

Blue Coat® Systems SG™ Appliance

Volume 3: Web Communication Proxies

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: 231-02840
Document Revision: SGOS 5.2.2—09/2007

Contents

Contact Information

Chapter 1: Introduction

Document Conventions	7
----------------------------	---

Chapter 2: Managing Instant Messaging Protocols

About the Risks of Instant Messaging	9
About the Blue Coat IM Proxies	9
HTTP Proxy Support	9
Instant Messaging Proxy Authentication	9
Access Logging	10
Managing Skype	10
About Instant Message Network Inter-activity	10
Recommended Deployments	10
About Instant Messaging Reflection	11
Configuring SG Appliance IM Proxies	13
Configuring IM Services	14
Configuring IM DNS Redirection	17
The Default IM Hosts	18
Configuring Instant Messaging HTTP Handoff	18
Configuring IM Alerts	19
Configuring IM Clients	20
General Configuration	20
AOL Messenger Client Explicit Proxy Configuration	20
MSN Messenger Client Explicit Proxy Configuration	22
Yahoo Messenger Client Explicit Proxy Configuration	23
Policy Examples	24
Example 1: File Transfer	24
Example 2: Send an IM Alert Message	26
Reference: Equivalent IM CLI Commands	28
Reference: Access Log Fields	28
Reference: CPL Triggers, Properties, and Actions	29
Triggers	29
Properties and Actions	29
IM History Statistics	29

Chapter 3: Managing Streaming Media

Section A: Concepts: Streaming Media

About Streaming Media	34
Supported Streaming Media Clients and Protocols	34

Supported Streaming Media Clients and Servers	34
Supported Streaming Protocols	35
About Processing Streaming Media Content.....	38
Delivery Methods	38
Serving Content: Live Unicast	38
Serving Content: Video-on-Demand Unicast	38
Serving Content: Multicast Streaming.....	38
About HTTP Handoff.....	39
Limiting Bandwidth	39
Caching Behavior: Protocol Specific	42
Caching Behavior: Video on Demand	42
Caching Behavior: Live Splitting.....	42
Multiple Bit Rate Support.....	43
Bitrate Thinning	43
Pre-Populating Content	43
About Fast Streaming (Windows Media).....	44
About QoS Support	44
About Windows Media Over RTSP	44
License Requirements	44
Upgrade/Downgrade Issues	44
Management Console and CLI Changes	45
Supported Streaming Features	45
Other Supported Features	46
Supported VPM Properties and Actions	46
Bandwidth Management	47
About Streaming Media Authentication	47
Windows Media Server-Side Authentication	47
Windows Media Proxy Authentication.....	47
Real Media Proxy Authentication	48
QuickTime Proxy Authentication	48
Section B: Configuring Streaming Media	
Configuring Streaming Services	49
Configuring Streaming Proxies.....	52
Limiting Bandwidth	53
Configuring Bandwidth Limits—Global.....	54
Configuring Bandwidth Limits—Protocol-Specific.....	54
Configuring Bandwidth Limitation—Fast Start (WM)	55
Configuring the SG Appliance Multicast Network	55
Configuring Media Server Authentication Type (Windows Media)	56
Related CLI Syntax to Manage Streaming.....	56
Reference: Access Log Fields.....	57

Reference: CPL Triggers, Properties, and Actions	58
Triggers.....	58
Properties and Actions.....	58
Streaming History Statistics	58
Viewing Windows Media Statistics	58
Viewing Real Media Statistics.....	59
Viewing QuickTime Statistics.....	60
Viewing Current and Total Streaming Data Statistics	60
Viewing Streaming Bandwidth Gain.....	62
Section C: Additional Configuration Tasks—Windows Media (CLI)	
Managing Multicast Streaming for Windows Media	63
About Multicast Stations	63
About Broadcast Aliases	64
Creating a Multicast Station	64
Monitoring the Multicast Station.....	66
Managing Simulated Live Content (Windows Media)	67
About Simulated Live Content	67
Creating a Broadcast Alias for Simulated Live Content	68
ASX Rewriting (Windows Media).....	69
About ASX Rewrite	69
Section D: Windows Media Player	
Configuring Windows Media Player	72
Windows Media Player Inter-activity Notes	73
Striding	73
Other Notes.....	73
Section E: RealPlayer	
Configuring RealPlayer.....	75
Section F: QuickTime Player	
Configuring QuickTime Player.....	79

Appendix A: Glossary

Index

Chapter 1: Introduction

A *proxy* filters traffic, monitors Internet and intranet resource usage, blocks or allows specific Internet and intranet resources for individuals or groups, and enhances the quality of Internet or intranet user experiences.

The Blue Coat SG appliance Instant Messaging (IM) proxies allow you to control, track, and record communications that occur over AOL, MSN, or Yahoo IM clients on your corporate networks. The Streaming proxies allow you to alter allowed bandwidth and manage the broadcasts of streaming content over Microsoft and RealNetworks (with limited support for Apple) protocols.

This document contains the following chapters:

- ❑ Chapter 2: "Managing Instant Messaging Protocols" on page 9
- ❑ Chapter 3: "Managing Streaming Media" on page 33

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: Managing Instant Messaging Protocols

This chapter discusses how to control Instant Messaging (IM) activity through the SG appliance.

About the Risks of Instant Messaging

Instant Messaging use in an enterprise environment creates security concerns because regardless of how network security is configured, IM connections can occur from any established protocol, such as HTTP or SOCKS, on any open port. Because it is common for coworkers to use IM to communicate, especially in remote offices, classified company information can be exposed outside the network. Viruses and other malicious code can also be introduced into the network from file sharing through IM clients.

About the Blue Coat IM Proxies

The SG appliance serves as an IM proxy. With policy, you can control IM actions by allowing or denying IM communications and file sharing based on users (both employee identities and IM handles), groups, file types and names, and other triggers. All IM communications can be logged and archived for review.

