock a system:

Related CLI Syntax for Locking A System

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) lock system_number
```

To unlock:

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) no lock system_number
```

Replacing an SG Appliance System

You can specify the system to be replaced when a new system is downloaded. If no system is specified, the oldest unlocked system is replaced by default. You cannot specify a locked system for replacement.

To specify the system to replace:

1. Select **Maintenance > Upgrade > Systems**.
2. Select the system to replace in the **Replace** column.
3. Click **Apply**.

Related CLI Syntax to Specify the System to Replace

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) replace system_number
```

Deleting an SG Appliance System

You can delete any of the system versions except the current running system. A locked system must be unlocked before it can be deleted. If the system you want to delete is the default boot system, you need to select a new default boot system before the system can be deleted.

You cannot delete a system version through the Management Console; you must use the CLI.

To delete a system:

At the (config) command prompt:

```
SGOS#(config) installed-systems
SGOS#(config installed-systems) delete system_number
      where system_number is the system you want to delete.
```

Disk Reinitialization

You can reinitialize disks on a multi-disk SG appliance. You cannot reinitialize the disk on a single-disk SG appliance. If you suspect a disk fault in a single-disk system, contact Blue Coat Technical Support for assistance.

Note: If a disk containing an unmirrored event or access log is reinitialized, the logs are lost. Similarly, if two disks containing mirrored copies of the logs are reinitialized, both copies of the logs are lost.

Multi-Disk SG Appliances

On a multi-disk SG appliance, the master disk is the leftmost valid disk. *Valid* means that the disk is online, has been properly initialized, and is not marked as invalid or unusable. If the current master disk is taken offline, reinitialized, or declared invalid or unusable, the leftmost valid disk that has not been reinitialized since restart becomes the master disk. Thus, as disks are reinitialized in sequence, a point is reached where no disk can be chosen as the master. At this point, the current master disk is the last disk. If this disk is taken offline, reinitialized, or declared invalid or unusable, the SG appliance is restarted.

On a multi-disk SG appliance, a disk is reinitialized by setting it to empty and copying pre-boot programs, boot programs, and starter programs, and system images from the master disk to the reinitialized disk.

Reinitialization is done online without rebooting the system. (For more information, refer to the `#disk` command in the *Volume 11: Command Line Interface Reference*.) SGOS operations, in turn, are not affected, although during the time the disk is being reinitialized, that disk is not available for caching. Only the master disk reinitialization restarts the SG appliance.

Only persistent objects are copied to a newly-reinitialized disk. This is usually not a problem because most of these objects are replicated or mirrored. If the reinitialized disk contained one copy of these objects (which is lost), another disk contains another copy.

You cannot reinitialize all of the SG appliance disks over a very short period of time. Attempting to reinitialize the last disk in a system before critical components can be replicated to other disks in the system causes a warning message to appear.

Immediately after reinitialization is complete, the SG appliance automatically starts using the reinitialized disk for caching.

Single-Disk SG Appliance

The disk on a single-disk SG appliance cannot be reinitialized by the customer. If you suspect a disk fault in a single-disk SG appliance, contact Blue Coat Technical Support for assistance.

Deleting Objects from the SG Appliance

The ability to delete either individual or multiple objects from the SG appliance makes it easy to delete stale or unused data and make the best use of the storage in your system.

Note: The maximum number of objects that can be stored in an SG appliance is affected by a number of factors, including the SGOS version it is running and the hardware platform series.

This feature is not available in the Management Console. Use the CLI instead.

To delete a single object from the SG appliance:

At the (config) prompt, enter the following command:

```
SGOS#(config) content delete url url
```

To delete multiple objects from the SG appliance:

At the (config) prompt, enter the following command:

```
SGOS#(config) content delete regex regex
```

Chapter 4: Diagnostics

Blue Coat Systems has a number of resources to provide diagnostic information:

- ❑ Heartbeats: Enabled by default, Heartbeats (statistics) are a diagnostic tool used by Blue Coat, allowing them to proactively monitor the health of appliances.
- ❑ Core images: Created when there is an unexpected system restart. This stores the system state at the time of the restart, enhancing the ability for Blue Coat to determine the root cause of the restart.
- ❑ SysInfo (System Information): SysInfo provides a snapshot of statistics and events on the SG appliance.
- ❑ PCAP: An onboard packet capture utility that captures packets of Ethernet frames going in or out of an SG appliance.
- ❑ Policy trace: A policy trace can provide debugging information on policy transactions. This is helpful, even when policy is not the issue. For information on using policy tracing, refer to *Volume 10: Content Policy Language Guide*.
- ❑ Event Logging: The event log files contain messages generated by software or hardware events encountered by the appliance. For information on configuring event logging, see “[Setting Up Event Logging and Notification](#)” on page 15.
- ❑ Access Logging: Access logs allow for analysis of Quality of Service, content retrieved, and other troubleshooting. For information on Access Logging, refer to *Volume 8: Access Logging*.
- ❑ CPU Monitoring: With CPU monitoring enabled, you can determine what types of functions are taking up the majority of the CPU.

To test connectivity, use the following commands from the enable prompt:

- ❑ ping: Verifies that a particular IP address exists and is responding to requests.
- ❑ traceroute: Traces the route from the current host to the specified destination host.
- ❑ test http get *path_to_URL*: Makes a request through the same code paths as a proxied client.
- ❑ display *path_to_URL*: Makes a direct request (bypassing the cache).
- ❑ show services: Verifies the port of the Management Console configuration.
- ❑ show policy: Verifies if policy is controlling the Management Console.

For information on using these commands, refer to Chapter 2: “Standard and Privileged Mode Commands” in the *Blue Coat ProxySG Command Line Reference*.

Note: If you cannot access the Management Console at all, be sure that you are using HTTPS (`https://SG_IP_address:8082`). If you want to use HTTP, you must explicitly enable it before you can access the Management Console.

This chapter discusses the following topics:

- ❑ “Diagnostic Reporting (Service Information)” on page 46 (This includes taking snapshots of the system.)
- ❑ “Packet Capturing (the Job Utility)” on page 52
- ❑ “Core Image Restart Options” on page 57
- ❑ “Diagnostic Reporting (Heartbeats)” on page 58
- ❑ “Diagnostic Reporting (CPU Monitoring)” on page 59

If the SG appliance does not appear to work correctly and you are unable to diagnose the problem, contact Blue Coat Technical Support.

Diagnostic Reporting (Service Information)

The service information options allow you to send service information to Blue Coat using either the Management Console or the CLI. You can select the information to send, send the information, view the status of current transactions, and cancel current transactions. You can also send service information automatically in case of a crash.

Sending Service Information Automatically

Enabling automatic service information allows you to enable the transfer of relevant service information automatically whenever a crash occurs. This saves you from initiating the transfer, and increases the amount of service information that Blue Coat can use to solve the problem. The core image, system configuration, and event log are system-use statistics that are sent for analysis. If a packet capture exists, it is also sent.

The auto-send feature requires that a valid Service Request is entered. If you do not have a Service Request open you must first contact Blue Coat Technical Support.

Important: A core image and packet capture can contain sensitive information—for example, parts of an HTTP request or response. The transfer to Blue Coat is encrypted, and therefore secure; however, if you do not want potentially sensitive information to be sent to Blue Coat automatically, do not enable the automatic service information feature.

To send service information automatically:

1. Select **Maintenance > Service Information > Send Information > General**.

The screenshot shows the 'Send Service Information' configuration page. The 'General' tab is selected. Under 'Auto Send Settings', the 'Enable auto-send' checkbox is unchecked. The 'Auto Send Service Request Number' field is empty. Under 'Bandwidth Class Settings', the 'Service Information Bandwidth Class' dropdown is set to '<none>'.

2. To send core image service information to Blue Coat automatically, select **Enable auto-send**.

3. Enter the service-request number that you received from a Technical Support representative into the **Auto Send Service Request Number** field (the service-request number is in the form xx-xxxxxxx or x-xxxxxxx).
4. Click **Apply** to commit the changes to the SG appliance.
5. (Optional) To clear the service-request number, clear the **Auto Send Service Request Number** field and click **Apply**.

Related CLI Syntax to Send Service Information

To send service information automatically:

1. To enable (or disable) the automatic service information feature, enter the following commands at the (config) command prompt:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(diagnostics service-info) auto {enable | disable}
SGOS#(diagnostics service-info) auto sr-number sr_number
```

2. (Optional) To clear the service-request number, enter the following command:

```
SGOS#(diagnostics service-info) auto no sr-number
```

Managing the Bandwidth for Service Information

You can control the allocation of available bandwidth for sending service information. Some service information items are large, and you might want to limit the bandwidth used by the transfer. Changing to a new bandwidth management class does not affect service information transfers already in progress. However, changing the details of the bandwidth management class used for service information, such as changing the minimum or maximum bandwidth settings, affects transfers already in progress if that class was selected prior to initiating the transfer.

Note: Before you can manage the bandwidth for the automatic service information feature, you must first create an appropriate bandwidth-management class. Refer to *Volume 5: Advanced Networking* for information about creating and configuring bandwidth classes.

To manage bandwidth for service information:

1. Select **Maintenance > Service Information > Send Information > General**.
2. To manage the bandwidth of automatic service information, select a bandwidth class from the **Service Information Bandwidth Class** drop-down menu.
3. Click **Apply** to commit the changes to the SG appliance.
4. (Optional) To disable the bandwidth-management of service information, select **none** from the **Service Information Bandwidth Class** drop-down menu; click **Apply**.

Related CLI Syntax to Manage Bandwidth for Service Information

```
SGOS#(diagnostics service-info) bandwidth-class bw_class_name
```

Configure Service Information Settings

The service information options allow you to send service information to Blue Coat using either the Management Console or the CLI. You can select the information to send, send the information, view the status of current transactions, and cancel current transactions using either the Management Console or the CLI. For information about sending service information automatically, see “Sending Service Information Automatically” on page 46.

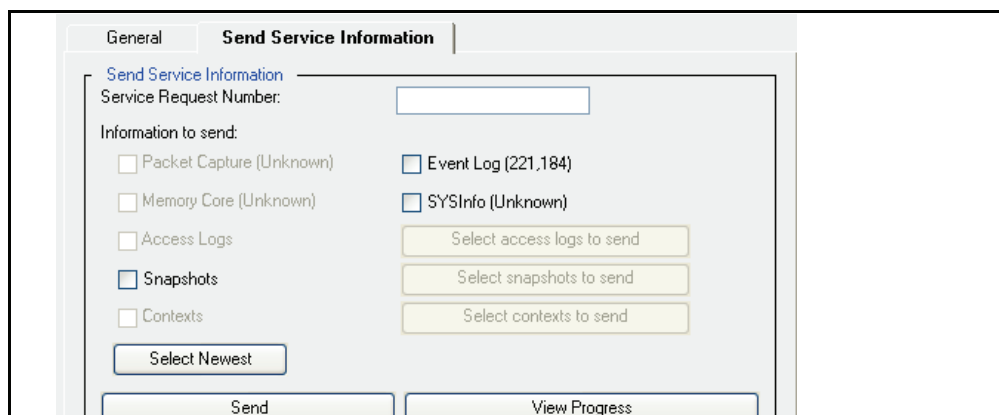
Important: You must specify a service-request number before you can send service information. See Blue Coat Technical Support at: <http://www.bluecoat.com/support/index.html> for details on opening a service request ticket.

The following list details information that you can send:

- Packet Capture
- Event Log
- Memory Core
- SYSInfo
- Access Logs (can specify multiple)
- Snapshots (can specify multiple)
- Contexts (can specify multiple)

To send service information:

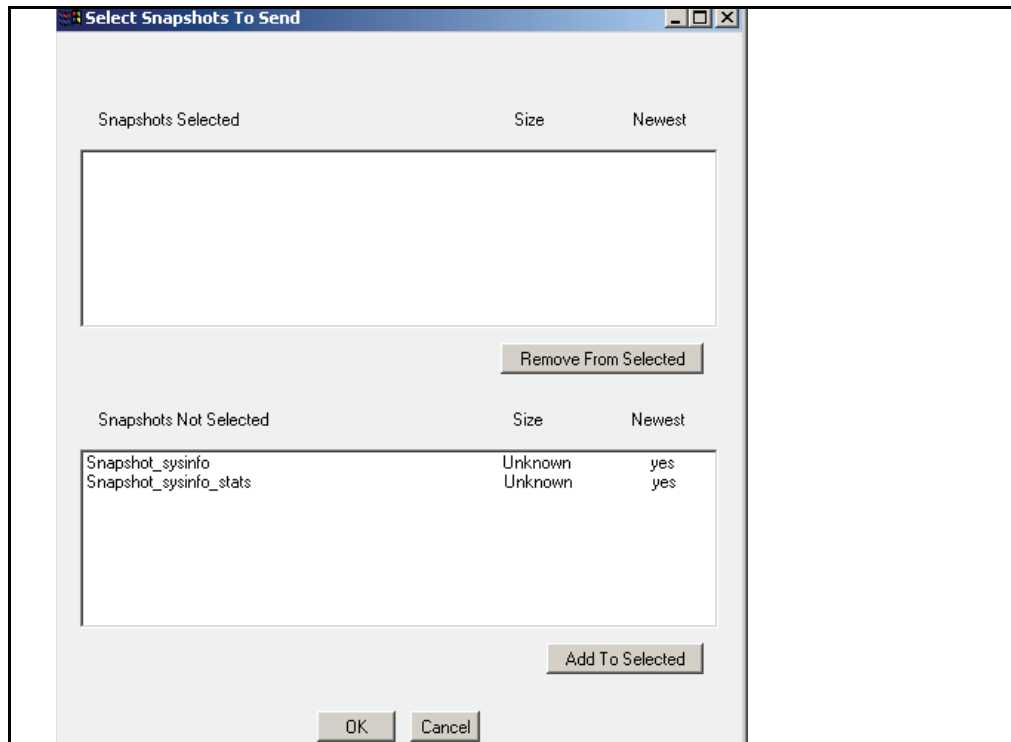
1. Select **Maintenance > Service Information > Send Information > Send Service Information**.



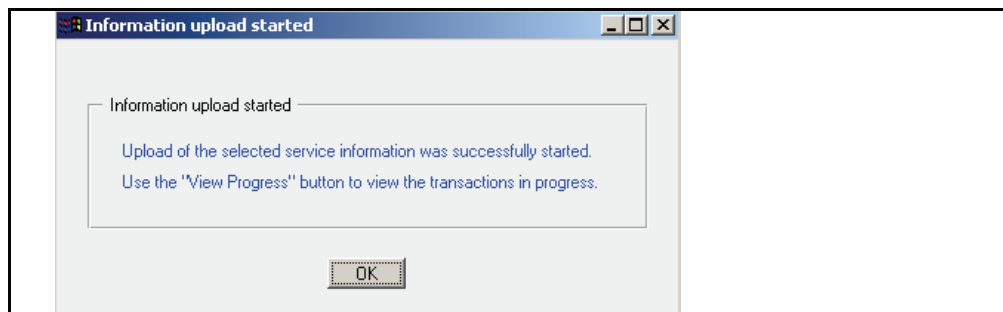
2. Enter the service-request number that you received from a Technical Support representative (the service-request number is in the form xx-xxxxxxx or x-xxxxxxx).
3. Select the appropriate check boxes (as indicated by a Technical Support representative) in the **Information to send** field.

Note: Options for items that you do not have on your system are grayed out and cannot be selected.

4. (Optional) If you select **Access Logs**, **Snapshots**, or **Contexts**, you must also click **Select access logs to send**, **Select snapshots to send**, or **Select contexts to send** and complete the following steps in the corresponding dialog that appears:



- a. To select information to send, highlight the appropriate selection in the **Access Logs/Snapshots/Contexts Not Selected** field and click **Add to Selected**.
 - b. To remove information from the **Access Logs/Snapshots/Contexts Selected** field, highlight the appropriate selection and click **Remove from Selected**.
 - c. Click **Ok**.
5. Click **Send**.
 6. Click **Ok** in the Information upload started dialog that appears.



7. Click **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Send Service Information

```
SGOS#(diagnostics service-info) [subcommands]
```

Creating and Editing Snapshot Jobs

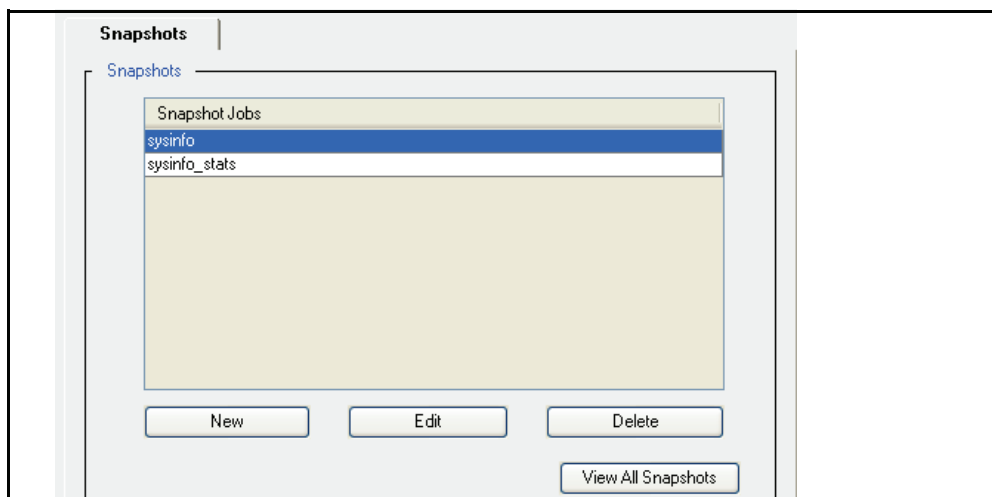
The snapshot subsystem periodically pulls a specified console URL and stores it in a repository, offering valuable resources for Blue Coat customer support in diagnosing problems.

By default, two snapshots are defined. The first takes a snapshot of the system information URL once every 24 hours. The second snapshot takes an hourly snapshot of the system information statistics. Both of these snapshot jobs keep the last 30 snapshots.

Determining which console URL to poll, the time period between snapshots, and how many snapshots to keep are all configurable options for each snapshot job.

To create a new snapshot job:

1. Select **Maintenance > Service Information > Snapshots**.



2. Click **New**.
3. Enter a snapshot job into the Add list item dialog that displays; click **Ok**.
4. Click **Apply** to commit the changes to the SG appliance.
5. (Optional) To view snapshot job information, click **View All Snapshots**. Close the window that opens when you are finished viewing.

Related CLI Syntax to Send Service Information

```
SGOS#(config diagnostics) snapshot create snapshot_name
```

To edit an existing snapshot job:

1. Select **Maintenance > Service Information > Snapshots**.
2. Select the snapshot job you want to edit (highlight it).
3. Click **Edit**.

The Edit Snapshot dialog displays.

4. Enter the following information into the Edit Snapshot fields:
 - a. **Target:** Enter the object to snapshot.
 - b. **Interval (minutes):** Enter the interval between snapshot reports.
 - c. **Total Number To Take:** Enter the total number of snapshots to take or select **Infinite** to take an infinite number of snapshots.
 - d. **Maximum Number To Store:** Enter the maximum number of snapshots to store.
 - e. **Enabled:** Select this to enable this snapshot job or deselect it to disable this snapshot job.
5. (Optional) Click **View URL List** to open a window displaying a list of URLs; close the window when you are finished viewing.
6. (Optional) Click **View Snapshots** to open a window displaying snapshot information; close the window when you are finished viewing.
7. (Optional) Click **Clear Snapshots** to clear all stored snapshot reports.

Related CLI Syntax to Edit an Existing Snapshot Job

- ❑ To enter configuration mode:
SGOS#(config) **diagnostics**
- ❑ The following subcommands are available:
SGOS#(config diagnostics) **snapshot edit snapshot_name**
SGOS#(config snapshot snapshot_name) {**disable** | **enable**}
SGOS#(config snapshot snapshot_name) **interval** minutes
SGOS#(config snapshot snapshot_name) **keep** number_to_keep (from 1 - 100)
SGOS#(config snapshot snapshot_name) **take** {**infinite** | number_to_take}
SGOS#(config snapshot snapshot_name) **target** object_to_fetch

Packet Capturing (the Job Utility)

You can capture packets of Ethernet frames going into or leaving an SG appliance. Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. The maximum PCAP size allowed is 100MB. Any packet filters must be defined before a capture is initiated, and the current packet filter can only be modified if no capture is in progress.

The `pcap` utility captures all received packets that are either directly addressed to the SG appliance through an interface's MAC address or through an interface's broadcast address. The utility also captures transmitted packets that are sent from the appliance. The collected data can then be transferred to the desktop or to Blue Coat for analysis.

Note: Packet capturing increases the amount of processor usage performed in TCP/IP.

To analyze captured packet data, you must have a tool that reads Packet Sniffer Pro 1.1 files (for example, Ethereal or Packet Sniffer Pro 3.0).

PCAP File Name Format

The name of a downloaded packet capture file has the format: `bluecoat_date_filter-expression.cap`, revealing the date and time (UTC) of the packet capture and any filter expressions used. Because the filter expression can contain characters that are not supported by a file system, a translation can occur. The following characters are not translated:

- ❑ Alphanumeric characters (a-z, A-Z, 0-9)
- ❑ Periods (.)

Characters that are translated are:

- ❑ Space (replaced by an underscore)
- ❑ All other characters (including the underscore and dash) are replaced by a dash followed by the ASCII equivalent; for example, a dash is translated to `-2D` and an ampersand (&) to `-26`.

Common PCAP Filter Expressions

Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. PCAP filter expressions can be defined in the Management Console or the CLI. Below are examples of filter expressions; for PCAP configuration instructions, see [“Configuring Packet Capturing”](#) on page 53.

Some common filter expressions for the Management Console and CLI are listed below. The filter uses the Berkeley Packet Filter format (BPF), which is also used by the `tcpdump` program. A few simple examples are provided below. If filters with greater complexity are required, you can find many resources on the Internet and in books that describe the BPF filter syntax.

Note: Some qualifiers must be escaped with a backslash because their identifiers are also keywords within the filter expression parser.

- ❑ `ip proto protocol`
where *protocol* is a number or name (icmp, udp, tcp).
- ❑ `ether proto protocol`
where *protocol* can be a number or name (ip, arp, rarp).

Table 4-1. PCAP Filter Expressions

| Filter Expression | Packets Captured |
|--|---|
| <code>ip host 10.25.36.47</code> | Captures packets from a specific host with IP address 10.25.36.47. |
| <code>not ip host 10.25.36.47</code> | Captures packets from all IP addresses except 10.25.36.47. |
| <code>ip host 10.25.36.47 and ip host 10.25.36.48</code> | Captures packets sent between two IP addresses: 10.25.36.47 and 10.25.36.48. Packets sent from one of these addresses to other IP addresses are not filtered. |
| <code>ether host 00:e0:81:01:f8:fc</code> | Captures packets to or from MAC address 00:e0:81:01:f8:fc:. |
| <code>port 80</code> | Captures packets to or from port 80. |
| <code>ip sr www.bluecoat.com and ether broadcast</code> | Captures packets that have IP source of www.bluecoat.com and ethernet broadcast destination. |

Using Filter Expressions in the CLI

To add a filter to the CLI, use the command:

```
SGOS# pcap filter expr parameters
```

To remove a filter, use the command:

```
SGOS# pcap filter <enter>
```

Important: Define CLI filter expr parameters with double-quotes to avoid confusion with special characters. For example, a space is interpreted by the CLI as an additional parameter, but the CLI accepts only one parameter for the filter expression. Enclosing the entire filter expression in quotations allows multiple spaces in the filter expression.

Configuring Packet Capturing

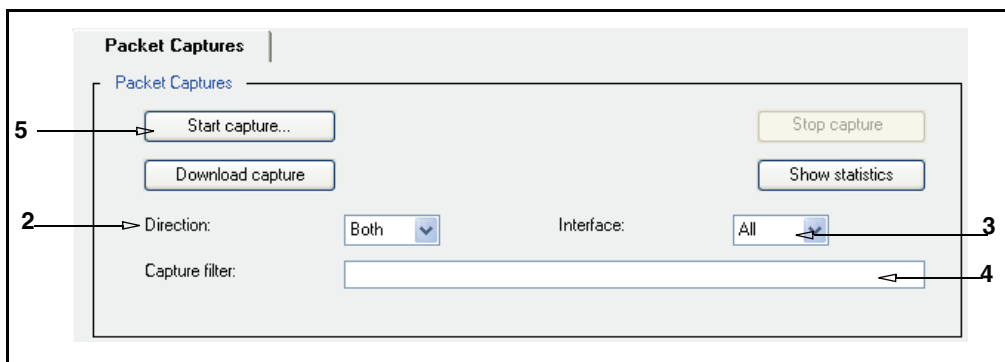
Use the following procedures to configure packet capturing. If a download of the captured packets is requested, packet capturing is implicitly stopped. In addition to starting and stopping packet capture, a filter expression can be configured to control which packets are captured. For information on configuring a PCAP filter, see "[Common PCAP Filter Expressions](#)" above.

Note: Requesting a packet capture download stops packet capturing.

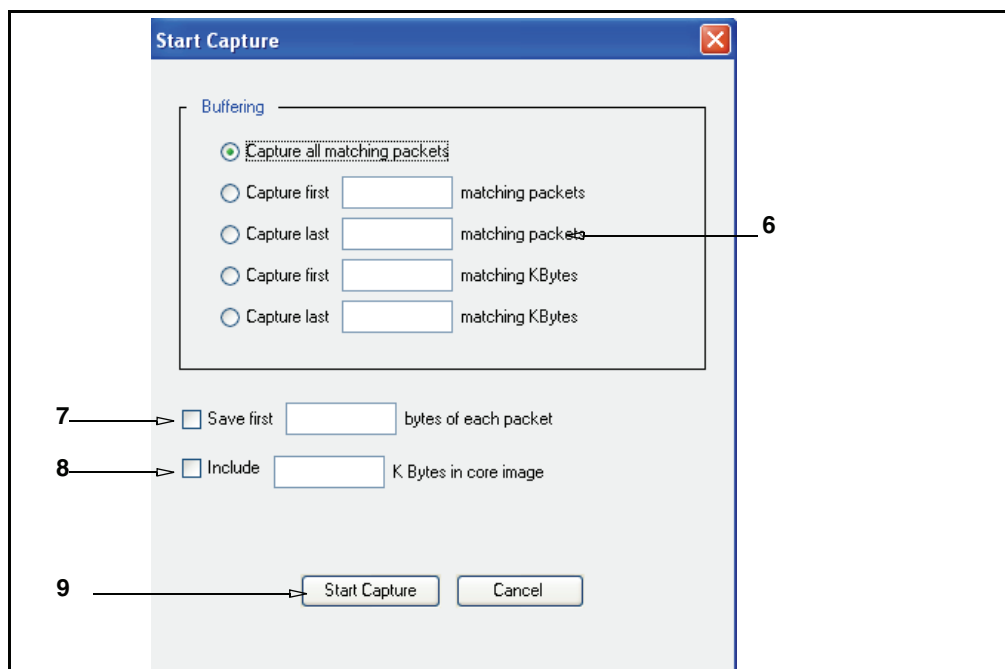
To analyze captured packet data, you must have a tool that reads Packet Sniffer Pro 1.1 files (for example, Ethereal or Packet Sniffer Pro 3.0).

To enable, stop, and download packet captures:

1. Select **Maintenance > Service Information > Packet Captures**.

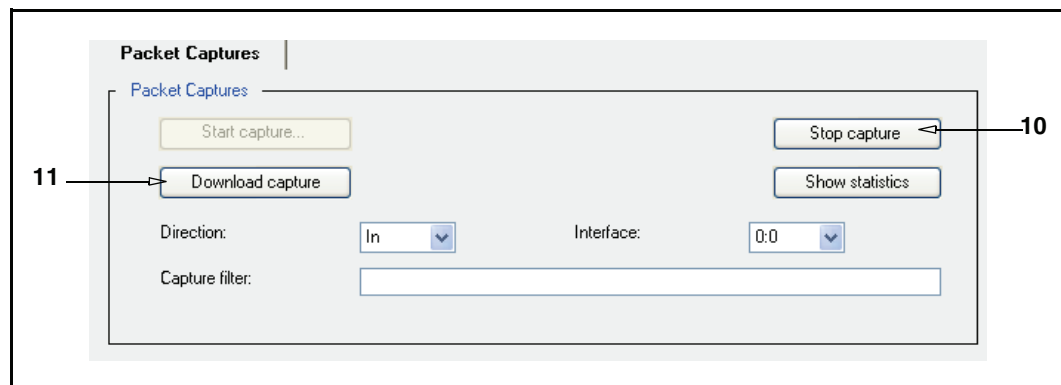


2. In the **Direction** drop-down list, select the capture direction: **in**, **out**, or **both**.
3. In the **Interface** drop-down list, select the interface on which to capture.
4. To define or change the PCAP filter expression, enter the filter information into the **Capture filter** field. (See [“Common PCAP Filter Expressions”](#) on page 52 for information about PCAP filter expressions for this field.) To remove the filter, clear this field.
5. Click **Start Capture**. The Start Capture dialog displays.



6. Set the buffer size and method by choosing one of the following radio buttons:
 - a. Capture all matching packets.
 - b. Capture first n matching packets. Enter the number of matching packets (n) to capture. If the number of packets reaches this limit, packet capturing stops automatically. The value must be between 1 and 1000000.
 - c. Capture last n matching packets. Enter the number of matching packets (n) to capture. Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is stopped. The value must be between 1 and 1000000.
 - d. Capture first n matching Kilobytes. Enter the number of kilobytes (n) to capture. If the buffer reaches this limit, packet capturing stops automatically. The value must be between 1 and 102400.
 - e. Capture last n matching Kilobytes. Enter the number of kilobytes (n) to capture. Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is stopped. The value must be between 1 and 102400.
7. Optional—To truncate the number of bytes saved in each frame, enter a number in the **Save first n bytes of each packet** field. When configured, `pcap` collects, at most, n bytes of packets from each frame when writing to disk. The range is 1 to 65535.
8. Optional—To specify the number of kilobytes of packets kept in a core image, enter a value in the **Include n K Bytes in core image** field. You can capture packets and include them along with a core image. This is extremely useful if a certain pattern of packets causes the unit to restart unexpectedly. The core image size must be between 0 and 102400. By default, no packets are kept in the core image.
9. To start the capture, click the **Start Capture** button. The Start Capture dialog closes. Note that the **Start captures** button in the **Packet Captures** tab is now grayed out because packet capturing is already started.

You do not have to click **Apply** because all changes are applied when you start the packet capture.



10. To stop the capture, click the **Stop capture** button. This button is grayed out if a packet capture is already stopped.
11. To download the capture, click the **Download capture** button. This button is grayed out if no file is available for downloading.

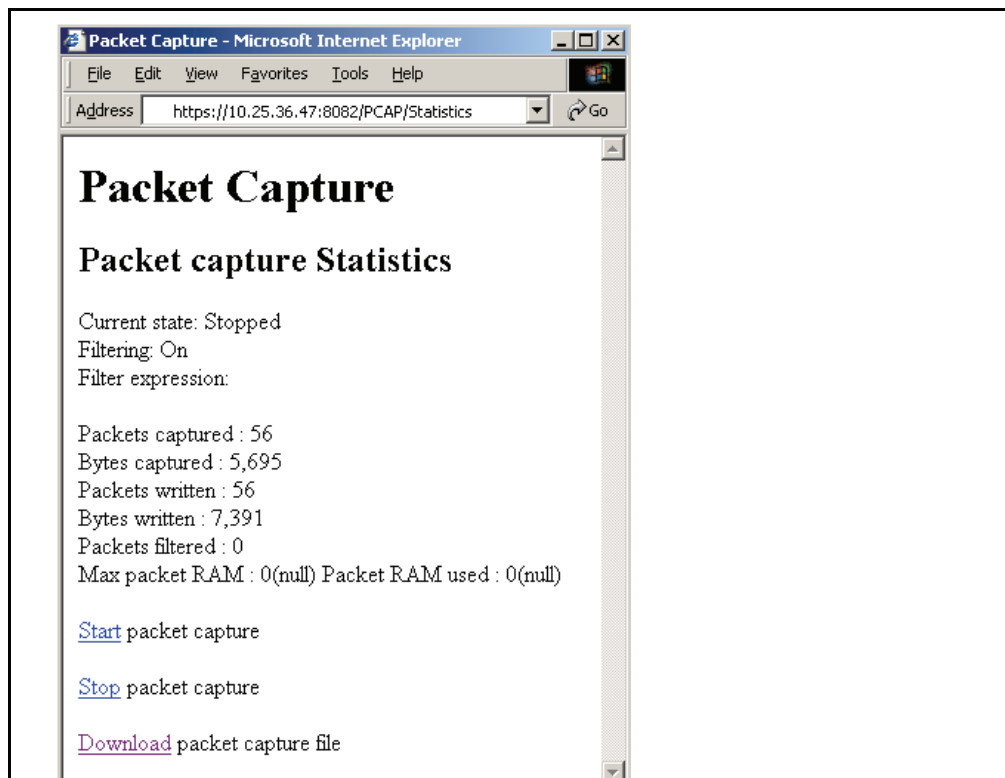
Related CLI Syntax to Define Packet Capturing Settings

```
SGOS# pcap filter parameters
SGOS# pcap start [subcommands]
```

To start, stop, and download packet captures through a browser:

1. Start your Web browser.
2. Enter the URL: `https://appliance_IP_address:8082/PCAP/Statistics` and log on to the appliance as needed.

The Packet Capture Web page opens.



3. Select the desired action: **Start packet capture**, **Stop packet capture**, **Download packet capture file**.

You can also use the following URLs to configure these individually:

- ❑ To start packet capturing, use this URL:
`https://SG_IP_address:8082/PCAP/start`
- ❑ To stop packet capturing, use this URL:
`https://SG_IP_address:8082/PCAP/stop`
- ❑ To download packet capturing data, use this URL:
`https://SG_IP_address:8082/PCAP/bluecoat.cap`

Viewing Current Packet Capture Data

Use the following procedures to display current capture information from the SG appliance.

To view current packet capture statistics:

1. Select **Maintenance > Service Information > Packet Captures**.
2. To view the packet capture statistics, click the **Show statistics** button.

A window opens displaying the statistics on the current packet capture settings. Close the window when you are finished viewing the statistics.

Related CLI Syntax to View Packet Capture Data

```
SGOS# pcap info
```

Uploading Packet Capture Data

Use the following command to transfer packet capture data from the SG appliance to an FTP site. You cannot use the Management Console. After uploading is complete, you can analyze the packet capture data.

```
SGOS# pcap transfer ftp://url/path/filename.cap username password
```

Specify a username and password, if the FTP server requires these. The username and password must be recognized by the FTP server.

Core Image Restart Options

This option specifies how much detail is logged to disk when a system is restarted. Although this information is not visible to the user, Blue Coat Technical Support uses it in resolving system problems. The more detail logged, the longer it takes the SG appliance to restart. There are three options:

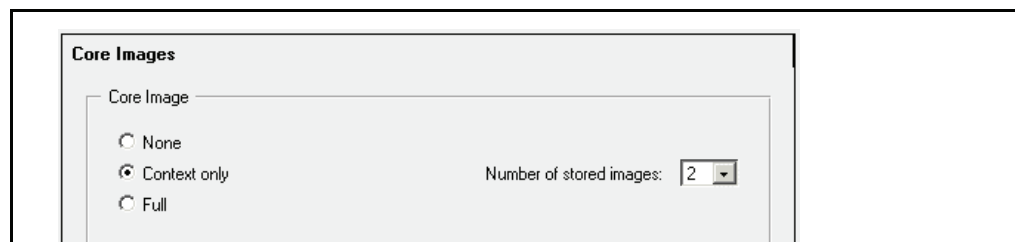
- None**—no system state information is logged. Not recommended.
- Context only**—the state of active processes is logged to disk. This is the default.
- Full**—A complete dump is logged to disk. Use only when asked to do so by Blue Coat Technical Support.