The SG appliance supports the AOL, MSN, and Yahoo IM client protocols. For the most current list of supported client versions, refer to the most current *Release Notes* for this release.

HTTP Proxy Support

The SG appliance supports instant messaging through the HTTP proxy. IM clients are configured to connect to IM services through HTTP, which allows IM activity from behind restrictive firewalls.

The application of policies and IM activity logging is accomplished by the HTTP proxy handing off IM communications to the IM proxy.

Notes

- ❑ AOL and Yahoo clients lose certain features when connected through HTTP proxy rather than through SOCKS or transparent connections:
- ❑ AOL—Direct connections, file transfers, and files sharing are not available.
- ❑ Yahoo—Client cannot create a chat room.

Instant Messaging Proxy Authentication

The SG appliance supports explicit proxy authentication if explicit SOCKS V5 proxy is specified in the IM client configuration.

Because the IM protocols do not natively support proxy authentication, authentication for transparently redirected clients is not supported because policies requiring authentication would deny transparently redirected clients.

Notes

Consider the following proxy authentication notes, which apply to IM clients using HTTP proxy:

- ❑ AOL IM—Proxy authentication is supported.
- ❑ MSN IM (5.0 and above)—The SG appliance supports MSN/Live Messenger if the appliance is configured to use HTTP ProxyAuth code 407, not HTTP auth code 401.
- ❑ Yahoo IM—Yahoo IM clients do not have proxy authentication configuration abilities.

Access Logging

Access log entries occur from various IM actions, such as logging on or joining a chat room. By default, the SG appliance uses the Blue Coat IM access log format:

```
date time c-ip cs-username cs-auth-group cs-protocol x-im-method x-im-  
user-id x-im-user-name x-im-user-state x-im-client-info x-im-buddy-id  
x-im-buddy-name x-im-buddy-state x-im-chat-room-id x-im-chat-room-type  
x-im-chat-room-members x-im-message-text x-im-message-size x-im-  
message-route x-im-message-type x-im-file-path x-im-file-size s-action
```

For a reference list and descriptions of used log fields, see [“Reference: Access Log Fields”](#) on page 28.

Managing Skype

Skype is the most used IM service outside of the United States. It provides free PC-to-PC calling using VoIP. Skype communication is based on Peer-to-Peer technology. Managing Skype communications requires the creation of firewall and SG appliance policies, procedures that are outside the scope of this chapter.

See the Blue Coat *Controlling Skype* Technical Brief, available on the Blue Coat Web site Download page.

About Instant Message Network Inter-activity

This section discusses IM deployment and describes IM reflection, which is how the SG appliance policy dictates IM communications.

Recommended Deployments

Blue Coat recommends the following deployments:

- ❑ For large networks with unimpeded Internet access, Blue Coat recommends transparently redirecting the IM protocols to the SG appliance, which requires the SG appliance bridging feature or an L4 switch or WCCP.
- ❑ For networks that do not allow outbound access, Blue Coat recommends using the SOCKS proxy and configuring policy and content filtering denials for HTTP requests to IM servers.

About Instant Messaging Reflection

IM reflection allows you to contain IM traffic within the enterprise network, which further reduces the risk of exposing company-confidential information through public IM networks or allow a client to incur a virus or malicious code. Normally, an IM sent from one buddy to another is sent to and from an IM service. With IM reflection, IM traffic between buddies, including chat messaging, on the same network never has to travel beyond the SG appliance. This includes IM users who login to two different SG appliances configured in a hierarchy (proxy chaining).

IM Reflection with Fail Open

When the SG appliance policy is configured to fail open, IM reflection operates essentially the same as passthrough mode. All messages are allowed in and out of the network. The following diagram illustrates IM processes with SG appliance fail open policy.

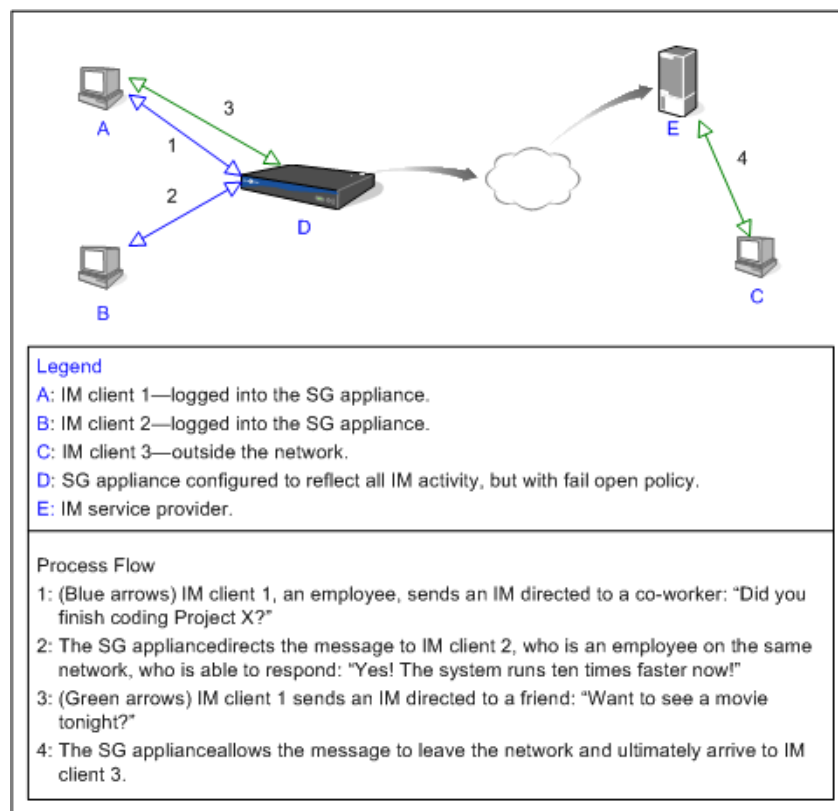


Figure 2-1. IM Reflection with SG appliance fail open policy.

IM Reflection With Fail Closed

If the SG appliance is configured with fail closed policy, messages cannot leave the network (they never reach the IM service provider). Only clients on allowed enterprise networks can send and receive IMs. The following diagram illustrates IM processes with SG appliance fail closed policy.

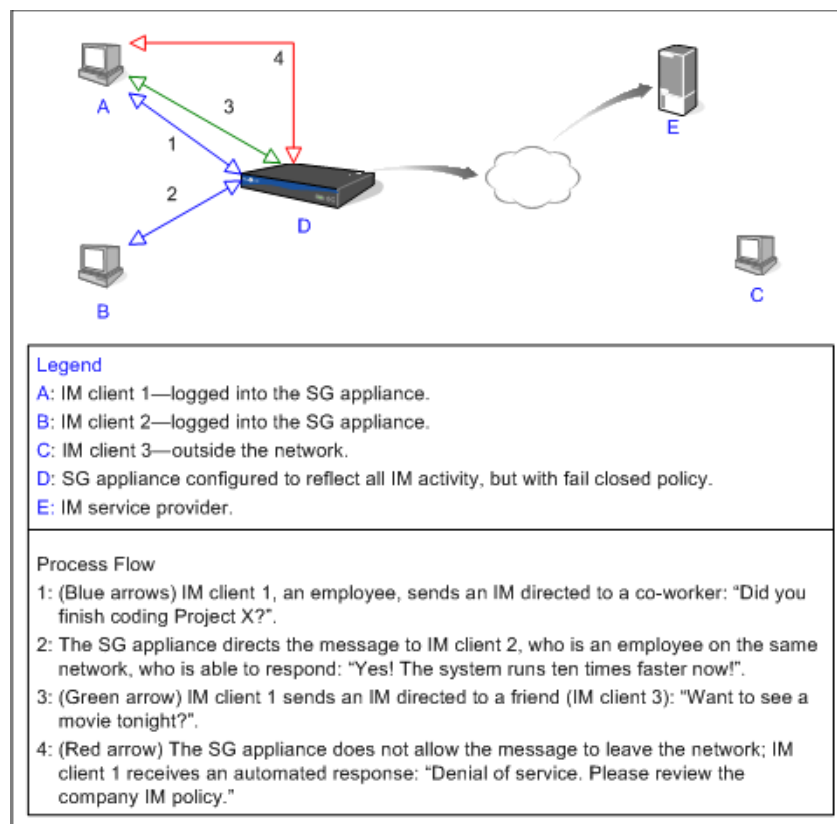


Figure 2-2. IM Reflection with SG appliance fail close policy

IM Reflection With A Hierarchy Of Proxies

While the previous two sections document the conceptual fail open/fail closed functionality, larger, more typical enterprise networks have users logging in through different primary SG appliance appliances. IM reflection involving clients in different buildings and even on different sites is still possible by using SOCKS and HTTP forwarding, policy, and an SG appliance hierarchy. The following diagram illustrates IM processes with SG appliance proxy chaining and a combination of fail open/fail closed policies.

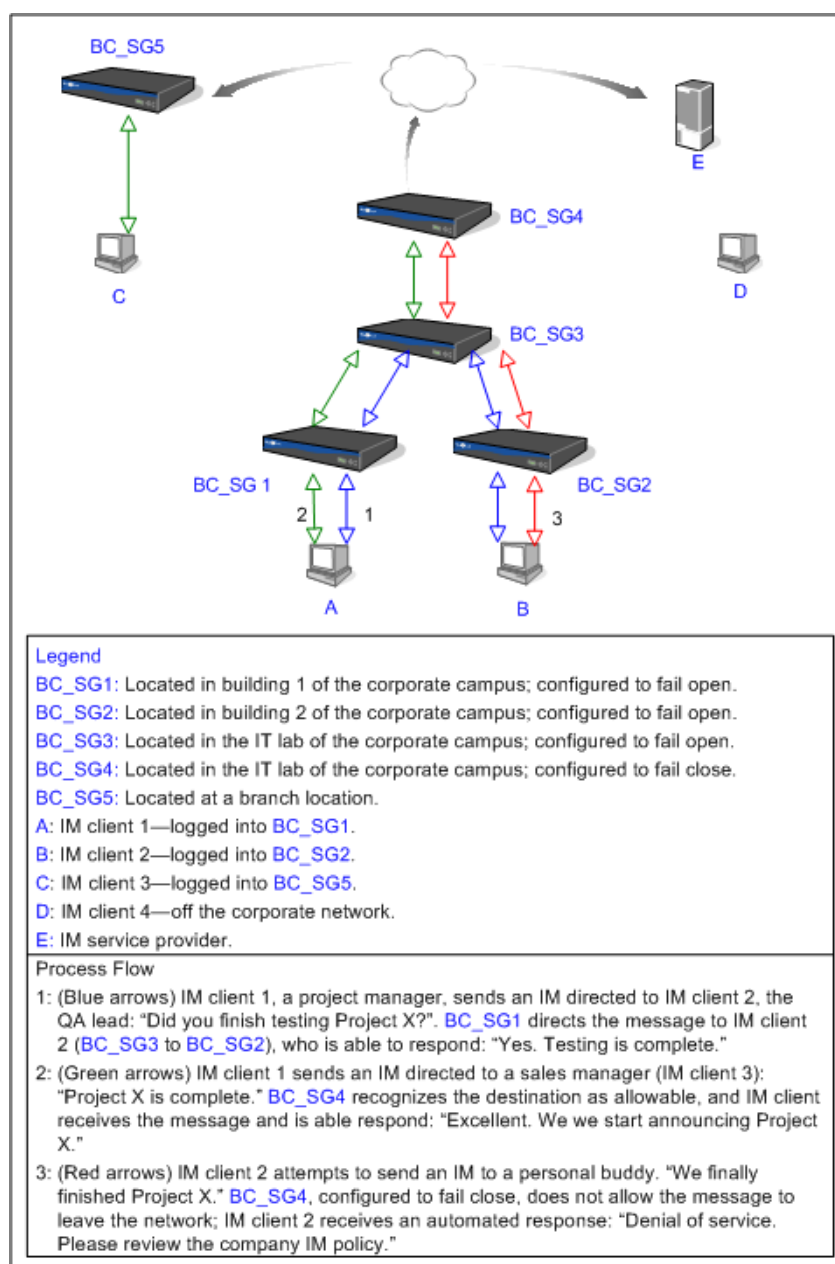


Figure 2-3. Proxy chaining deployment with fail open/fail closed policies.