The default setting of Context only is the optimum balance between restart speed and the information needs of Blue Coat Technical Support in helping to resolve a system problem.

You can also select the number of core images that are retained. The default value is 2; the range is between 1 and 10.

To configure core image restart options:

1. Select **Maintenance > Core Images**.



2. Select a core image restart option.
3. (Optional) Select the number of core images that are retained from the **Number of stored images** drop-down list.
4. Click **Apply** to commit the changes to the SG appliance.

Related CLI Syntax for Configuring Core Image Restart Options

```
SGOS#(config) restart core-image {context | full | keep number | none}
```

Diagnostic Reporting (Heartbeats)

The SG appliance diagnostic reporting configurations are located in the Management Console (under the **Maintenance > Heartbeats** tab), and in the CLI (under the configuration diagnostics submode).

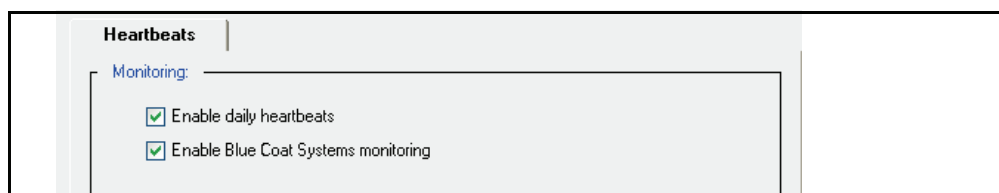
The daily heartbeat is a periodic message that is sent every 24 hours and contains SG appliance statistical data. Besides telling the recipient that the device is alive, heartbeats also are an indicator of the appliance's health. Heartbeats do not contain any private information; they contain only aggregate statistics that can be used to preemptively diagnose support issues. The daily heartbeat is encrypted and transferred to Blue Coat using HTTPS. Administrators can have the daily heartbeat messages e-mailed to them by configuring event log notification. The content that is e-mailed to the administrator is the same content sent to Blue Coat.

If monitoring is enabled, Blue Coat receives encrypted information over HTTPS whenever the appliance is rebooted. The data sent does not contain any private information; it contains restart summaries and daily heartbeats. This allows the tracking of SG appliance unexpected restarts due to system issues, and allows Blue Coat to address system issues preemptively.

If the daily heartbeats setting is disabled, you can still send a heartbeat message by using the `send-heartbeat` command through the CLI (this feature is not available through the Management Console).

To set daily heartbeats and/or Blue Coat monitoring:

1. Select **Maintenance > Heartbeats**.



2. Select or deselect **Enable daily heartbeats** or **Enable Blue Coat monitoring**.
3. Click **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Manage Heartbeats and Monitoring

- ❑ To enter configuration mode:
SGOS#(config) **diagnostics** [*Command_Modes*]
- ❑ The following subcommands are available:
SGOS#(config diagnostics) **heartbeat enable**
SGOS#(config diagnostics) **monitor enable**
SGOS#(config diagnostics) **send-heartbeat**

Note: This option is not available through the Management Console.

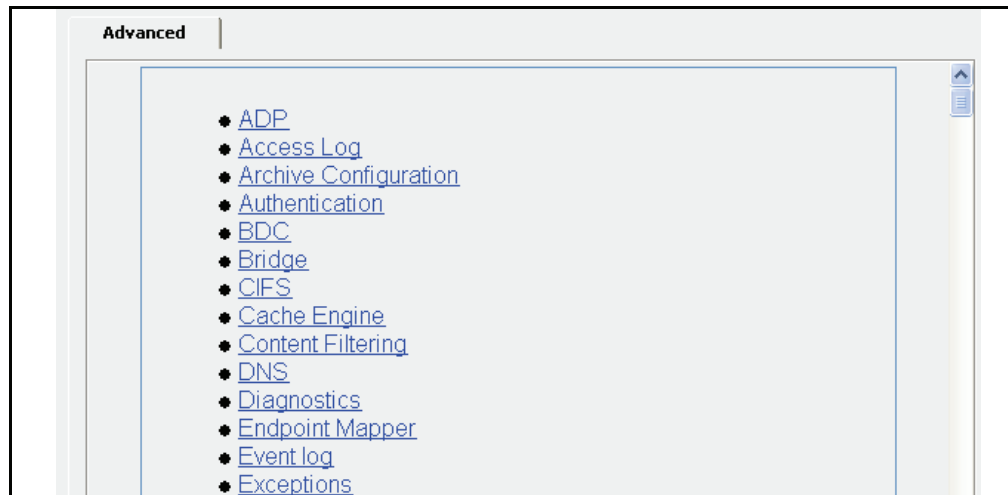
Diagnostic Reporting (CPU Monitoring)

You can enable CPU monitoring whenever you want to see the percentage of CPU being used by specific functional groups. For example, if you look at the CPU consumption and notice that compression/decompression is consuming most of the CPU, you can change your policy to compress/decompress more selectively.

Note: CPU monitoring uses about 2-3% CPU when enabled, and so is disabled by default.

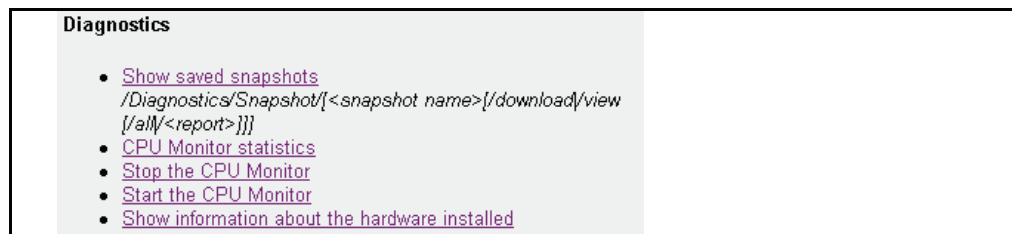
To configure and view CPU monitoring:

1. Select **Statistics > Advanced**.



2. Click the **Diagnostics** link.

A list of links to Diagnostic URLs displays.



3. To enable CPU monitoring, click the **Start the CPU Monitor** link; to disable it, click the **Stop the CPU Monitor** link.
4. To view CPU monitoring statistics, click the CPU Monitor statistics link. You can also click this link from either of the windows described in Step 3.