Configuring SG Appliance IM Proxies

This chapter contains the following sections:

- ❑ "Configuring IM Services" on page 14
- ❑ "Configuring IM DNS Redirection" on page 17
- ❑ "The Default IM Hosts" on page 18
- ❑ "Configuring Instant Messaging HTTP Handoff" on page 18
- ❑ "Configuring IM Alerts" on page 19

Configuring IM Services

Defaults:

- ❑ Proxy Edition: Upon upgrade and on new systems, the SG appliance has IM services configured for transparent connections on the following ports:
 - AOL-IM: 5190
 - MSN-IM: 1863 and 6891
 - Yahoo-IM: 5050 and 5101
- ❑ MACH5 Edition: IM services are not created and are not included in trend data.

Notes:

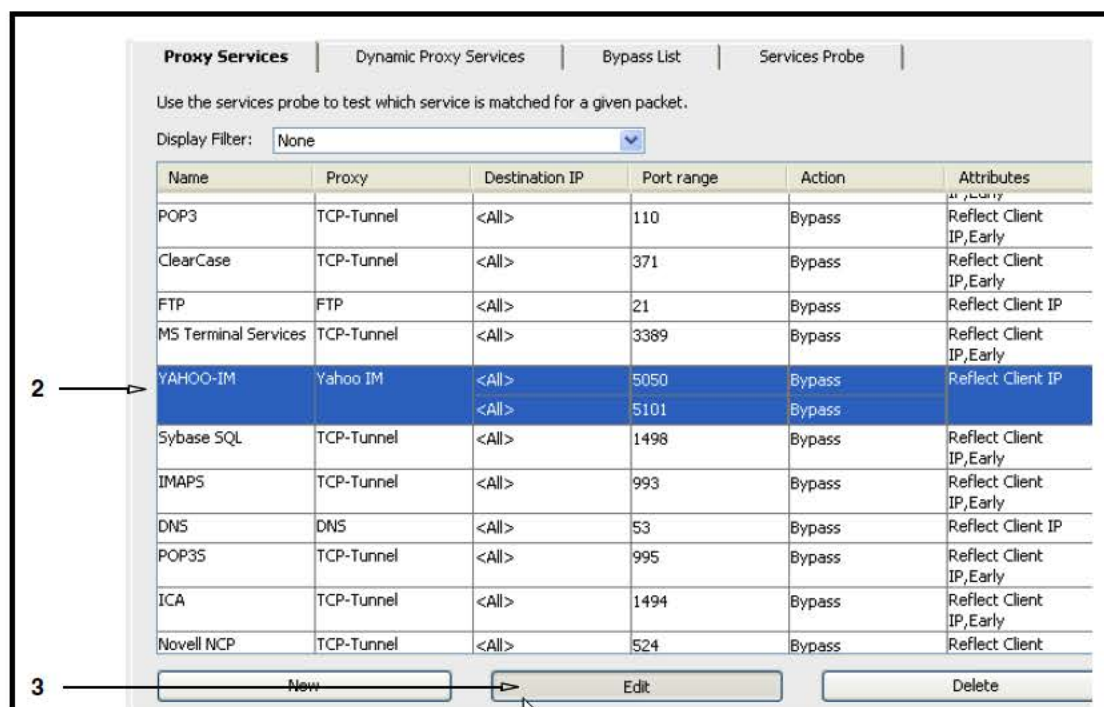
- ❑ MSN port 1863 and Yahoo port 5050 are the default client login ports. MSN port 6891 and Yahoo port 5101 are the default for client-to-client direct connections and file transfers. If these ports are not enabled:
- ❑ Client-to-client direct connections do not occur.
- ❑ After a file transfer request is allowed by the SG appliance, the resulting data is sent directly from one client to another without passing through the SG appliance:
 - For MSN: The above bullet point only applies to MSN version previous to and including 6.0. Post-6.0 versions use a dynamic port for file transfers; therefore, port 6891 is not required for the SG appliance to intercept file transfers.
 - For Yahoo: The above bullet only applies to standard file transfer requests. Port 5101 must be enabled to allow file list requests.

Note: All file transfers for AOL clients are handled through the default (5190) or specified client login port.

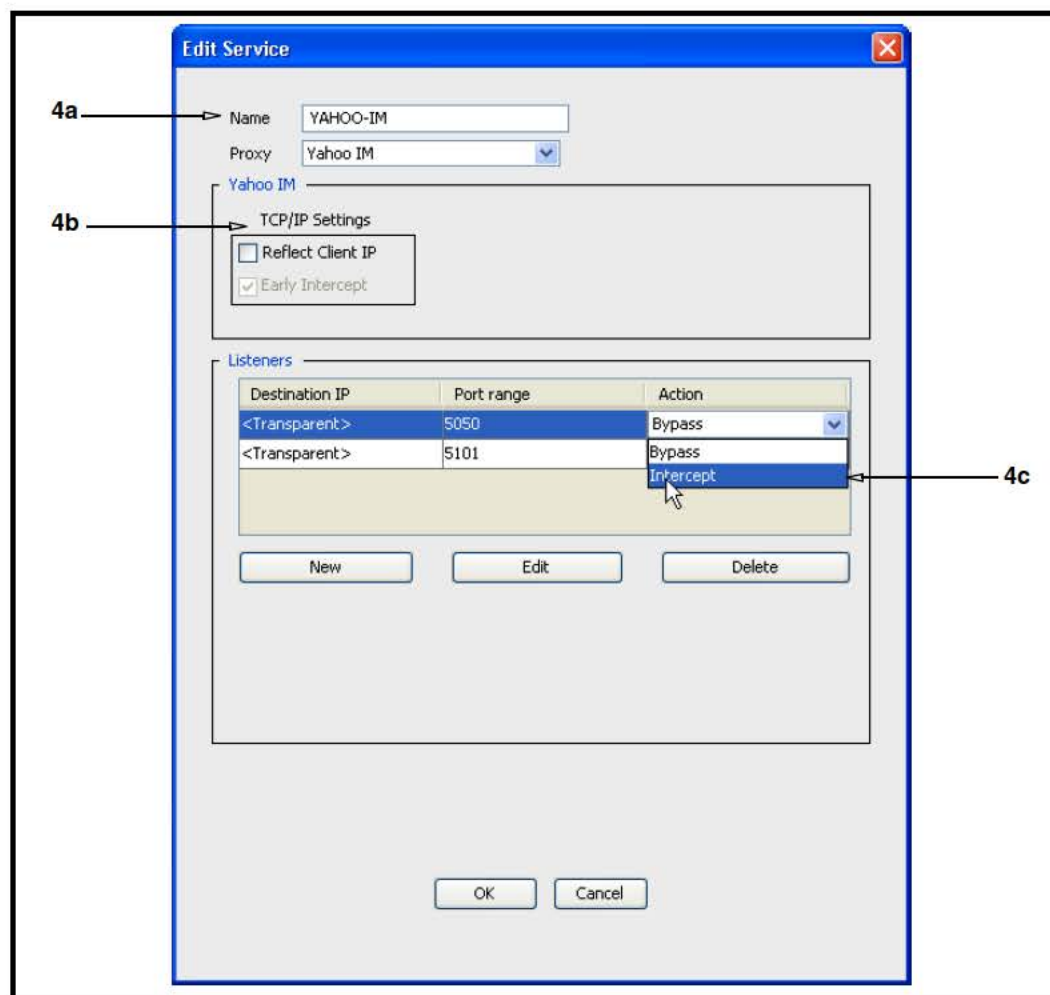
By default, these services are configured be **Transparent** and in **Bypass** mode. The following procedure describes how to change them to **Intercept** mode, and explains other attributes within the service.

To configure the IM proxies services attributes:

1. From the Management Console, select **Configuration > Services > Proxy Services**.



2. Scroll the list of services to display the default one of the IM service lines (this example uses Yahoo). Notice the **Action** is **Bypass**. You can select **Intercept** from the drop-down list, but for the purposes of this procedure, select the service line to highlight it.
3. Click **Edit**. The Edit Service dialog appears with the default settings displays.



4. Configure the service attributes:
 - a. In the **Name** field, enter a name that intuitively labels this service. This example accepts the default name.
 - b. The **TCP/IP Settings** options allow you to manage the data connections:
 - **Reflect Client IP**: If this is enabled, the connection to the IM server appears to come from the client, not the SG appliance.
 - **Early Intercept**: Not valid for this service.
 - c. In the **Listeners** field, select **Intercept** from the drop-down list; the SG appliance must intercept the IM connection. Perform this step for both ports

Note: You can also change the mode from **Bypass** to **Intercept** from the main services page.

- d. Click **OK**.
 5. Click **Apply**.
- Result: The IM service status appears in Management Console.

The screenshot shows the 'Proxy Services' configuration window. It has tabs for 'Dynamic Proxy Services', 'Bypass List', and 'Services Probe'. Below the tabs, there is a 'Display Filter' dropdown set to 'None'. A table lists the configured services:

Name	Proxy	Destination IP	Port range	Action	Attributes
MS Terminal Services	TCP-Tunnel	<All>	3389	Bypass	Reflect Client IP, Early
YAHOO-IM	Yahoo IM	<Transparent>	5050	Intercept	Reflect Client IP
		<Transparent>	5101	Intercept	

Figure 2-4. The Configured IM Listener

6. (Optional) Configure AOL and MSN IM proxies to **Intercept**.

Now that the IM listeners are configured, you can configure the IM proxies.

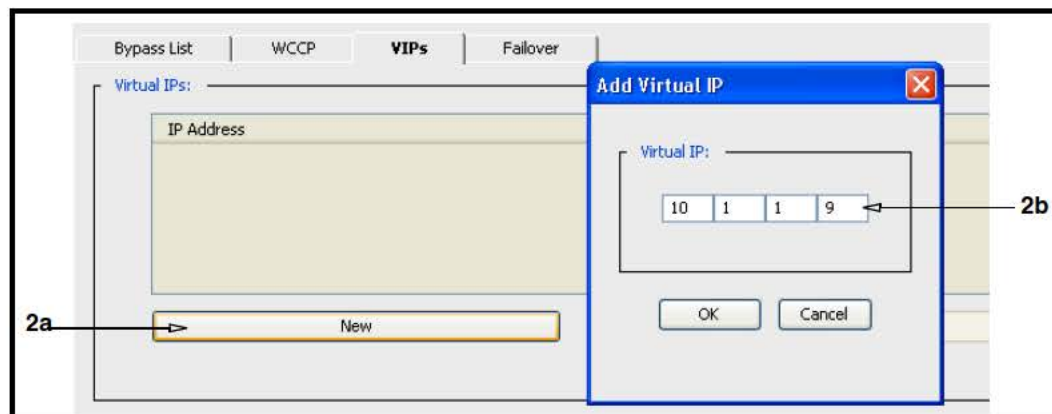
Configuring IM DNS Redirection

The SG appliance is configured as an IM proxy that performs a DNS redirection for client requests. This provides greater control because it prevents IM clients from making outside connections.