Related CLI Syntax to Configure and View CPU Monitoring

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) cpu-monitor disable | enable
SGOS#(config diagnostics) cpu-monitor interval seconds
```

Note: The total percentages do not always add up because the display only shows those functional groups that are using 1% or more of the CPU processing cycles.

Note: The commands `SGOS#(config) show cpu` and `SGOS#(config diagnostics) view cpu-monitor` can sometimes display CPU statistics that differ by about 2-3%. This occurs because different measurement techniques are used for the two displays.

Chapter 5: Statistics

The Statistics tabs of the Management Console allow you to view the status of many system operations. Many statistics are available through the CLI, but only in text output.

You can also view detailed system information through the CLI using the `show` command. Access this command through either the enable command prompt (`SGOS#`) or the config command prompt (`SGOS#(config)`). For convenience, the procedures in this chapter show only the enable command prompt. See [“Using the CLI show Command to View Statistics”](#) on page 88 for information about using the `show` command.

This chapter includes the following topics:

- ❑ [“Viewing Traffic Distribution Statistics”](#) on page 62
- ❑ [“Viewing Traffic History”](#) on page 65
- ❑ [“Viewing the ADN History”](#) on page 68
- ❑ [“Viewing Bandwidth Management Statistics”](#) on page 68
- ❑ [“Viewing Protocol Statistics”](#) on page 68
- ❑ [“Viewing System Statistics”](#) on page 70
- ❑ [“Viewing Traffic Distribution Statistics”](#) on page 62
- ❑ [“Active Sessions—Viewing Per-Connection Statistics”](#) on page 76
- ❑ [“Viewing the Access Log”](#) on page 87
- ❑ [“Viewing Advanced Statistics”](#) on page 87

Selecting the Graph Scale

is allowed to fall off the scale. For example, if you select **clip 25% of peaks**, the top 25% of the values are allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. To set the graph scale, select a value from the **Graph scale should** drop-down list.

Some of the graphs offer the option of viewing statistics in bytes or objects. On these pages, you can switch among viewing modes by selecting the desired value from the drop-down list. You can also move your cursor over the bar graphs to dynamically display color-coded statistical information.

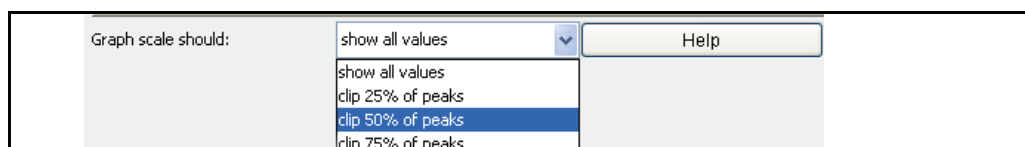


Figure 5-1. Graph Scale Drop-Down Example

Viewing Traffic Distribution Statistics

Use the **Statistics > Traffic Mix** page to display traffic distribution and bandwidth statistics for traffic running through the SG appliance. You can display statistics for proxy types, or for services, and for various time periods.

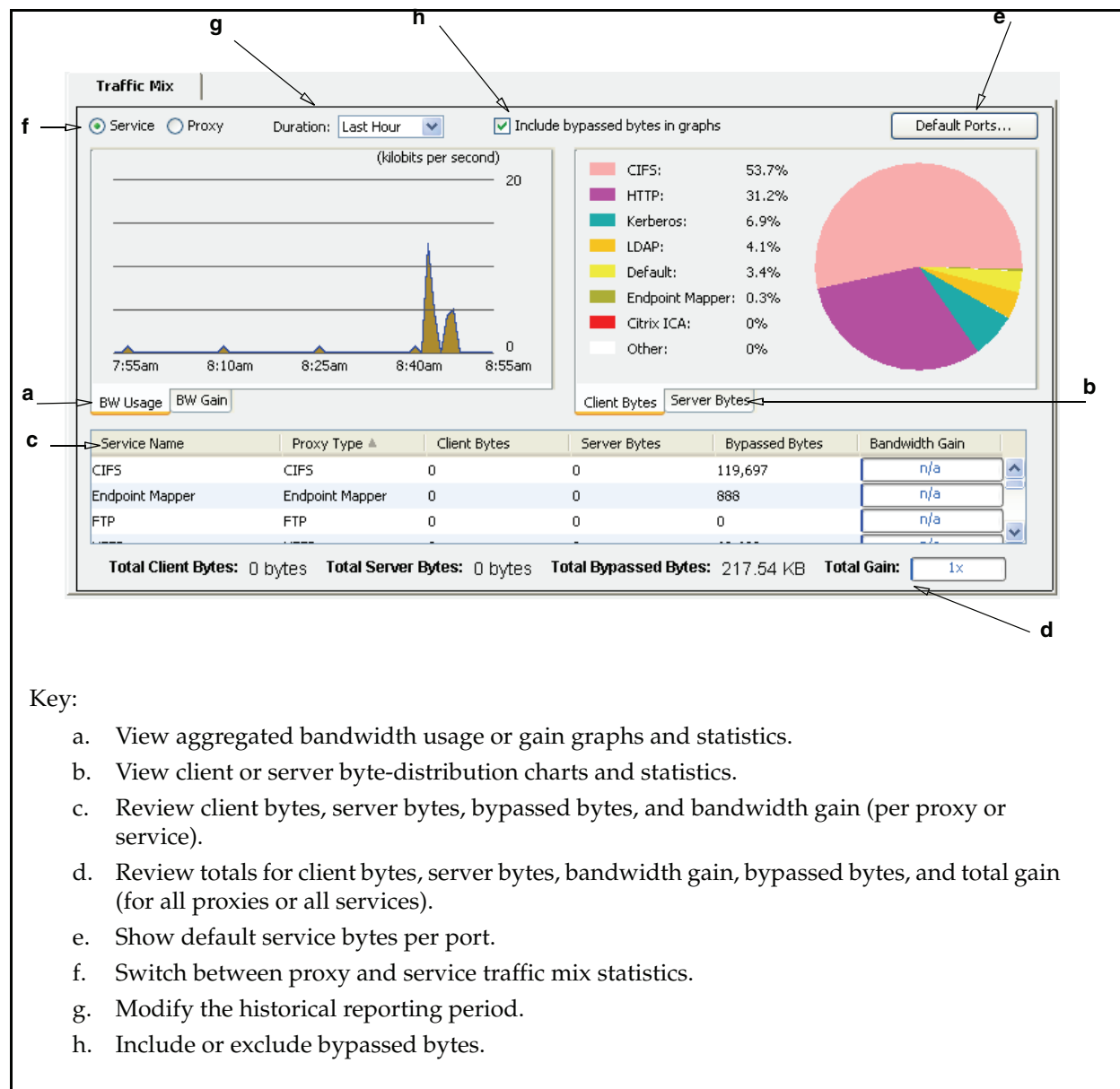


Figure 5-2. Traffic Mix Page

Note: Bypassed bytes are bytes that are not intercepted by a service or proxy. When you include or exclude bypassed bytes, only the graph data and totals are affected. The table data in the lower half of the page is not altered.

For a list of supported proxies, see [“Supported Proxy Types and Services”](#) on page 66.

Note: Endpoint Mapper proxy bytes are the result of Microsoft Remote Procedure Call (MSRPC) communication for MAPI traffic.

Understanding Chart Data

The chart data updates automatically every 60 seconds. The units for the X and Y axis change according to the selected duration. For example, if you select "Last Week," the X-axis displays the days of the week (the most current day is to the far right).

The word "Hit" can display at the top of the BW Gain graph if the gain was the result of a cache hit.

The colors in the bandwidth usage and bandwidth gain charts represent the following information:

- Green—Client bytes
- Blue—Server bytes
- Brown—Bypassed bytes
- Dark Blue—Bandwidth Gain (which includes bypassed bytes, if selected)

In the tool tips (as shown in figure 5-3), bandwidth gain is represented in black text. Hover the mouse cursor over the graph data to view detailed values.

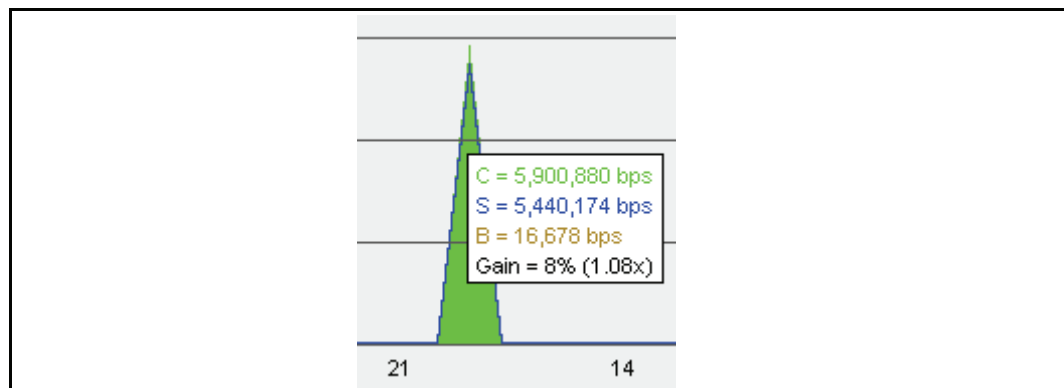


Figure 5-3. Traffic mix statistics displayed when cursor hovers over chart data

Refreshing the Data

The data in the **Traffic Mix** page refreshes whenever you switch views or change the duration of the sample. If there is no activity, the data refreshes every 60 seconds.

About Bypassed Bytes

Bypassed bytes are bytes that are not intercepted by a service or proxy. By default, bypassed bytes are included in the traffic mix views. When evaluating traffic statistics for potential optimization, it can be useful to include or exclude the bypassed byte statistics. Include or exclude bypassed bytes in the charts and graphs by selecting or clearing **Include bypassed bytes in graphs**.

When you include or exclude bypassed bytes, only the graph data and totals are affected. The table data in the lower half of the page is not altered.

About the Default Service Statistics

The default service statistics represent bytes for traffic that has been bypassed because it did not match:

- ❑ An existing service listener
- ❑ Other rules, such as static or dynamic bypass

To view the default service bytes, click **Default Ports...** in the upper-right section of the **Traffic Mix** page.

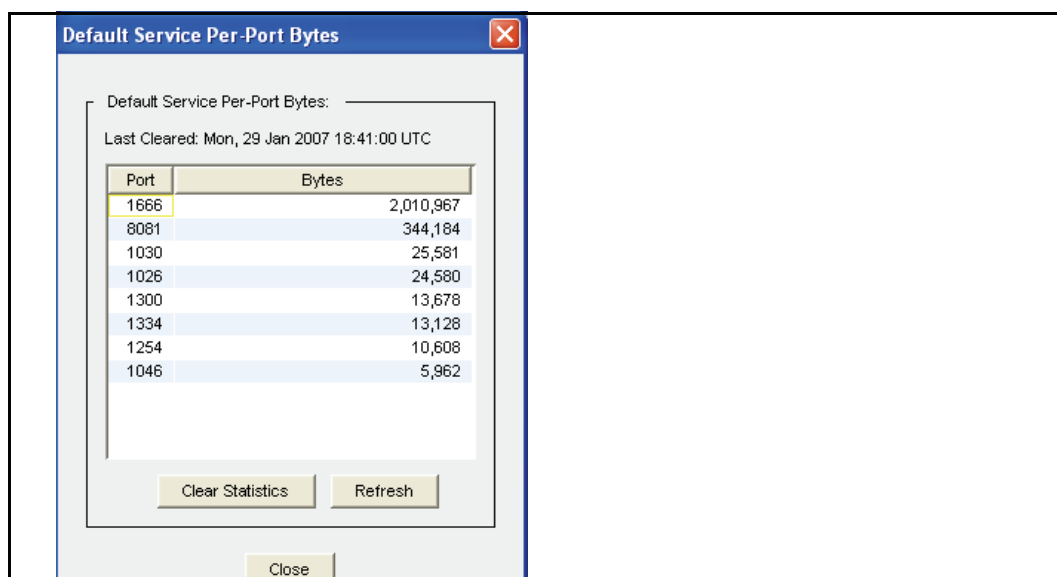


Figure 5-4. Default Service Per Port Bytes Dialog

Refer to *Volume 2: Proxies and Proxy Services* for more information about the default service.

Viewing Bandwidth Usage or Gain

Select the **BW Usage** or **BW Gain** tab in the **Traffic Mix** page to view bandwidth usage and bandwidth gain statistics for the SG appliance over the last hour, day, week, month, and year. To view per-service or per-proxy bandwidth usage statistics, go to the **Traffic History (Statistics > Traffic History)** page.

In the **BW Usage** graph, the green display represents client data; the blue display represents server data; the brown represents bypassed bytes data. Hover your cursor over the graph to see the bandwidth usage and gain data.

To view bandwidth usage or gain statistics:

1. Select **Statistics > Traffic Mix > BW Usage** or **BW Gain**.
2. Select a time period from the **Duration** drop-down list.
3. (Optional) Select **Include bypassed bytes in graphs** to include statistics for bytes not intercepted by a proxy or service.
4. Select the **Service** radio button to display the bandwidth usage statistics for all configured services.

5. Select the **Proxy** radio button to display the bandwidth usage statistics for all supported proxies.

Viewing Client Byte and Server Byte Traffic Distribution

Select the **Client Bytes** or **Server Bytes** tabs in the **Traffic Mix** page to view a pie chart of client byte or server byte statistics for the SG appliance over the last hour, day, week, month, or year. The pie charts display data for the top seven services or proxies; all other proxy and service statistics are categorized in the “**Other**” category. These items are arranged in a sorted order—the item that has highest percentage is displayed at the top of the list.

To view client and server byte statistics:

1. Select **Statistics > Traffic Mix > Client Bytes** or **Server Bytes**.
2. Select a time period from the **Duration** drop-down list.
3. (Optional) Select **Include bypassed bytes in graphs** to include statistics for bytes not intercepted by a proxy or service.
4. Select the **Service** radio button to display the traffic distribution statistics for all services.
5. Select the **Proxy** radio button to display the traffic distribution statistics for all supported proxies.

Viewing Traffic History

Use the **Statistics > Traffic History** page to monitor the traffic statistics for all traffic running through the SG appliance. You can display statistics for all proxy types or all services.

Key:

- View traffic history statistics by service or by proxy.
- Modify the historical reporting period.
- Include or exclude bypassed bytes.
- View totals for client bytes, server bytes, and bandwidth gain for the selected service or proxy type.
- Display charts for bandwidth usage, bandwidth gain, client bytes, and server bytes.

Note: Bypassed bytes are bytes that are not intercepted by a service or proxy.

Supported Proxy Types and Services

The **Traffic History** (and **Traffic Mix**) page displays data for the following proxy types (and services of these proxy types):

- CIFS
- HTTP
- MAPI
- Real Media
- TCP Tunnel
- Endpoint Mapper
- HTTPS Forward Proxy
- MSRPC
- RTSP
- Windows Media
- FTP
- HTTPS Reverse Proxy
- Quicktime
- SSL

Note: Endpoint Mapper proxy bytes are the result of Remote Procedure Call (RPC) communication for MAPI traffic.

Unsupported Proxy Types

The **Traffic History** does not display data for the following proxy types:

- DNS
 - IM
 - P2P
 - SOCKS
 - Telnet
-

Understanding Chart Data

The **Traffic History** chart data updates automatically every 60 seconds. The colors in the chart represent the following information:

- Bandwidth Usage chart:
 - Green—Client bytes
 - Blue—Server bytes
 - Brown—Bypassed bytes
 - Dark Blue—Bandwidth gain
- Bandwidth Gain chart
 - Dark Blue—Bandwidth gain
- Client and Server Byte charts:
 - Green—Intercepted client bytes
 - Blue—Intercepted server bytes
 - Brown—Bypassed bytes

Hover the mouse cursor over the chart data to view detailed values.



Figure 5-5. Traffic history statistics displayed when cursor hovers over chart data

Refreshing the Data

The data in the **Traffic History** page refreshes whenever you switch views or change the duration of the sample. If there is no activity, the data refreshes every minute.

About Bypassed Bytes

Bypassed bytes are bytes that are not intercepted by a service or proxy. By default, bypassed bytes are included in the traffic mix views. When evaluating traffic statistics for potential optimization, it can be useful to include or exclude the bypassed byte statistics. Include or exclude bypassed bytes in the charts and graphs by selecting or deselecting **Include bypassed bytes**.

Viewing Bandwidth Usage or Gain or Client Byte and Server Byte Traffic History

To view client and server byte or bandwidth gain statistics:

1. Select **Statistics > Traffic History > BW Usage, BW Gain, Client Bytes, or Server Bytes**.
2. Generate history data for a service or proxy
Service history:
 - a. Select the **Service** radio button.
 - b. Select a service from the drop-down list.Proxy history:
 - a. Select the **Proxy** radio button.
 - b. Select a proxy from the drop-down list.
3. Select a time period from the **Duration** drop-down list
4. (Optional) Select **Include bypassed bytes in graphs** to include statistics for bytes not intercepted by a proxy or service.

Viewing the ADN History

The **Statistics > ADN History** pages display WAN optimization statistics for inbound and outbound compression gain. Refer to the WAN optimization information in *Volume 5: Advanced Networking* for more information about these statistics.

Viewing Bandwidth Management Statistics

The **Statistics > Bandwidth Mgmt** pages display the current class and total class statistics. Refer to the bandwidth management information in *Volume 5: Advanced Networking* for more information about these statistics.

Viewing Protocol Statistics

The **Statistics > Protocol Details** pages provide statistics for the protocols serviced by the SG appliance. These statistics should be used to compliment the statistics in the **Traffic History** and **Traffic Mix** pages.

The descriptions of these statistics are located in the proxy services to which they pertain. The following list provides a listing of these statistics and describes where to find additional information.

❑ CIFS History

The **Statistics > Protocol Details > CIFS History** pages enable you view statistics for CIFS objects, CIFS bytes read, CIFS bytes written, and CIFS clients. Refer to the CIFS chapter in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

❑ HTTP/FTP History

The **Statistics > Protocol Details > HTTP/FTP History** pages enable you view statistics for HTTP/HTTPS/FTP objects, HTTP/HTTPS/FTP bytes, HTTP/HTTPS/FTP clients, client compression gain, and server compression gain. Refer to the HTTP and FTP chapters in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

For HTTP/FTP bandwidth usage statistics, see the **Traffic Mix** and **Traffic History** pages.

❑ IM History

The **Statistics > Protocol Details > IM History** pages enable you view statistics for IM connection data, IM activity data, and IM clients. Refer to the IM chapter in *Volume 3: Web Communication Proxies* for more information about these statistics.

❑ MAPI History

The **Statistics > Protocol Details > MAPI History** pages enable you view statistics for MAPI client bytes read, MAPI client bytes written, and MAPI clients. Refer to the MAPI chapter in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

For MAPI bandwidth usage statistics, see the **Traffic Mix** and **Traffic History** pages.

❑ P2P History

The **Statistics > Protocol Details > P2P History** pages enable you view statistics for P2P data, P2P clients, and P2P bytes. Refer to the P2P information in *Volume 6: The Visual Policy Manager and Advanced Policy Tasks* for more information about these statistics.

❑ Shell History

The **Statistics > Protocol Details > Shell History** pages enable you view statistics for shell clients. Refer to the shell proxy information in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

❑ SOCKS History

The **Statistics > Protocol Details > SOCKS History** pages enable you view statistics for SOCKS clients, SOCKS connections, client compression gain, and server compression gain. Refer to the SOCKS chapter in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

❑ SSL History

The **Statistics > Protocol Details > SSL History** pages enable you view statistics for unintercepted SSL data, unintercepted SSL clients, and unintercepted SSL bytes. Refer to the SSL chapter in *Volume 2: Proxies and Proxy Services* for more information about these statistics.

- ❑ Streaming History

The **Statistics > Protocol Details > Streaming History** pages enable you view statistics for Windows Media, Real Media, QuickTime, current streaming data, total streaming data, and bandwidth gain. Refer to the streaming chapter in *Volume 3: Web Communication Proxies* for more information about these statistics.

For MMS bandwidth usage statistics, see the **Traffic Mix** and **Traffic History** pages.

Viewing System Statistics

The **System Statistics** pages enable you to view:

- ❑ “Resources Statistics” on page 70
- ❑ “Contents Statistics” on page 74
- ❑ “Event Logging Statistics” on page 75
- ❑ “Failover Statistics” on page 76

Resources Statistics

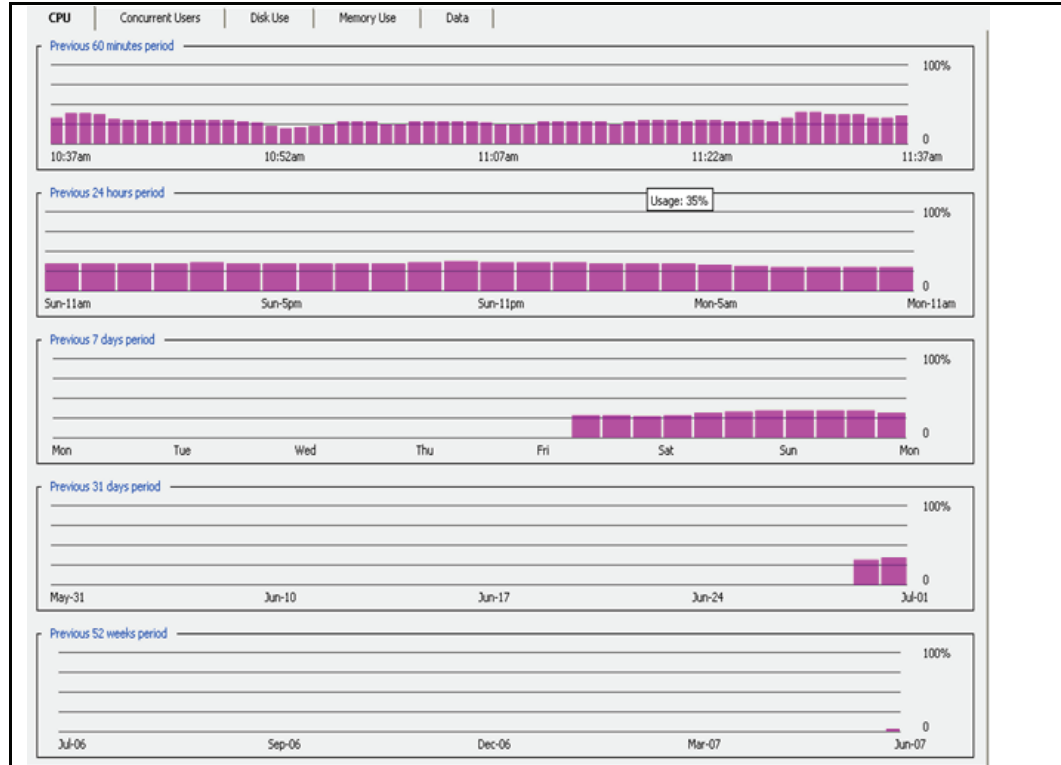
The **Resources** tabs (**CPU**, **Disk Use**, **Memory Use**, and **Data**) allow you to view information about how disk space and memory are being used, and how disk and memory space are allocated for cache data. You can view data allocation statistics through both the Management Console and the CLI, but disk and memory use statistics are available only through the Management Console.

Viewing CPU Utilization

Through the Management Console, you can view the average CPU utilization percentages for the SG appliance over the last 60 minutes, 24 hours, and 30 days. You can see the current CPU utilization statistic in the CLI.

To view CPU utilization:

1. Select **Statistics > System > Resources > CPU**.

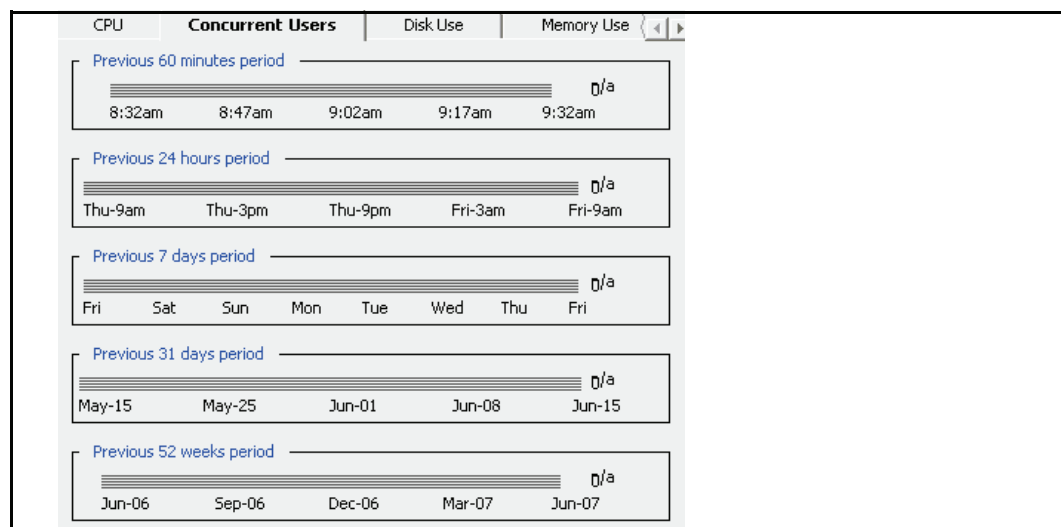


Viewing Concurrent Users

The **Concurrent Users** tab shows users (IP addresses) going through the SG appliance for the last 60 minutes, day, week, month, and year. Only unique IP addresses of connections intercepted by proxy services are counted toward the user limit.

To view concurrent users:

Click **Statistics > System > Resources > Concurrent Users**.



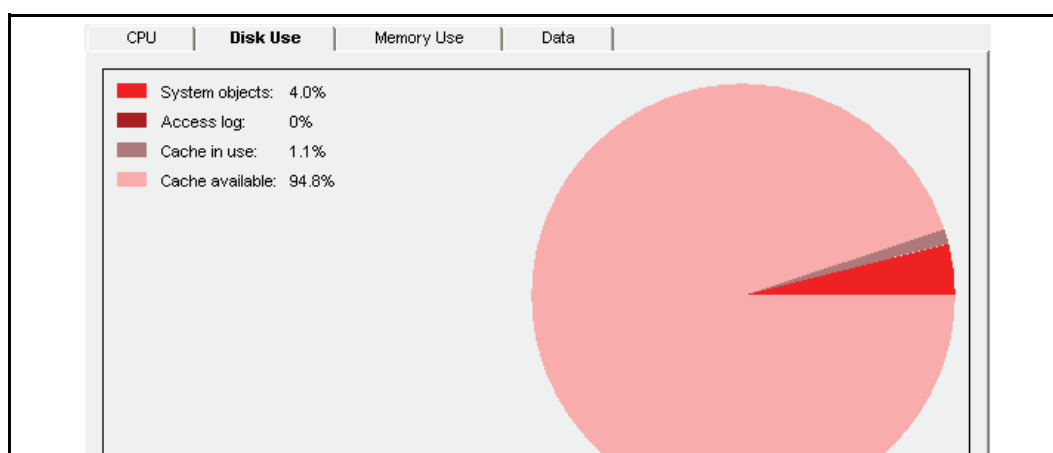
Viewing Disk Use Statistics

The **Disk Use** tab shows the SG appliance disk usage. The fields on the tab are:

- ❑ **System Objects**—the percentage of storage resources currently used for non-access-log system objects
- ❑ **Access log**—the percentage of storage resources currently used for the access log
- ❑ **Cache in Use**—the percentage of non-system, non-access-log resources currently in use for cached objects
- ❑ **Cache available**—the percentage of non-system, non-access-log resources still available for caching objects

To view disk use statistics:

Select **Statistics > System > Resources > Disk Use**.



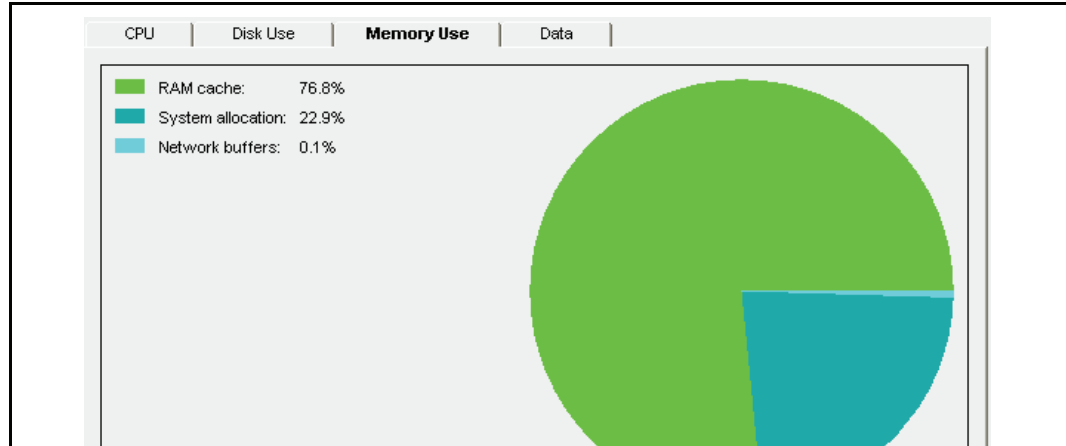
Viewing Memory Use Statistics

The **Memory Use** tab shows the amount of memory used for RAM, the SG appliance itself, and for network buffers. The fields on the Memory Use tab are:

- ❑ **RAM Cache**—the amount of RAM that is used for caching
- ❑ **System allocation**—the amount of RAM allocated for the device system
- ❑ **Network buffers**—the amount of RAM currently allocated for network buffers

To view memory use statistics:

Select **Statistics > System > Resources > Memory Use**.



Viewing Data Allocation Statistics in RAM and on Disk

The **Data** tab shows the total and available disk space and RAM, and how they are currently allocated. The fields on the Data tab are described below. You can also view this information in the CLI.

- ❑ **Maximum objects supported**—The maximum number of objects that can be supported
- ❑ **Cached objects**—The number of objects that are currently cached
- ❑ **Disk used by system objects**—The amount of disk space used by the system objects
- ❑ **Disk used by access log**—The amount of disk space used for access logs
- ❑ **Total disk installed**—The total amount of disk space installed on the device
- ❑ **RAM used by cache**—The amount of RAM allocated for caching
- ❑ **RAM used by system**—The amount of RAM allocated for system use
- ❑ **RAM used by network**—The amount of RAM allocated for network use
- ❑ **Total RAM installed**—The total amount of RAM installed

To view data allocation statistics:

Select **Statistics > System > Resources > Data**.

| CPU | Disk Use | Memory Use | Data |
|------------------------------|-------------------|------------|------|
| Maximum objects supported: | 2,292,607 objects | | |
| Cached Objects: | 27,797 objects | | |
| Disk used by system objects: | 1.5 gigabytes | | |
| Disk used by access log: | 0 bytes | | |
| Total disk installed: | 37.27 gigabytes | | |
| RAM used by cache: | 374.61 megabytes | | |
| RAM used by system: | 112.13 megabytes | | |
| RAM used by network: | 864.03 kilobytes | | |
| Total RAM installed: | 487.59 megabytes | | |

Contents Statistics

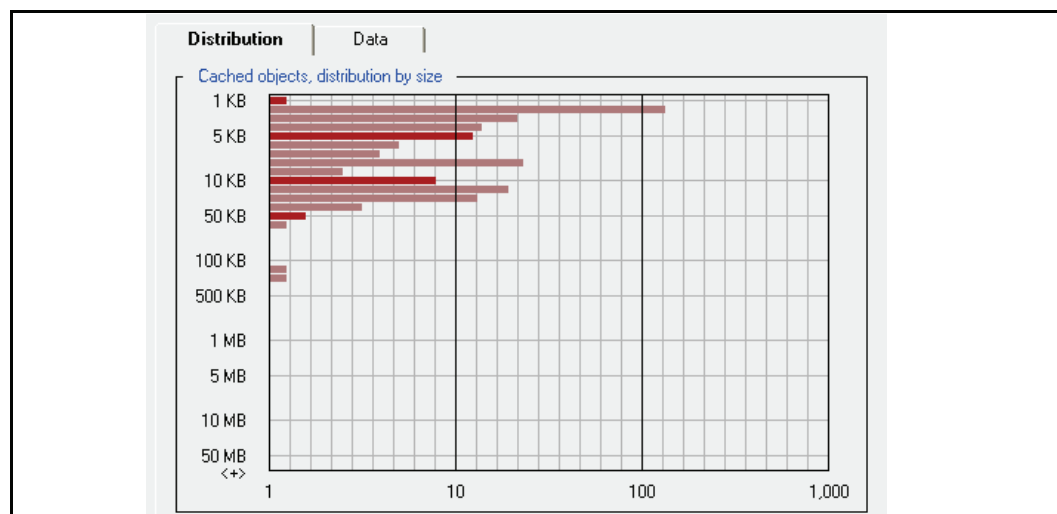
The **Contents** tabs (**Distribution** and **Data**) allow you to see information about objects currently stored or served organized by size. The cache contents include all objects currently stored by the SG appliance. The cache contents are not cleared when the appliance is powered off.

Viewing Cached Objects by Size

The **Distribution** tab shows the objects currently stored by the SG appliance, ordered by size.

To view the distribution of cache contents:

Select **Statistics > System > Contents > Distribution**.



Viewing the Number of Objects Served by Size

The **Data** tab displays the number of objects served by the SG appliance, organized by size. This chart shows you how many objects of various sizes have been served.

To view the number of objects served:

Select **Statistics > System > Contents > Data**.

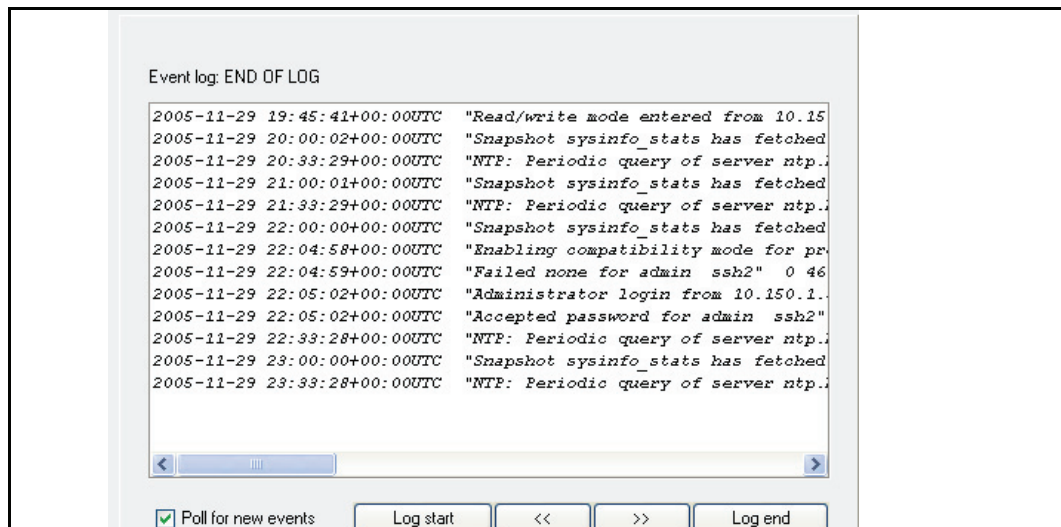
| Distribution | | Data | |
|--------------|-------------------|---------------|--|
| 0-1 KB: 1 | 9-10 KB: 9 | 90-100 KB: 0 | |
| 1-2 KB: 130 | 10-20 KB: 29 | 100-200 KB: 1 | |
| 2-3 KB: 34 | 20-30 KB: 12 | 200-300 KB: 1 | |
| 3-4 KB: 15 | 30-40 KB: 5 | 300-400 KB: 0 | |
| 4-5 KB: 10 | 40-50 KB: 2 | 400-500 KB: 0 | |
| 5-6 KB: 7 | 50-60 KB: 1 | 500-600 KB: 0 | |
| 6-7 KB: 6 | 60-70 KB: 0 | 600-700 KB: 0 | |
| 7-8 KB: 37 | 70-80 KB: 0 | 700-800 KB: 0 | |
| 8-9 KB: 4 | 80-90 KB: 0 | 800-900 KB: 0 | |
| .9-1 MB: 0 | 9-10 MB: 0 | over 50 MB: 0 | |
| 1-2 MB: 0 | 10-20 MB: 0 | | |
| 2-3 MB: 0 | 20-30 MB: 0 | | |
| 3-4 MB: 0 | 30-40 MB: 0 | | |
| 4-5 MB: 0 | 40-50 MB: 0 | | |
| 5-6 MB: 0 | | | |
| 6-7 MB: 0 | | | |
| 7-8 MB: 0 | | | |
| 8-9 MB: 0 | | | |
| | Objects in cache: | 304 | |

Event Logging Statistics

The event log contains all events that have occurred on the SG appliance. Configure the level of detail available by selecting **Maintenance > Event Logging > Level** (For details, see “Configuring Which Events to Log” on page 15).

To view the event log:

1. Select **Statistics > System > Event Logging**.



2. Click **Log start** or **Log end** or the forward and back arrow buttons to move through the event list.
3. (Optional) Click the **Poll for new events** check box to poll for new events that occurred while the log was being displayed.

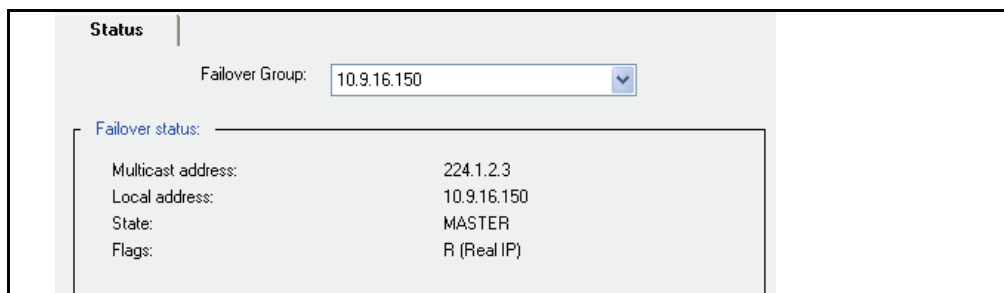
Note: The Event Log cannot be cleared.

Failover Statistics

At any time, you can view statistics for any failover group you have configured on your system.

To view failover statistics:

1. Select **Statistics > System > Failover**.



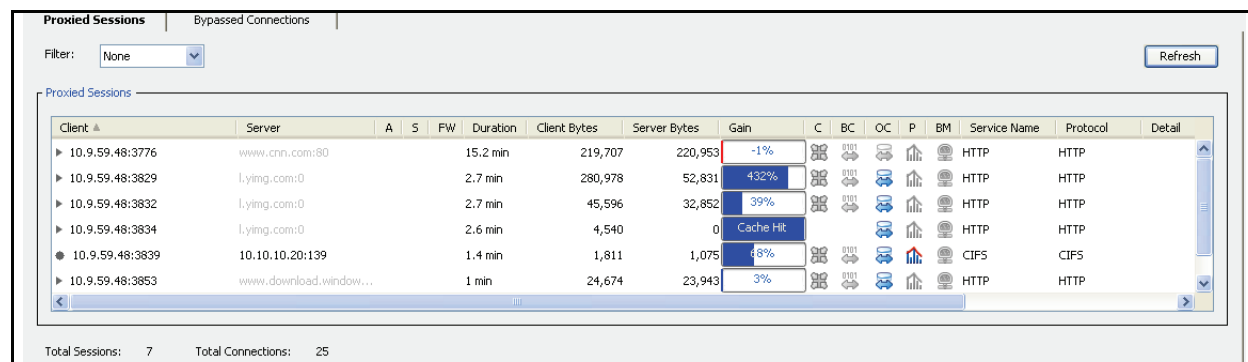
2. From the **Failover Group** drop-down list, select the group to view.

The information displayed includes the multicast address, the local address, the state, and any flags, where **V** indicates that the group name is a virtual IP address, **R** indicates that the group name is a physical IP address, and **M** indicates that this machine can be configured to be the master if it is available.

Active Sessions—Viewing Per-Connection Statistics

The **Statistics > Active Sessions** pages display per-connection statistics for all proxied sessions and bypassed connections running through the SG appliance.

The following figure shows an example of the **Active Sessions** pages.



The **Active Sessions** feature has two pages:

- ❑ **Proxied Sessions**—Displays statistics for all connections intercepted by configured proxies or services
To learn more about proxied sessions, see [“Analyzing Proxied Sessions”](#) on page 77.
- ❑ **Bypassed Connections**—Displays statistics for all unintercepted traffic
To learn more about bypassed connections, see [“Analyzing Bypassed Connections Statistics”](#) on page 84.

Analyzing *Proxied Sessions*

Use the **Statistics > Active Sessions > Proxied Sessions** page to get an immediate picture of the sessions, protocol types, services, bytes, and bandwidth gains (derived from WAN optimization and object caching) associated with client traffic.

The first time you navigate to the **Proxied Sessions** page, no data is displayed. To display proxied sessions data, click **Show**. The statistics displayed in the window are not automatically updated. To update the statistics, click **Show** again.

Important: Use the statistics on the **Proxied Sessions** pages as a diagnostic tool only. The **Proxied Sessions** pages do not display every connection running through the SG appliance. Rather, this feature displays only the active sessions—one client connection (or several), together with the relevant information collected from other connections associated with that client connection. Because it displays only open connections, you cannot use the data for reporting purposes.

The **Proxied Sessions** tab displays statistics for the following proxies:

- HTTP
- SSL
- FTP
- MAPI
- HTTPS Reverse Proxy
- CIFS
- Endpoint Mapper
- MSRPC
- HTTPS Forward Proxy
- TCP-Tunnel
- MMS

Client connections are available for viewing as soon as the connection request is received. However, if delayed intercept is enabled, the connection is not shown until the three-way handshake completes. Server connections are registered and shown in the table after the `connect` call completes.

Viewing Proxied Sessions

To view proxied sessions:

1. Select **Statistics > Active Sessions > Proxied Sessions**.
2. (Optional) Select a filter from the **Filter** drop-down list.

About the Proxied Sessions Statistics

When reviewing the proxied session statistics, note that:

- Active client and server connections are displayed in black.
- Inactive connections are displayed in gray.
- Session and connection totals are displayed on the bottom left side of the page.

The following table describes the column headings and icons on the **Proxied Sessions** page.

Table 5-1. Table Column Heading Descriptions on the Proxied Sessions Page





| Column Heading | Description |
|---|--|
| Client | <p>IP address and port of the client PC (or other downstream host).</p> <p>When the client connection is inactive, the contents of this column are unavailable (gray). A client connection can become inactive if, for example, a client requests a large object and then aborts the download before the SG appliance has completed downloading it into its cache.</p> <p>When the session had multiple client connections, a tree view is provided. See “Viewing Sessions with Multiple Connections” on page 81 for more information.</p> |
| Server | <p>Final destination of the request.</p> <p>By default, the hostname is displayed. However, if a user entered an IP address in the URL, the IP address is displayed.</p> <p>The contents of this column are unavailable if the server connection is inactive. This can occur when a download has completed (and the server connection is closed or returned to the idle pool), but the object is still being served to the client.</p> <p>If a server connection was never made (a pure cache hit case), the Server column displays the hostname (or IP address) of the requested server.</p> <p>Active server connections are shown in black; inactive connections are unavailable.</p> |
| <p>A</p>   | <p>ADN. Indicates that the server connection is flowing over an ADN tunnel. If the icon is not present, it indicates that an ADN tunnel is not in use.</p> <p>Encrypted ADN tunnel.</p> |
| <p>S</p>  | <p>SOCKS. Indicates that the next hop is a SOCKS proxy. If the icon is not present, it indicates that a SOCKS proxy is not in use.</p> |
| <p>FW</p>  | <p>Forwarding. Indicates that the next hop is a proxy server. If the icon is not present, it indicates that forwarding is not in effect.</p> |
| Duration | <p>Displays the amount of time the session has been established.</p> |
| Client Bytes | <p>Represents the number of bytes (to and from the client) at the socket level on the client connection. All application-level bytes are counted, including application overhead such as HTTP headers, CIFS headers, and so on.</p> <p>TCP and IP headers, packet retransmissions, and duplicate packets are not counted.</p> <p>See “About the Byte Totals” on page 83 for more information.</p> |

Table 5-1. Table Column Heading Descriptions on the Proxied Sessions Page (Continued)







| Column Heading | Description |
|---|--|
| Server Bytes | <p>Represents the number of bytes (to and from the server) at the socket level on the server connection. All application-level bytes are counted, including application overhead such as HTTP headers, CIFS headers, and so on.</p> <p>If the traffic is flowing through an ADN tunnel, the bytes are counted after ADN optimization, meaning that compressed byte counts are displayed.</p> <p>TCP and IP headers, packet retransmissions, and duplicate packets are not counted.</p> <p>See “About the Byte Totals” on page 83 for more information.</p> |
| Gain | <p>Displays the bandwidth gain for the session. The calculation is: $(\text{Client Bytes} - \text{Server Bytes}) / \text{Server Bytes}$</p> <p>When the request results in a pure cache hit, this column displays Cache Hit.</p> |
| C  | <p>Compression. When displayed in color, this icon indicates that an ADN Tunnel is in use and gzip compression is active in either direction on that tunnel.</p> <p>This icon has three states:</p> <ul style="list-style-type: none"> • Active (color icon) • Inactive (gray icon) • Not possible (not displayed) |
| BC  | <p>Byte Caching. When displayed in color, this icon indicates that an ADN Tunnel is in use and byte-caching is active in either direction on that tunnel</p> <p>This icon has three states:</p> <ul style="list-style-type: none"> • Active (color icon) • Inactive (gray icon) • Not possible (not displayed) |

Table 5-1. Table Column Heading Descriptions on the Proxied Sessions Page (Continued)

| Column Heading | Description |
|---|--|
| <p data-bbox="396 304 435 331">OC</p>  | <p data-bbox="667 289 1412 373">Object Caching. When displayed in color, this icon indicates that an HTTP, HTTPS, CIFS, Streaming, or FTP proxy is in use and the content is cacheable.</p> <p data-bbox="667 388 938 415">This icon has three states:</p> <ul data-bbox="667 426 998 527" style="list-style-type: none"> <li data-bbox="667 426 889 453">• Active (color icon) <li data-bbox="667 464 902 491">• Inactive (gray icon) <li data-bbox="667 501 998 527">• Not possible (not displayed) <p data-bbox="667 537 768 564">The icon:</p> <ul data-bbox="667 579 1412 800" style="list-style-type: none"> <li data-bbox="667 579 1412 674">☐ Is unavailable if the content is non-cacheable (or for CIFS, when the entire connection is non-cacheable—not on an object-by-object basis). <li data-bbox="667 684 1304 711">☐ Is not displayed for MAPI and TCP-Tunnel traffic. <li data-bbox="667 722 1412 800">☐ Does not indicate a cache hit; it indicates only that the object is cacheable. |
|  | <p data-bbox="667 825 1412 884">Live splitting. When displayed in color, this icon indicates that a live MMS stream is being split to the client.</p> <p data-bbox="667 894 927 921">This icon has two states:</p> <ul data-bbox="667 932 894 991" style="list-style-type: none"> <li data-bbox="667 932 894 959">• Active (color icon) <li data-bbox="667 970 902 997">• Inactive (gray icon) |
| <p data-bbox="396 1031 412 1058">P</p>  | <p data-bbox="667 1014 1412 1098">Protocol Optimization. When displayed in color, this icon indicates that a proxy is in use that is capable of performing latency optimizations. These proxies include HTTP, HTTPS, CIFS, and MAPI.</p> <p data-bbox="667 1108 938 1136">This icon has three states:</p> <ul data-bbox="667 1146 998 1247" style="list-style-type: none"> <li data-bbox="667 1146 889 1173">• Active (color icon) <li data-bbox="667 1184 902 1211">• Inactive (gray icon) <li data-bbox="667 1222 998 1247">• Not possible (not displayed) |
| <p data-bbox="396 1287 435 1314">BM</p>  | <p data-bbox="667 1270 1412 1354">Bandwidth Management. When displayed in color, this icon indicates that either the client or server connection has been assigned to a bandwidth class.</p> <p data-bbox="667 1365 927 1392">This icon has two states:</p> <ul data-bbox="667 1402 894 1461" style="list-style-type: none"> <li data-bbox="667 1402 894 1430">• Active (color icon) <li data-bbox="667 1440 902 1467">• Inactive (gray icon) |