The IM clients provide the DNS lookup to the IM server, which the SG appliance DNS module uses to connect to the IM server. To the client, the SG appliance appears to be the IM server. A virtual IP address used only for IM must be configured, as it is used to represent the IM server address for all IM protocols.

To configure DNS redirection for IM:

1. Select **Configuration > Network > Advanced > VIPs**.

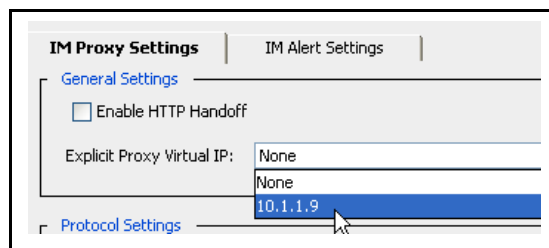


2. Create a virtual IP address:
 - a. Click **New**. The Add Virtual IP dialog appears.
 - b. Enter a unique IP address (used only to represent IM connections).
 - c. Click **OK** to add the VIP to the list.
3. Click **Apply**.
4. From the Management Console, select **Configuration > Services > IM Proxies > IM Proxy Settings**.

5. In the **General Settings** field, select the VIP from the **Explicit Proxy Virtual IP** drop-down list.
6. Click **Apply**.

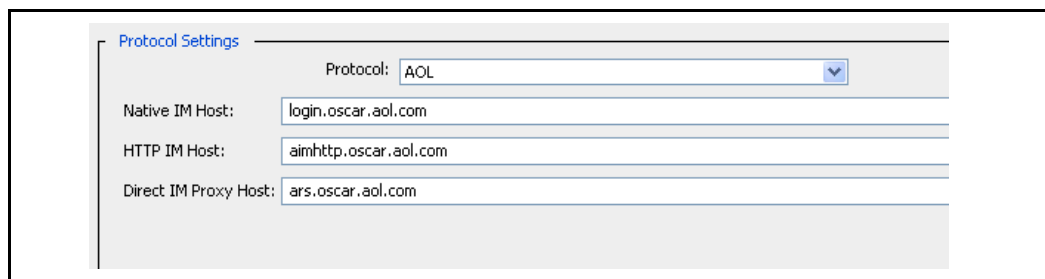
Result: IM clients regard the SG appliance as the IM server.

Remain on this screen and continue to the next section.



The Default IM Hosts

Each IM client has hard-coded IM hosts. The SG appliance displays these values on the **Configuration > Services > IM Proxies > IM Proxy Settings** tab, which vary in number and fields dependent upon the selected IM protocol. Do not alter these hosts unless the client experiences a hard-coded change.



Configuring Instant Messaging HTTP Handoff

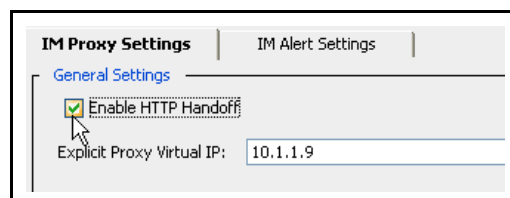
HTTP handoff allows the Blue Coat HTTP proxy to handle requests from supported IM protocols. If HTTP handoff is disabled, requests are passed through, and IM-specific policies are not applied. Enable HTTP handoff if you create and apply IM policy.

To allow a specific IM client to connect using the HTTP protocol through the SG appliance and that IM protocol has not been licensed, disable HTTP handoff to allow the traffic to be treated as plain HTTP traffic and to avoid an error in the licensing check performed by the IM module. This might be also be necessary to temporarily pass through traffic from new versions of IM clients that are not yet supported by Blue Coat.

To enable HTTP handoff:

1. From the Management Console, select **Configuration > Services > IM Proxies > IM Proxy Settings**.
2. In the **General Settings** field, select **Enable HTTP Handoff**.
3. Click **Apply**.

Result: IM-specific policies are applicable on IM communications.



Configuring IM Alerts

A SG appliance IM alert is an IM message sent to clients upon an action triggered by policy. An IM alert contains two elements:

- ❑ **Admin buddy names:** You can assign an administrator buddy name for each client type. An administrator buddy name can be a registered name user handle or a fictitious handle. The benefit of using a registered name is that users can send IM messages to the administrator directly to report any issues, and that communication can be logged for tracking and record-keeping. By default, the SG appliance assigns each IM protocol the admin buddy name: Blue Coat SG appliance.
- ❑ **Exception message delivery method:** Alert messages can be delivered in the same window or spawn a new window.

To configure IM alert components:

1. From the Management Console, select **Configuration > Services > IM Proxies > IM Alert Settings**.

The screenshot shows the 'IM Alert Settings' configuration page. It includes fields for 'Admin buddy names' for AOL, MSN, and Yahoo, and a section for 'Exception message delivery' with two radio button options and a text box for a prefix message.

2. In the **Admin buddy names** field, enter the handle or handles to represent the administrator. In this example, the company sanctions AOL Messenger as the one used for internal communications. IM alerts are sent from **Example Corp IT**. MSN and Yahoo are acceptable for personal use, but a created policy denies file transfers. Alerts are sent from **Example Corp HR**.
3. Specify the exceptions message delivery method:
 - a. **Send exception messages in a separate window (out-of-band)**—If an exception occurs, the user receives the message in a separate IM window.
 - b. **Send exception messages in the existing window (in-band)**—If an exception occurs, the message appears in the same IM window. The message appears to be sent by the buddy on the other end, with the exception that when in a chat room, the message always appears to be sent by the configured Admin buddy name. You can enter a prefix message that appears in the client window before the message. For example: **Inappropriate IM use. Refer to Employee Conduct Handbook concerning Internet usage.**

Note: Regardless of the IM exception delivery configuration, IM alert messages triggered by policy based on certain protocol methods are always sent out-of-band because a specific buddy is not associated.