| <p data-bbox="396 1493 548 1520">Service Name</p> | <p data-bbox="667 1493 1094 1520">Displays the service used by the session.</p> <p data-bbox="667 1530 1406 1614">Even if a client connection is handed off to a different application proxy, this column shows the service name of the original service that intercepted the client connection.</p> |
| <p data-bbox="396 1640 483 1667">Protocol</p> | <p data-bbox="667 1640 1110 1667">Displays the protocol used by the session.</p> |
| <p data-bbox="396 1692 461 1719">Detail</p> | <p data-bbox="667 1692 1382 1751">Provides additional information. For example, it can indicate that a CIFS connection is "pass-through" due to SMB signing.</p> |

Using the Tool Tips

Hover the cursor over the following components to get more information:

- Table column headers—Displays the full name of the column header.
- Row values.
- Acceleration icons (**C**, **BC**, **OC**, **P**, **BM**)—Displays the icon identity.
- ADN, SOCKS, and FW icons—Displays the next hop.
- Client and Server icons—Displays the full hostname or IP address.

About MMS Streaming Connections

The Active Sessions feature displays connection statistics for MMS streams over HTTP, TCP, or UDP only. Multicast connections are not displayed. When an MMS stream is displayed, the service name is listed as “HTTP” or “MMS” (depending on the transport used) and the protocol indicates “Windows Media.”

| Client | Server | A | S | F... | Duration | Client Bytes | Server Bytes | Gain | C | BC | OC | P | BM | Service Name | Protocol |
|-----------------|-------------------------|---|---|------|----------|--------------|--------------|------|---|----|----|---|----|--------------|---------------|
| 10.9.59.48:2597 | msert.wmod.llnwd.net:80 | | | | 14 sec | 494,885 | 166,012 | 198% | | | | | | HTTP | Windows Media |

Figure 5-6. MMS Streaming Connection Example

Viewing Sessions with Multiple Connections

When multiple client or server connections are associated with a single session, the **Client** column provides a tree-view that allows you to expand the row to view more details about the associated connections. The tree view is represented by the ▶ icon.

The following figure shows an HTTP example of this tree view.

| Client | Server | A | S | F... | Duration | Client Bytes | Server Bytes | Gain | C | BC | OC | P | BM | Service Name | Protocol |
|-------------------|---------------------------|---|---|------|----------|--------------|--------------|------|---|----|----|---|----|--------------|----------|
| ▶ 10.9.59.48:3579 | amch.questionmarket.co... | | | | 1 sec | 13,760 | 4,496 | 206% | | | | | | HTTP | HTTP |
| ● 10.9.59.48:3579 | amch.questionmarket.co... | | | | 1 sec | 13,760 | 1,638 | 740% | | | | | | HTTP | HTTP |
| ● :0 | i.cnn.net:0 | | | | 0 sec | 0 | 0 | | | | | | | HTTP | HTTP |
| ● :0 | ads.cnn.com:80 | | | | 0 sec | 0 | 1,508 | | | | | | | HTTP | HTTP |
| ● :0 | view.atdnt.com:80 | | | | 0 sec | 0 | 700 | | | | | | | HTTP | HTTP |
| ● :0 | ad.doubleclick.net:80 | | | | 0 sec | 0 | 650 | | | | | | | HTTP | HTTP |

Figure 5-7. Multiple Server Connections Example

HTTP

The tree view displays (as shown above) for HTTP if multiple hosts are contacted during a session or if pipelining is used.

FTP

FTP uses multiple, concurrent connections. These are represented as separate rows in the tree view, as shown in the following figure.

| Client | Server | A | S | F... | Duration | Client Bytes | Server Bytes | Gain | C | BC | OC | P | BM | Service Name | Protocol |
|-------------------|-------------------|---|---|------|----------|--------------|--------------|------|---|----|----|---|----|--------------|----------|
| ▶ 10.9.59.48:3718 | 146.6.54.21:21 | | | | 3 sec | 752 | 747 | 1% | | | | | | FTP | FTP |
| ● 10.9.59.48:3718 | 146.6.54.21:21 | | | | 3 sec | 324 | 319 | 2% | | | | | | FTP | FTP |
| ● 10.9.59.48:3719 | 146.6.54.21:16499 | | | | 0 sec | 428 | 428 | 0% | | | | | | FTP | FTP |

Figure 5-8. FTP Connections Example

CIFS, MAPI, and Endpoint Mapper do not display multiple connections.

MMS

The active sessions feature displays MMS streams that have a client associated with them. MMS streams that do not have a client associated with them (multicast, content management requests, and so on) are not displayed. MMS streams are displayed as follows:

- ❑ MMS UDP streams have two connections, one for data and one for control.
- ❑ MMS TCP streams have a single connection.
- ❑ MMS HTTP streams have a single connection.

For additional information about streaming connections, see “About MMS Streaming Connections” on page 81.

Understanding the Tree View

When collapsed, the cumulative totals for all connections are displayed, as shown in Figure 5-9.

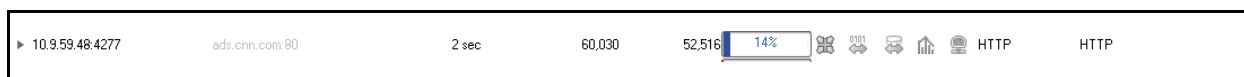


Figure 5-9. Active Sessions Tree View

When expanded, the tree view displays per-connection statistics for the session, as shown in the following example. The top line is a summary of that session’s statistics. The second line displays the statistics for the *primary session*.

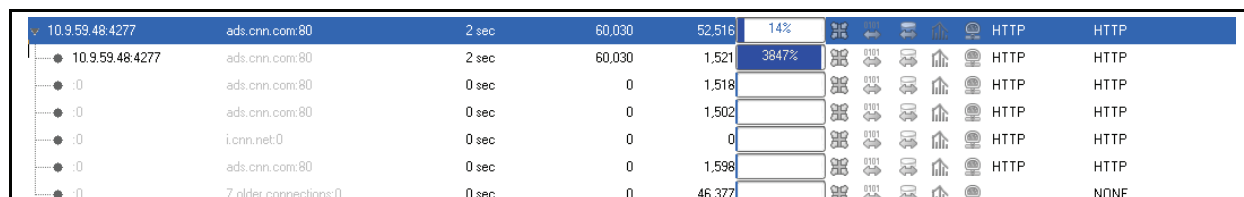


Figure 5-10. Active Sessions Tree View (Expanded)

The **Gain** column result differs according to the server or client byte totals:

- ❑ Zero client bytes: displays no gain.
- ❑ Zero client and server bytes: displays no gain.
- ❑ Zero server bytes: displays **Cache Hit** (see the figure below).
- ❑ Client and server are non-zero: displays the calculated gain.

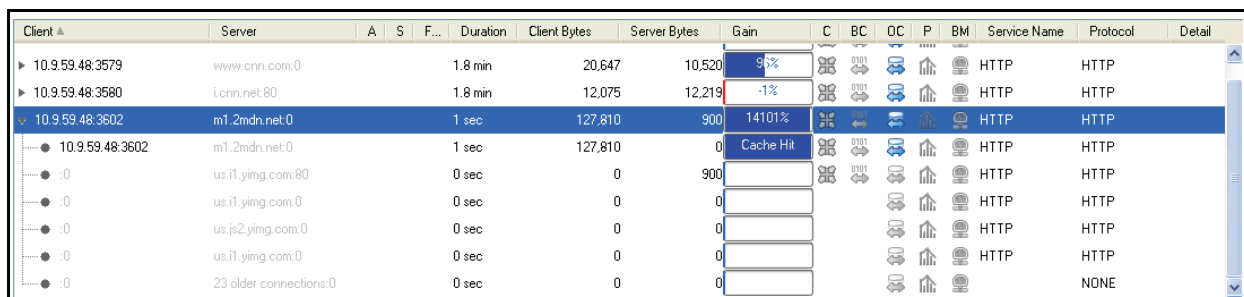


Figure 5-11. Gain Column Example

About the Byte Totals

The client and server byte total is the sum of all bytes going to and from the client or server. All application-level bytes are counted, including application overhead such as HTTP headers, CIFS headers, and so on. TCP and IP headers, packet retransmissions, and duplicate packets are not counted.

The following sections describe some of the factors that can affect the byte totals.

ADN Tunnels

If the traffic is flowing through an ADN tunnel, the bytes are counted after ADN optimization, meaning that compressed byte counts are displayed.

Multiple Server Connections

A single client connection can use many server connections. The server byte counts include the total bytes transferred over all server connections accessed over the lifetime of a client connection. Even though a server connection can serve many clients, the same server byte is never included in more than one client connection total.

Aborted Downloads

In some cases, you might see the server bytes increasing even after the client has closed the connection. This can occur when a client requests a large object and aborts the download before receiving the entire object. The server bytes continue to increase because the SG appliance is retrieving the object for caching.

Explicit Proxying and Pipelining

If clients are explicitly proxied and the session has multiple connections or is pipelined, no client bytes are displayed and the expanded server connections display no gain when the tree view is shown. This is because the SG appliance is downloading the content before serving it to the client.

What Is Not Displayed

The **Proxied Sessions page** does not display statistics for:

- IM (Yahoo, AOL, MSN), DNS, SOCKS, and Telnet
- Inbound ADN connections
- Bridged connections
- Administrative connections (Management Console, SSH console, SNMP, DSAT, access-logging, Director, and so on)
- Off-box processing connections (ICAP, DRTR, etc.)

Note: In some cases, an administrative or off-box connection might correspond to a specific client connection, for example, an ICAP AV scanning connection associated with a specific HTTP client connection. However, the byte counts collected from administrative or off-box connections are not included in the Active Sessions display.

Filtering the Display

Use the **Filter** drop-down list to filter the proxied session statistics.



Figure 5-12. Filtering Proxied Sessions

When you select a filter, a text field or popup displays so that you can enter filtering criteria.



If you select a filter, you must enter a filtering criteria (or select **None**) before clicking **Show**.

The following filters are available:

- Client Address
Filter by IP address and IP address and subnet mask.
- Client Port
- Server Address
Filter by IP address or hostname. Hostname filters automatically search for suffix matches. For example, if you filter for google.com, gmail.google.com is included in the results.
- Server Port
- Proxy
- Service (drop-down list)

The drop-down list enables you to filter for enabled services. If you filter for a service that is not supported for active sessions (see “[What Is Not Displayed](#)” on page 83), the resulting filtering list will be empty.

Viewing HTML and XML Views of Proxied Sessions Data

Access the following URLs to get HTML and XML views of active session statistics:

HTML: <https://SGIP:8082/AS/Sessions/>

XML: <https://SGIP:8082/AS/Sessions/xml>

Analyzing Bypassed Connections Statistics

The **Statistics > Active Sessions > Bypassed Connections** page displays data for all unintercepted TCP traffic.

When the appliance is first installed in an inline deployment, all services are bypassed by default. By analyzing the connection data in the **Bypassed Connections** page, you can review the types of traffic flowing through the appliance to identify traffic flows that would benefit from optimization. The **Bypassed Connections** page is also useful for identifying new types of traffic flowing through the appliance.

The **Bypassed Connections** page displays data for connections that were not intercepted because:

- ❑ A service has not been configured to intercept the traffic.
- ❑ A static or dynamic bypass rule caused the traffic to be bypassed.
- ❑ The interface transparent interception setting is disabled.

Viewing Bypassed Connections

To view bypassed connections:

1. Select **Statistics > Active Sessions > Bypassed Connections**.
2. (Optional) Select a filter from the **Filter** drop-down list.

See “[Filtering the Display](#)” on page 86 for more information about display filters.

The following figure shows an example of the **Bypassed Connections** page.

| Client | Server | Duration | Bypassed Bytes | Service Name | Details |
|-----------------|----------------|----------|----------------|-----------------|---------|
| 10.9.59.48:4509 | 10.2.2.51:135 | 30 sec | 444 | Endpoint Mapper | |
| 10.9.59.48:4510 | 10.2.2.51:1026 | 0 sec | 406 | Default | |
| 10.9.59.48:4511 | 10.2.2.51:1026 | 30 sec | 1,896 | Default | |
| 10.9.59.48:4513 | 10.2.1.64:135 | 30 sec | 444 | Endpoint Mapper | |
| 10.9.59.48:4514 | 10.2.1.64:1030 | 30 sec | 2,556 | Default | |
| 10.9.59.48:4515 | 10.2.2.51:389 | 0 sec | 3,143 | LDAP | |
| 10.9.59.48:4516 | 10.2.2.51:389 | 0 sec | 4 | LDAP | |
| 10.9.59.48:4520 | 10.2.2.51:135 | 30 sec | 444 | Endpoint Mapper | |
| 10.9.59.48:4521 | 10.2.2.51:1026 | 1 min | 4,676 | Default | |
| 10.9.59.48:4523 | 10.2.1.64:135 | 29 sec | 444 | Endpoint Mapper | |

Total Connections: 13

Figure 5-13. Bypassed Connections Page

Note the following:

- ❑ Unavailable connections (gray) indicate connections that are now closed.
- ❑ Previously-established connections displayed with (<--?-->) text indicate that the direction of these connections is unknown.
- ❑ One-way connections are displayed in color.

About the Bypassed Connection Statistics

The following table describes the column headings on the **Bypassed Connections** page.

Table 5-2. Table Column Heading Descriptions on the Bypassed Connections Page

| Column Heading | Description |
|----------------|--|
| Client | IP address and port of the client PC (or other downstream host). |
| Server | Server IP address and port number. |

Table 5-2. Table Column Heading Descriptions on the Bypassed Connections Page (Continued)

| Column Heading | Description |
|----------------|---|
| Duration | Displays the amount of time the connection has been established. |
| Bypassed Bytes | Displays the total number of bypassed bytes for the connection. |
| Service Name | Displays the service used by the connection. |
| Details | Provides additional information. For example: <ul style="list-style-type: none"> • One-way traffic (forward) • One-way traffic (reverse) • Previously Established • Bypassed because of network interface setting |

Filtering the Display

Use the **Filter** drop-down list to filter the bypassed connection statistics.



Figure 5-14. Filter Drop-Down List

When you select a filter, a text field or drop-down displays so that you can enter filtering criteria.



Figure 5-15. Filter Drop-Down

If you select a filter, you must enter a filtering criteria (or select **None**) before clicking **Show**.

The following filters are available:

- Client Address
 - Filter by IP address and IP address and subnet mask.
- Client Port
- Server Address
 - Filter by IP address or hostname. Hostname filters automatically search for suffix matches. For example, if you filter for google.com, gmail.google.com is included in the results.
- Server Port
- Service (drop-down list)
 - The drop-down list enables you to filter for enabled services. If you filter for a service that is not supported for active sessions (see [“What Is Not Displayed”](#) on page 83), the resulting filtered list will be empty.

Viewing HTML and XML Views of Bypassed Connections Data

Access the following URLs to get HTML and XML views of active session statistics

HTML: <https://SGIP:8082/AS/BypassedConnections/>

XML: <https://SGIP:8082/AS/BypassedConnections/xml>

Viewing Health Monitoring Statistics

The **Statistics > Health** page enables you to get more details about the current state of the health monitoring metrics. Health monitoring uses key hardware and software metrics to provide administrators with a remote view of the health of the system. See [Chapter 2: "Monitoring the SG Appliance"](#) for information about health monitoring.

Viewing Health Check Statistics

Use the **Statistics > Health Check** page to view the state of various health checks: whether the health check is enabled or disabled, if it is reporting the device or service to be healthy or sick, or if errors are being reported. Refer to the health check information in *Volume 5: Advanced Networking* for more information.

Viewing the Access Log

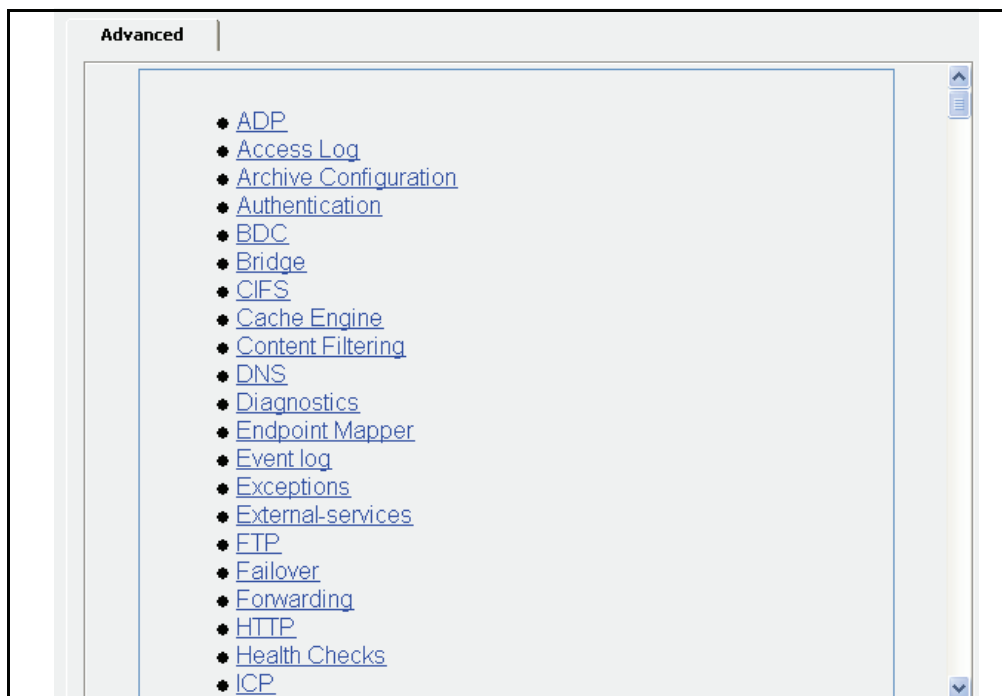
The **Statistics > Access Logging** pages enable you to view the log tail, log size, and upload status of the access log. Refer to *Volume 8: Access Logging* for more information.

Viewing Advanced Statistics

A variety of system statistics are conveniently located in one place and accessible by clicking the links listed in the Advanced tab of the Management Console.

To view system-wide advanced statistics:

1. Select **Statistics > Advanced**.



2. Click the appropriate link for the service you want to view.

A list of categories for that service displays.

Note: If you upgraded from SGOS 2.x or CacheOS 4.x and have log files generated by those versions, you can view or retrieve them through the **Statistics > Advanced > Access Log > Show Old Logs URL**.

3. To view the statistics for a particular category, click that category's link.
A window opens, detailing the relevant statistics.
4. Close the window when you have finished viewing the statistics.
5. To return to the list of links, either reselect **Statistics > Advanced** or click your browser's **Back** button.

Using the CLI show Command to View Statistics

You can use the `show` command to view a variety of different statistics. The following output lists the `show` options pertaining to topics in this chapter.

```
SGOS# show ?
cpu                CPU usage summary
disk               Disk status and information
health-checks     Health Checks statistics
http              HTTP settings
http-stats        HTTP statistics
im                IM information
ip-stats          TCP/IP statistics
p2p               Peer-to-peer information
```


| | |
|-------------------------|--------------------------------|
| resources | Allocation of system resources |
| snmp | SNMP statistics |
| streaming | Streaming information |
| system-resource-metrics | System Resource Metrics |

Appendix A: Glossary

A

| | |
|--------------------------------------|--|
| access control list | Allows or denies specific IP addresses access to a server. |
| access log | A list of all the requests sent to an appliance. You can read an access log using any of the popular log-reporting programs. When a client uses HTTP streaming, the streaming entry goes to the same access log. |
| account | A named entity that has purchased the appliance or the Entitlements from Blue Coat. |
| activation code | A string of approximately 10 characters that is generated and mailed to customers when they purchase the appliance. |
| active content stripping | Provides a way to identify potentially dangerous mobile or active content and scripts, and strip them out of a response. |
| active content types | Used in the Visual Policy Manager. Referring to Web Access policies, you can create and name lists of active content types to be stripped from Web pages. You have the additional option of specifying a customized message to be displayed to the user |
| administration access policy | A policy layer that determines who can access the SG appliance to perform administrative tasks. |
| administration authentication policy | A policy layer that determines how administrators accessing the SG appliance must authenticate. |
| Application Delivery Network (ADN) | A WAN that has been optimized for acceleration and compression by Blue Coat. This network can also be secured through the use of appliance certificates. An ADN network is composed of an ADN manager and backup ADN manager, ADN nodes, and a network configuration that matches the environment. |
| ADN backup manager | Takes over for the ADN manager in the event it becomes unavailable. See <i>ADN manager</i> . |
| ADN manager | Responsible for publishing the routing table to SG Clients (and to other SG appliances). |
| ADN optimize attribute | Controls whether to optimize bandwidth usage when connecting upstream using an ADN tunnel. |
| asx rewrite | Allows you to rewrite URLs and then direct a client's subsequent request to the new URL. One of the main applications of ASX file rewrites is to provide explicit proxy-like support for Windows Media Player 6.4, which cannot set explicit proxy mode for protocols other than HTTP. |
| audit | A log that provides a record of who accessed what and how. |

| | |
|----------------------------|---|
| authenticate-401 attribute | All transparent and explicit requests received on the port always use transparent authentication (cookie or IP, depending on the configuration). This is especially useful to force transparent proxy authentication in some proxy-chaining scenarios |
| authenticated content | Cached content that requires authentication at the origin content server (OCS). Supported authentication types for cached data include basic authentication and IWA (or NTLM). |
| authentication | Allows you to verify the identity of a user. In its simplest form, this is done through usernames and passwords. Much more stringent authentication can be employed using digital certificates that have been issued and verified by a Certificate Authority. <i>See also</i> basic authentication, proxy authentication, and SSL authentication. |
| authentication realm | Authenticates and authorizes users to access SG services using either explicit proxy or transparent proxy mode. These realms integrate third-party vendors, such as LDAP, Windows, and Novell, with the Blue Coat operating system. |
| authorization | The permissions given to an authenticated user. |
| B | |
| bandwidth class | A defined unit of bandwidth allocation. |
| bandwidth class hierarchy | Bandwidth classes can be grouped together in a class hierarchy, which is a tree structure that specifies the relationship among different classes. You create a hierarchy by creating at least one parent class and assigning other classes to be its children. |
| bandwidth management | Classify, control, and, if needed, limit the amount of bandwidth used by network traffic flowing in or out of an SG appliance. |
| basic authentication | The standard authentication for communicating with the target as identified in the URL. |
| BCAAA | Blue Coat Authentication and Authorization Agent. Allows SGOS 5.x to manage authentication and authorization for IWA, CA eTrust SiteMinder realms, Oracle COREid, Novell, and Windows realms. The agent is installed and configured separately from SGOS 5.x and is available from the Blue Coat Web site. |
| BCLP | Blue Coat Licensing Portal. |
| byte-range support | The ability of the SG appliance to respond to byte-range requests (requests with a Range : HTTP header). |
| C | |
| cache | An "object store," either hardware or software, that stores information (objects) for later retrieval. The first time the object is requested, it is stored, making subsequent requests for the same information much faster. A cache helps reduce the response time and network bandwidth consumption on future, equivalent requests. The SG appliance serves as a cache by storing content from many users to minimize response time and prevent extraneous network traffic. |
| cache control | Allows you to configure which content the SG appliance stores. |

| | |
|------------------------------|--|
| cache efficiency | A tab found on the Statistics pages of the Management Console that shows the percent of objects served from cache, the percent loaded from the network, and the percent that were non-cacheable. |
| cache hit | Occurs when the SG appliance receives a request for an object and can serve the request from the cache without a trip to the origin server. |
| cache miss | Occurs when the appliance receives a request for an object that is not in the cache. The appliance must then fetch the requested object from the origin server. . |
| cache object | Cache contents includes all objects currently stored by the SG appliance. Cache objects are not cleared when the SG appliance is powered off. |
| Certificate Authority (CA) | A trusted, third-party organization or company that issues digital certificates used to create digital signatures and public key/private key pairs. The role of the CA is to guarantee that the individuals or company representatives who are granted a unique certificate are who they claim to be. |
| child class (bandwidth gain) | The child of a parent class is dependent upon that parent class for available bandwidth (they share the bandwidth in proportion to their minimum/maximum bandwidth values and priority levels). A child class with siblings (classes with the same parent class) shares bandwidth with those siblings in the same manner. |
| client consent certificates | A certificate that indicates acceptance or denial of consent to decrypt an end user's HTTPS request. |
| client-side transparency | A way of replacing the appliance IP address with the Web server IP address for all port 80 traffic destined to go to the client. This effectively conceals the SG appliance address from the client and conceals the identity of the client from the Web server. |
| concentrator | An SG appliance, usually located in a data center, that provides access to data center resources, such as file servers. |
| content filtering | A way of controlling which content is delivered to certain users. SG appliances can filter content based on content categories (such as gambling, games, and so on), type (such as http, ftp, streaming, and mime type), identity (user, group, network), or network conditions. You can filter content using vendor-based filtering or by allowing or denying access to URLs. |
| D | |
| default boot system | The system that was successfully started last time. If a system fails to boot, the next most recent system that booted successfully becomes the default boot system. |
| default proxy listener | <i>See proxy service (d efault).</i> |
| denial of service (DoS) | <p>A method that hackers use to prevent or deny legitimate users access to a computer, such as a Web server. DoS attacks typically send many request packets to a targeted Internet server, flooding the server's resources and making the system unusable. Any system connected to the Internet and equipped with TCP-based network services is vulnerable to a DoS attack.</p> <p>The SG appliance resists DoS attacks launched by many common DoS tools. With a hardened TCP/IP stack, SG appliance resists common network attacks, including traffic flooding.</p> |

| | |
|---------------------------------|---|
| destination objects | Used in Visual Policy Manager. These are the objects that define the target location of an entry type. |
| detect protocol attribute | Detects the protocol being used. Protocols that can be detected include: HTTP, P2P (eDonkey, BitTorrent, FastTrack, Gnutella), SSL, and Endpoint Mapper. |
| diagnostic reporting | Found in the Statistics pane, the Diagnostics tab allows you to control whether Daily Heartbeats and/or Blue Coat Monitoring are enabled or disabled. |
| directives | Commands used in installable lists to configure forwarding and SOCKS gateway. |
| DNS access | A policy layer that determines how the SG appliance processes DNS requests. |
| domain name system (DNS) | An Internet service that translates domain names into IP addresses. <i>See also</i> private DNS or public DNS. |
| dynamic bypass | Provides a maintenance-free method for improving performance of the SG appliance by automatically compiling a list of requested URLs that return various kinds of errors. |
| dynamic real-time rating (DRTR) | Used in conjunction with the Blue Coat Web Filter (BCWF), DRTR (also known as <i>dynamic categorization</i>) provides real-time analysis and content categorization of requested Web pages to solve the problem of new and previously unknown uncategorized URLs—those not in the database. When a user requests a URL that has not already been categorized by the BCWF database (for example, a brand new Web site), the SG appliance dynamic categorization service analyzes elements of the requested content and assigns a category or categories. The dynamic service is consulted <i>only</i> when the installed BCWF database does not contain category information for an object. |
| E | |
| early intercept attribute | Controls whether the proxy responds to client TCP connection requests before connecting to the upstream server. When early intercept is disabled, the proxy delays responding to the client until after it has attempted to contact the server. |
| ELFF-compatible format | A log type defined by the W3C that is general enough to be used with any protocol. |
| emulated certificates | Certificates that are presented to the user by SG appliance when intercepting HTTPS requests. Blue Coat emulates the certificate from the server and signs it, copying the subjectName and expiration. The original certificate is used between the SG appliance and the server. |
| encrypted log | A log is encrypted using an external certificate associated with a private key. Encrypted logs can only be decrypted by someone with access to the private key. The private key is not accessible to the SG appliance. |
| EULA | End user license agreement. |
| event logging | Allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The appliance can also notify you by email if an event is logged. <i>See also</i> access logging. |

| | |
|---------------------------------|---|
| explicit proxy | <p>A configuration in which the browser is explicitly configured to communicate with the proxy server for access to content.</p> <p>This is the default for the SG appliance, and requires configuration for both browser and the interface card.</p> |
| extended log file format (ELFF) | <p>A variant of the common log file format, which has two additional fields at the end of the line—the referer and the user agent fields.</p> |
| F | |
| fail open/closed | <p>Failing open or closed applies to forwarding hosts and groups and SOCKS gateways. Fail open or closed applies when health checks are showing sick for each forwarding or SOCKS gateway target in the applicable fail-over sequence. If no systems are healthy, the SG appliance fails open or closed, depending on the configuration. If closed, the connection attempt simply fails.</p> <p>If open, an attempt is made to connect without using any forwarding target (or SOCKS gateway). Fail open is usually a security risk; fail closed is the default if no setting is specified.</p> |
| filtering | <p>See content filtering.</p> |
| forward proxy | <p>A proxy server deployed close to the clients and used to access many servers. A forward proxy can be explicit or transparent.</p> |
| FTP | <p>See Native FTP; Web FTP.</p> |
| G | |
| gateway | <p>A device that serves as entrance and exit into a communications network.</p> |
| H | |
| hardware serial number | <p>A string that uniquely identifies the appliance; it is assigned to each unit in manufacturing.</p> |
| health check tests | <p>The method of determining network connectivity, target responsiveness, and basic functionality. The following tests are supported:</p> <ul style="list-style-type: none">• ICMP• TCP• SSL• HTTP• HTTPS• Group• Composite and reference to a composite result• ICAP• Websense• DRTR rating service |

| | |
|----------------------------------|---|
| health check type | <p>The kind of device or service the specific health check tests. The following types are supported:</p> <ul style="list-style-type: none">• Forwarding host and forwarding group• SOCKS gateway and SOCKS gateway group• CAP service and ICAP service group• Websense off-box service and Websense off-box service group• DRTR rating service• User-defined host and a user-defined composite |
| heartbeat | <p>Messages sent once every 24 hours that contain the statistical and configuration data for the SG appliance, indicating its health. Heartbeats are commonly sent to system administrators and to Blue Coat. Heartbeats contain no private information, only aggregate statistics useful for pre-emptively diagnosing support issues.</p> <p>The SG appliance sends emergency heartbeats whenever it is rebooted. Emergency heartbeats contain core dump and restart flags in addition to daily heartbeat information.</p> |
| host affinity | <p>The attempt to direct multiple connections by a single user to the same group member. Host affinity is closely tied to load balancing behavior; both should be configured if load balancing is important.</p> |
| host affinity timeout | <p>The host affinity timeout determines how long a user remains idle before the connection is closed. The timeout value checks the user's IP address, SSL ID, or cookie in the host affinity table.</p> |
| | |
| inbound traffic (bandwidth gain) | <p>Network packets flowing into the SG appliance. Inbound traffic mainly consists of the following:</p> <ul style="list-style-type: none">• Server inbound: Packets originating at the origin content server (OCS) and sent to the SG appliance to load a Web object.• Client inbound: Packets originating at the client and sent to the SG appliance for Web requests. |
| installable lists | <p>Installable lists, comprised of directives, can be placed onto the SG appliance in one of the following ways:</p> <ul style="list-style-type: none">• Creating the list using the SG text editor• Placing the list at an accessible URL• Downloading the directives file from the local system |
| integrated host timeout | <p>An integrated host is an origin content server (OCS) that has been added to the health check list. The host, added through the <code>integrate_new_hosts</code> property, ages out of the integrated host table after being idle for the specified time. The default is 60 minutes.</p> |
| intervals | <p>Time period from the completion of one health check to the start of the next health check.</p> |
| IP reflection | <p>Determines how the client IP address is presented to the origin server for explicitly proxied requests. All proxy services contain a <code>reflect-ip</code> attribute, which enables or disables sending of client's IP address instead of the SG's IP address.</p> |

issuer keyring The keyring used by the SG appliance to sign emulated certificates. The keyring is configured on the appliance and managed through policy.

L

licensable component (LC) (Software) A subcomponent of a license; it is an option that enables or disables a specific feature.

license Provides both the right and the ability to use certain software functions within an AV (or SG) appliance. The license key defines and controls the license, which is owned by an account.

listener The service that is listening on a specific port. A listener can be identified by any destination IP/subnet and port range. Multiple listeners can be added to each service.

live content Also called live broadcast. Used in streaming, it indicates that the content is being delivered fresh.

LKF License key file.

load balancing A way to share traffic requests among multiple upstream systems or multiple IP addresses on a single host.

local bypass list A list you create and maintain on your network. You can use a local bypass list alone or in conjunction with a central bypass list. *See* bypass list.

local policy file Written by enterprises (as opposed to the central policy file written by Blue Coat); used to create company- and department-specific advanced policies written in the Blue Coat Policy Language (CPL).

log facility A separate log that contains a single logical file and supports a single log format. It also contains the file's configuration and upload schedule information as well as other configurable information such as how often to rotate (switch to a new log) the logs at the destination, any passwords needed, and the point at which the facility can be uploaded.

log format The type of log that is used: NCSA/Common, SQUID, ELFF, SurfControl, or Websense.

The proprietary log types each have a corresponding pre-defined log format that has been set up to produce exactly that type of log (these logs cannot be edited). In addition, a number of other ELFF type log formats are also pre-defined (im, main, p2p, ssl, streaming). These can be edited, but they start out with a useful set of log fields for logging particular protocols understood by the SG appliance. It is also possible to create new log formats of type ELFF or Custom which can contain any desired combination of log fields.

log tail The access log tail shows the log entries as they get logged. With high traffic on the SG appliance, not all access log entries are necessarily displayed. However, you can view all access log information after uploading the log.

M

MACH5 SGOS 5 MACH5 Edition.

| | |
|-----------------------------------|--|
| Management Console | A graphical Web interface that lets you to manage, configure, monitor, and upgrade the SG appliance from any location. The Management Console consists of a set of Web pages and Java applets stored on the SG appliance. The appliance acts as a Web server on the management port to serve these pages and applets. |
| management information base (MIB) | Defines the statistics that management systems can collect. A managed device (gateway) has one or more MIBs as well as one or more SNMP agents, which implements the information and management functionality defined by a specific MIB. |
| maximum object size | The maximum object size stored in the SG appliance. All objects retrieved that are greater than the maximum size are delivered to the client but are not stored in the SG appliance. |
| MIME/FILE type filtering | Allows organizations to implement Internet policies for both uploaded and downloaded content by MIME or FILE type. |
| multi-bit rate | The capability of a single stream to deliver multiple bit rates to clients requesting content from appliances from within varying levels of network conditions (such as different connecting bandwidths and traffic). |
| multicast | Used in streaming; the ability for hundreds or thousands of users to play a single stream. |
| multicast aliases | Used in streaming; a streaming command that specifies an alias for a multicast URL to receive an .nsc file. The .nsc files allows the multicast session to obtain the information in the control channel |
| multicast station | Used in streaming; a defined location on the proxy where the Windows Media player can retrieve streams. A multicast station enables multicast transmission of Windows Media content from the cache. The source of the multicast-delivered content can be a unicast-live source, a multicast (live) source, and simulated live (video-on-demand content converted to scheduled live content). |
| multimedia content services | Used in streaming; multimedia support includes Real Networks, Microsoft Windows Media, Apple QuickTime, MP3, and Flash. |
| N | |
| name inputting | Allows an SG appliance to resolve host names based on a partial name specification. When a host name is submitted to the DNS server, the DNS server resolves the name to an IP address. If the host name cannot be resolved, Blue Coat adds the first entry in the name-inputting list to the end of the host name and resubmits it to the DNS server |
| native FTP | Native FTP involves the client connecting (either explicitly or transparently) using the FTP protocol; the SG appliance then connects upstream through FTP (if necessary). |