4. Click **Apply**.

SG appliance IM proxy configuration is complete. The final step is to configure IM clients to send traffic to the SG appliance.

Configuring IM Clients

This section describes how to configure the IM clients to send traffic through the SG appliance.

General Configuration

As each IM client has different menu structures, the procedures to configure them differ. This section provides the generic tasks that need to be completed.

Explicit Proxy

Perform the following tasks on the IM client:

1. Navigate to the Connection Preferences dialog.
2. Select **Use Proxies**.
3. Select proxy type as **SOCKS V5**.
4. Enter the SG appliance IP address.
5. Enter the SOCKS port number; the default is **1080**.
6. Enter authentication information, if required.

Transparent Proxy

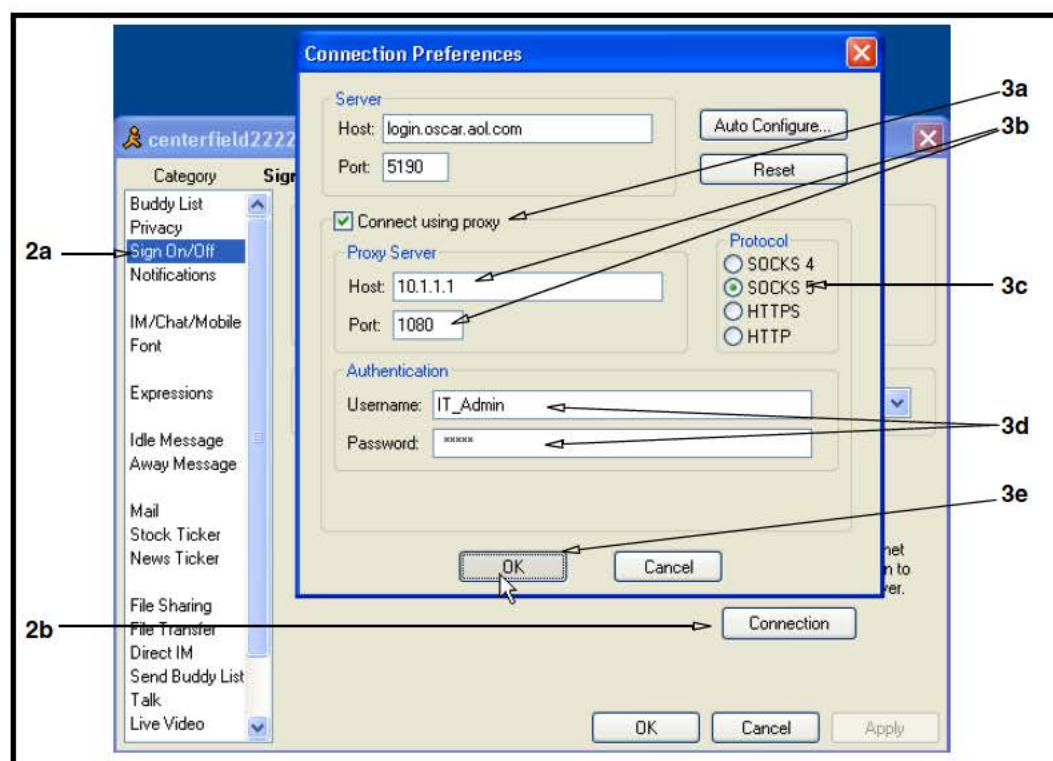
IM clients do not require any configuration changes for transparent proxy. An L4 switch or inline SG appliance routes the traffic.

AOL Messenger Client Explicit Proxy Configuration

The following example configures a Yahoo Messenger client for explicit proxy.

Note: This example uses AOL Messenger 5.9. Other versions might vary.