| NCSA common log format | Blue Coat products are compatible with this log type, which contains only basic HTTP access information. |
| network address translation (NAT) | The process of translating private network (such as intranet) IP addresses to Internet IP addresses and vice versa. This methodology makes it possible to match private IP addresses to Internet IP addresses even when the number of private addresses outnumbers the pool of available Internet addresses. |

| | |
|--|---|
| non-cacheable objects | <p>A number of objects are not cached by the Blue Coat appliance because they are considered non-cacheable. You can add or delete the kinds of objects that the appliance considers non-cacheable. Some of the non-cacheable request types are:</p> <ul style="list-style-type: none">• Pragma no-cache, requests that specify non-cached objects, such as when you click refresh in the Web browser.• Password provided, requests that include a client password.• Data in request that include additional client data.• Not a GET request. |
| .nsc file | <p>Created from the multicast station definition and saved through the browser as a text file encoded in a Microsoft proprietary format. Without an .nsc file, the multicast station definition does not work.</p> |
| NTP | <p>To manage objects in an appliance, an SG appliance must know the current Universal Time Coordinates (UTC) time. By default, the SG appliance attempts to connect to a Network Time Protocol (NTP) server to acquire the UTC time. SG appliance includes a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the NTP tab.</p> |
| <h2>O</h2> | |
| object (used in caching) | <p>An object is the item that is stored in an appliance. These objects can be frequently accessed content, content that has been placed there by content publishers, or Web pages, among other things.</p> |
| object (used in Visual Policy Manager) | <p>An object (sometimes referred to as a condition) is any collection or combination of entry types you can create individually (user, group, IP address/subnet, and attribute). To be included in an object, an item must already be created as an individual entry.</p> |
| object pipelining | <p>This patented algorithm opens as many simultaneous TCP connections as the origin server will allow and retrieves objects in parallel. The objects are then delivered from the appliance straight to the user's desktop as fast as the browser can request them.</p> |
| origin content server (OCS) | <p>Also called origin server. This is the original source of the content that is being requested. An appliance needs the OCS to acquire data the first time, to check that the content being served is still fresh, and to authenticate users.</p> |
| outbound traffic (bandwidth gain) | <p>Network packets flowing out of the SG appliance. Outbound traffic mainly consists of the following:</p> <ul style="list-style-type: none">• Client outbound: Packets sent to the client in response to a Web request.• Server outbound: Packets sent to an OCS or upstream proxy to request a service. |
| <h2>P</h2> | |
| PAC (Proxy AutoConfiguration) scripts | <p>Originally created by Netscape, PACs are a way to avoid requiring proxy hosts and port numbers to be entered for every protocol. You need only enter the URL. A PAC can be created with the needed information and the local browser can be directed to the PAC for information about proxy hosts and port numbers.</p> |
| packet capture (PCAP) | <p>Allows filtering on various attributes of the Ethernet frame to limit the amount of data collected. You can capture packets of Ethernet frames going into or leaving an SG appliance.</p> |

| | |
|--------------------------------------|---|
| parent class (bandwidth gain) | A class with at least one child. The parent class must share its bandwidth with its child classes in proportion to the minimum/maximum bandwidth values or priority levels. |
| passive mode data connections (PASV) | Data connections initiated by an FTP client to an FTP server. |
| pipelining | See object pipelining. |
| policies | Groups of rules that let you manage Web access specific to the needs of an enterprise. Policies enhance SG appliance feature areas such as authentication and virus scanning, and let you control end-user Web access in your existing infrastructure. See also refresh policies. |
| policy-based bypass list | Used in policy. Allows a bypass based on the properties of the client, unlike static and dynamic bypass lists, which allow traffic to bypass the appliance based on destination IP address. See also bypass lists and dynamic bypass. |
| policy layer | A collection of rules created using Blue Coat CPL or with the VPM. |
| pragma: no cache (PNC) | A metatag in the header of a request that requires the appliance to forward a request to the origin server. This allows clients to always obtain a fresh copy (<i>of the request?</i>). |
| proxy | <p>Caches content, filters traffic, monitors Internet and intranet resource usage, blocks specific Internet and intranet resources for individuals or groups, and enhances the quality of Internet or intranet user experiences.</p> <p>A proxy can also serve as an intermediary between a Web client and a Web server and can require authentication to allow identity based policy and logging for the client.</p> <p>The rules used to authenticate a client are based on the policies you create on the SG appliance, which can reference an existing security infrastructure—LDAP, RADIUS, IWA, and the like.</p> |
| Proxy Edition | SGOS 5 Proxy Edition. |
| proxy service | The proxy service defines the ports, as well as other attributes. that are used by the proxies associated with the service. |
| proxy service (default) | The default proxy service is a service that intercepts all traffic not otherwise intercepted by other listeners. It only has one listener whose action can be set to bypass or intercept. No new listeners can be added to the default proxy service, and the default listener and service cannot be deleted. Service attributes can be changed. |
| public key certificate | An electronic document that encapsulates the public key of the certificate sender, identifies this sender, and aids the certificate receiver to verify the identity of the certificate sender. A certificate is often considered valid if it has been digitally signed by a well-known entity, which is called a Certificate Authority (such as VeriSign). |
| public virtual IP (VIP) | Maps multiple servers to one IP address and then propagates that information to the public DNS servers. Typically, there is a public VIP known to the public Internet that routes the packets internally to the private VIP. This enables you to “hide” your servers from the Internet. |

R

| | |
|---|--|
| real-time streaming protocol (RTSP) | A standard method of transferring audio and video and other time-based media over Internet-technology based networks. The protocol is used to stream clips to any RTP-based client. |
| reflect client IP attribute | Enables the sending of the client's IP address instead of the SG's IP address to the upstream server. If you are using an application delivery network (ADN), this setting is enforced on the concentrator proxy through the Configuration > App. Delivery Network > Tunneling tab. |
| registration | An event that binds the appliance to an account, that is, it creates the Serial#, Account association. |
| remote authentication dial-in user service (RADIUS) | Authenticates user identity via passwords for network access. |
| reverse proxy | A proxy that acts as a front-end to a small number of pre-defined servers, typically to improve performance. Many clients can use it to access the small number of predefined servers. |
| routing information protocol (RIP) | Designed to select the fastest route to a destination. RIP support is built into Blue Coat appliances. |
| router hops | The number of jumps a packet takes when traversing the Internet. |

S

| | |
|-------------------------------|--|
| secure shell (SSH) | Also known as Secure Socket Shell. SSH is an interface and protocol that provides strong authentication and enables you to securely access a remote computer. Three utilities—login, ssh, and scp—comprise SSH. Security via SSH is accomplished using a digital certificate and password encryption. Remember that the Blue Coat SG appliance requires SSH1. An SG appliance supports a combined maximum of 16 Telnet and SSH sessions. |
| serial console | A third-party device that can be connected to one or more Blue Coat appliances. Once connected, you can access and configure the appliance through the serial console, even when you cannot access the appliance directly. |
| server certificate categories | The hostname in a server certificate can be categorized by BCWF or another content filtering vendor to fit into categories such as banking, finance, sports. |
| server portals | Doorways that provide controlled access to a Web server or a collection of Web servers. You can configure Blue Coat SG appliances to be server portals by mapping a set of external URLs onto a set of internal URLs. |
| server-side transparency | The ability for the server to see client IP addresses, which enables accurate client-access records to be kept. When server-side transparency is enabled, the appliance retains client IP addresses for all port 80 traffic to and from the SG appliance. In this scheme, the client IP address is always revealed to the server. |
| service attributes | Define the parameters, such as explicit or transparent, cipher suite, and certificate verification, that the SG appliance uses for a particular service. . |

| | |
|---|---|
| SG appliance | A Blue Coat security and cache box that can help manage security and content on a network. |
| sibling class (bandwidth gain) | A bandwidth class with the same parent class as another class. |
| simple network management protocol (SNMP) | The standard operations and maintenance protocol for the Internet. It uses MIBs, created or customized by Blue Coat, to handle <i>(needs completion)</i> . |
| simulated live | Used in streaming. Defines playback of one or more video-on-demand files as a scheduled live event, which begins at a specified time. The content can be looped multiple times, or scheduled to start at multiple start times throughout the day. |
| SmartReporter log type | A proprietary ELFF log type that is compatible with the SmartFilter SmartReporter tool. |
| SOCKS | A proxy protocol for TCP/IP-based networking applications that allows users transparent access across the firewall. If you are using a SOCKS server for the primary or alternate forwarding gateway, you must specify the appliance's ID for the identification protocol used by the SOCKS gateway. The machine ID should be configured to be the same as the appliance's name. |
| SOCKS proxy | A generic way to proxy TCP and UDP protocols. The SG appliance supports both SOCKSv4/4a and SOCKSv5; however, because of increased username and password authentication capabilities and compression support, Blue Coat recommends that you use SOCKS v5. |
| splash page | Custom message page that displays the first time you start the client browser. |
| split proxy | Employs co-operative processing at the branch and the core to implement functionality that is not possible in a standalone proxy. Examples of split proxies include: <ul style="list-style-type: none">• Mapi Proxy• SSL Proxy |
| SQUID-compatible format | A log type that was designed for cache statistics and is compatible with Blue Coat products. |
| squid-native log format | The Squid-compatible format contains one line for each request. |
| SSL authentication | Ensures that communication is with "trusted" sites only. Requires a certificate issued by a trusted third party (Certificate Authority). |
| SSL interception | Decrypting SSL connections. |
| SSL proxy | A proxy that can be used for any SSL traffic (HTTPS or not), in either forward or reverse proxy mode. |
| static route | A manually-configured route that specifies the transmission path a packet must follow, based on the packet's destination address. A static route specifies a transmission path to another network. |

| | |
|----------------------|---|
| statistics | Every Blue Coat appliance keeps statistics of the appliance hardware and the objects it stores. You can review the general summary, the volume, resources allocated, cache efficiency, cached contents, and custom URLs generated by the appliance for various kinds of logs. You can also check the event viewer for every event that occurred since the appliance booted. |
| stream | A flow of a single type of data, measured in kilobits per second (Kbps). A stream could be the sound track to a music video, for example. |
| SurfControl log type | A proprietary log type that is compatible with the SurfControl reporter tool. The SurfControl log format includes fully-qualified usernames when an NTLM realm provides authentication. The simple name is used for all other realm types. |
| syslog | An event-monitoring scheme that is especially popular in Unix environments. Most clients using Syslog have multiple devices sending messages to a single Syslog daemon. This allows viewing a single chronological event log of all of the devices assigned to the Syslog daemon. The Syslog format is: "Date Time Hostname Event." |
| system cache | The software cache on the appliance. When you clear the cache, all objects in the cache are set to expired. The objects are not immediately removed from memory or disk, but a subsequent request for any object requested is retrieved from the origin content server before it is served. |

T

| | |
|-------------------------------------|---|
| time-to-live (TTL) value | Used in any situation where an expiration time is needed. For example, you do not want authentication to last beyond the current session and also want a failed command to time out instead of hanging the box forever. |
| traffic flow (bandwidth gain) | <p>Also referred to as <i>flow</i>. A set of packets belonging to the same TCP/UDP connection that terminate at, originate at, or flow through the SG appliance. A single request from a client involves two separate connections. One of them is from the client to the SG appliance, and the other is from the SG appliance to the OCS. Within each of these connections, traffic flows in two directions—in one direction, packets flow out of the SG appliance (outbound traffic), and in the other direction, packets flow into the SG (inbound traffic). Connections can come from the client or the server. Thus, traffic can be classified into one of four types:</p> <ul style="list-style-type: none">• Server inbound• Server outbound• Client inbound• Client outbound <p>These four traffic flows represent each of the four combinations described above. Each flow represents a single direction from a single connection.</p> |
| transmission control protocol (TCP) | TCP, when used in conjunction with IP (Internet Protocol) enables users to send data, in the form of message units called packets, between computers over the Internet. TCP is responsible for tracking and handling, and reassembly of the packets; IP is responsible for packet delivery. |
| transparent proxy | A configuration in which traffic is redirected to the SG appliance without the knowledge of the client browser. No configuration is required on the browser, but network configuration, such as an L4 switch or a WCCP-compliant router, is required. |

| | |
|----------------------------------|--|
| trial period | Starting with the first boot, the trial period provides 60 days of free operation. All features are enabled during this time. |
| U | |
| unicast alias | Defines an name on the appliance for a streaming URL. When a client requests the alias content on the appliance, the appliance uses the URL specified in the unicast-alias command to request the content from the origin streaming server. |
| universal time coordinates (UTC) | An SG appliance must know the current UTC time. By default, the appliance attempts to connect to a Network Time Protocol (NTP) server to acquire the UTC time. If the SG appliance cannot access any NTP servers, you must manually set the UTC time. |
| URL filtering | <i>See</i> content filtering. |
| URL rewrite rules | Rewrite the URLs of client requests to acquire the streaming content using the new URL. For example, when a client tries to access content on <code>www.mycompany.com</code> , the appliance is actually receiving the content from the server on <code>10.253.123.123</code> . The client is unaware that <code>mycompany.com</code> is not serving the content; however, the appliance access logs indicate the actual server that provides the content. |
| W | |
| WCCP | Web Cache Communication Protocol. Allows you to establish redirection of the traffic that flows through routers. |
| Web FTP | Web FTP is used when a client connects in explicit mode using HTTP and accesses an <code>ftp://</code> URL. The SG appliance translates the HTTP request into an FTP request for the OCS (if the content is not already cached), and then translates the FTP response with the file contents into an HTTP response for the client. |
| <i>Websense</i> log type | A Blue Coat proprietary log type that is compatible with the Websense reporter tool. |
| X | |
| XML responder | HTTP XML service that runs on an external server. |
| XML requestor | XML realm. |

Index

A

- access logging 87
- active sessions 76
 - bypassed connections 84
 - proxied sessions 77
- ADN history 68
- appliance certificate 9
- automatic service information, enabling 46

B

- bandwidth gain 64
- bandwidth management 68
- bandwidth usage 64
- Blue Coat monitoring, enabling 58
- Blue Coat SG
 - deleting image 43
 - deleting objects from 44
 - locking and unlocking a system 42
 - managing 40
 - replacing a system 40, 42
 - restarting 33
 - setting the default system to boot 41
 - single-disk 44
 - system defaults 34
 - upgrading 37, 38
 - viewing details 40
- bypassed bytes 63
- bypassed connections 84
- byte distribution 65

C

- cache contents 74
- CacheOS 4.x, logs, retrieving 88
- caching
 - clearing the system cache 36
 - objects by size 74
 - purging the DNS cache 36
 - restarting the Blue Coat SG 33
- capturing packets, *see* packet capturing
- community strings 21
- concurrent users, viewing 71
- core image
 - restart options 57

CPU

- utilization 70
- CPU monitoring
 - configuring 59
- CPU utilization 70
- cpu utilization 70

D

- data allocation 73
- default service 64
- defaults, restoring system defaults 34
- deleting objects from the Blue Coat SG 44
- diagnostics
 - Blue Coat monitoring 58
 - core image restart options 57
 - CPU monitoring 59
 - heartbeats 58
 - packet capturing 52
 - sending service information 48
 - sending service information automatically 46
 - snapshot jobs 50
- Director
 - communicating with 11
 - SG appliance registration and setup 9
- disk
 - multi-disk Blue Coat SG 43
 - reinitialization 43
 - single-disk Blue Coat SG 44
- disk use 70, 72
- disks 70
- DNS
 - cache, purging 36
- document
 - conventions 7

E

- empty system 40
- event logging
 - configuration, viewing 18
 - contents, viewing 19
 - event notification 16
 - log levels 15
 - log size 16
 - overview 15

event logging statistics 75

F

failover statistics 76

filter expressions for packet capturing 52

G

graph scale 61

H

health monitoring

 configuring 23

 Director 23

 general metrics 26

 license expiration 25

 licensing metrics 26

 notification 26

 properties, modifying 28

 requirements 23

 status metrics 27

 thresholds 24

 viewing statistics 30

health statistics 87

heartbeats, configuring 58

I

image, deleting 43

L

licensing

 restore-default deletions 35

locking and unlocking Blue Coat SG systems 42

logging

see access logging and event logging

 SNMP 20

 syslog event monitoring 17

logs

 CacheOS 4.x, retrieving 88

 SGOS 2.x, retrieving 88

M

Management Console, troubleshooting, browser
 troubleshooting 37

memory use 70, 72

MIBs 20

O

objects

 deleting from Blue Coat SG 44

 served by size 74

P

packet capturing

 about 52

 capturing 53

 common filter expressions 52

 file name format 52

 uploading data 57

 viewing current data 56

protocol details 68

proxied sessions

 MMS connections 81

 multiple connections 81

 tree view 82

purging the DNS cache 36

R

rebooting, *see* restarting 33

replacing a Blue Coat SG system 42

reporting

 event logging 15

 syslog event monitoring 17

resources

 concurrent users, viewing 71

restart

 core image 57

restarting the Blue Coat SG

 restart options 33

 setting the default system to boot 41

restoring system defaults 34

S

service information

 enabling automatic 46

 sending 48

SG appliance

 active sessions 76

 bypassed bytes 63

 bypassed connections 84

 byte distribution 65

 controlling access 9

 registering with Director 9

 traffic history 65

 traffic mix 62

SGOS 2.x, logs, retrieving 88

Simple Network Management Protocol, *see* SNMP

snapshot jobs
 creating and editing 50

SNMP
 community strings 21
 enabling 20
 MIB variables 20
 MIBs 20
 traps 22

SSH-Console service 10

SSHv2 host key 10

SSL accelerator cards, statistics, viewing 15

statistics
 cached objects by size 74
 CPU utilization 70
 data allocation 73
 graph scale 61
 objects served by size 74
 system summary 12

syslog event monitoring 17

system cache
 clearing 36

system cache,
 troubleshooting 37
system defaults, restoring 34
system summary 12

T

traffic history 65
 supported proxies and services 66
traffic mix 62
 supported proxies and services 66
traps 22
troubleshooting
 browsers 37
 licenses disappear after restore-defaults
 command 35

U

upgrading
 overview 37
 system image from PC 38
 through Management Console 38