1. Select **My AIM > Edit Options > Edit Preferences**.



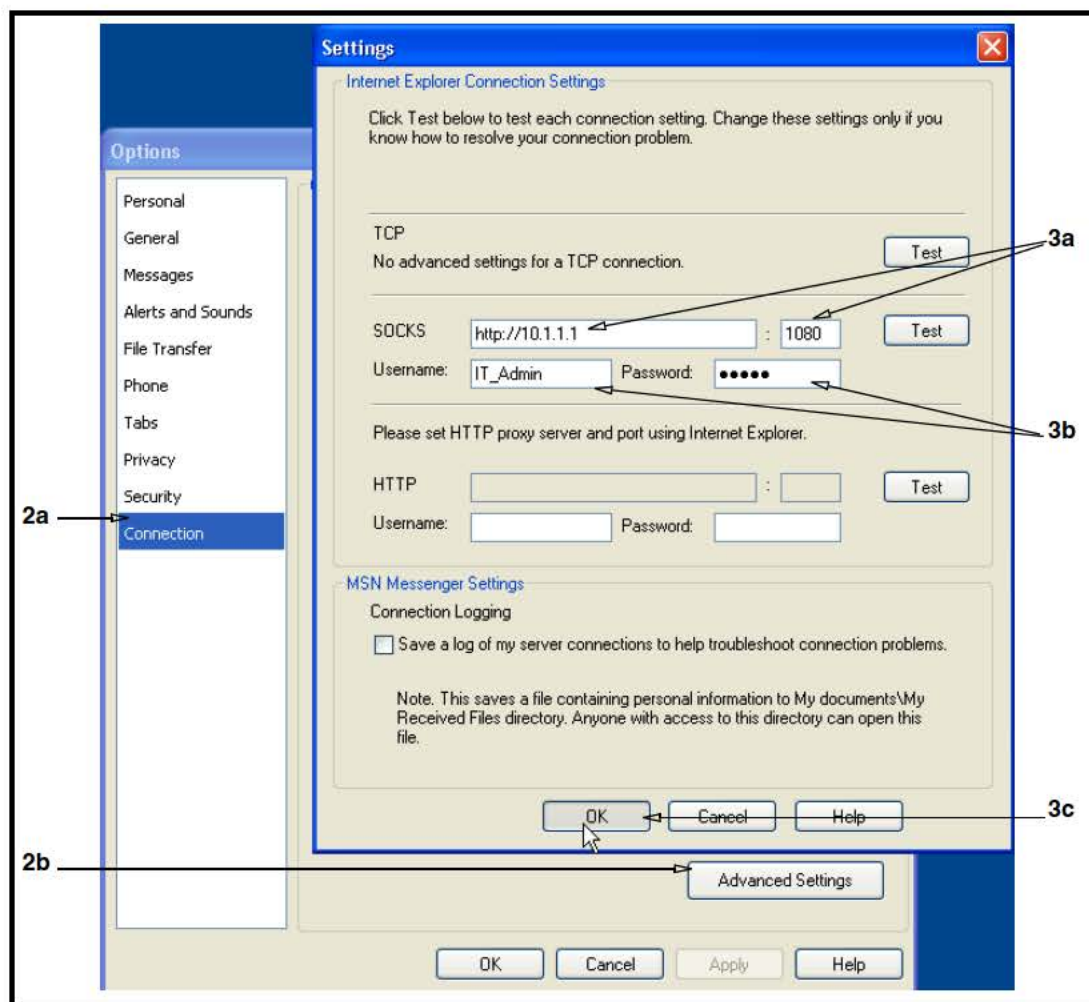
2. Navigate to Connection Preferences:
 - a. Select **Sign On/Off**.
 - b. Click **Connection**.
3. Configure the proxy settings:
 - a. Select **Connect using proxy**.
 - b. In the **Host** field, enter the SG appliance IP address. If the default port is **1080**, accept it; if not, change it to port **1080**.
 - c. Select **SOCKS 5**.
 - d. If authentication is required on the SG appliance, enter the authentication user name and password.
 - e. Click **OK** to close the Connections Preferences dialog.
4. Click **OK** to close the Preferences dialog. Result: the AOL client now sends traffic to the SG appliance.

MSN Messenger Client Explicit Proxy Configuration

The following example configures a Yahoo Messenger client for explicit proxy.

Note: This example uses MSN Messenger 7.5. Other versions might vary.

1. From MSN Messenger, select **Tools > Options**.



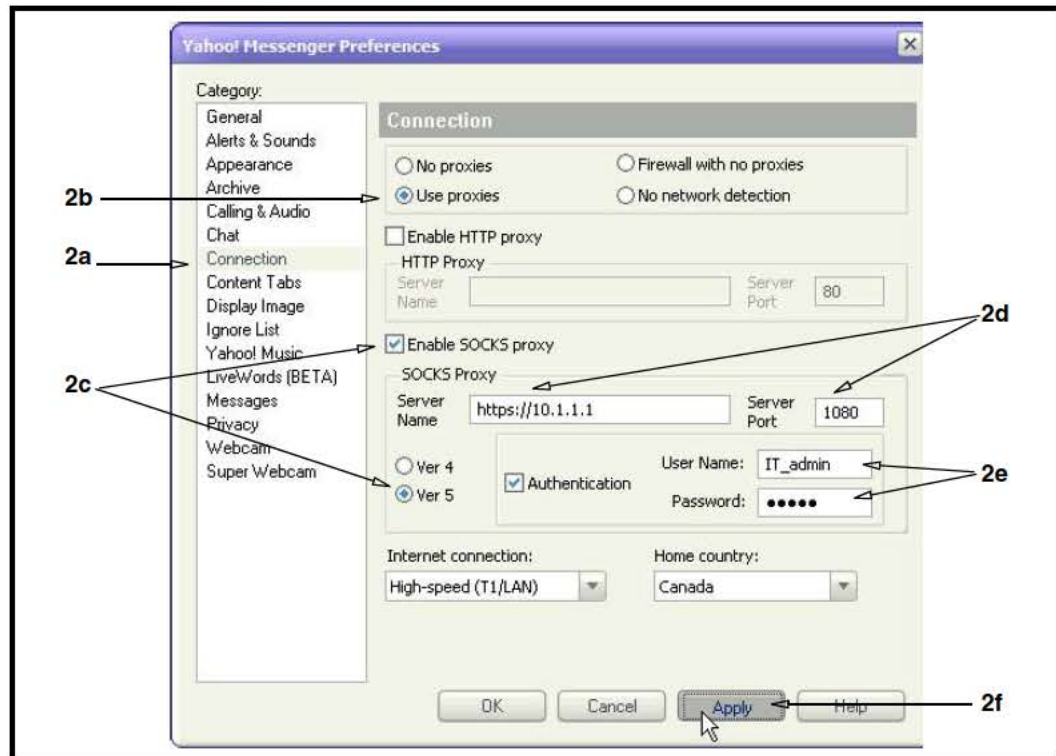
2. Navigate to Settings:
 - a. Click **Connection**.
 - b. Click **Advanced Settings**. The Settings dialog appears.
3. Configure the proxy settings:
 - a. In the **SOCKS** field, enter the SG appliance IP address. If the default port is **1080**, accept it; if not, change it to port **1080**.
 - b. If authentication is required on the SG appliance, enter the authentication user name and password.
 - c. Click **OK**.
4. Click **OK** to close the **Options** dialog. Result: the MSN client now sends traffic to the SG appliance.

Yahoo Messenger Client Explicit Proxy Configuration

The following example configures a Yahoo Messenger client for explicit proxy.

Note: This example uses Yahoo Messenger 7.0. Other versions might vary.

1. From Yahoo Messenger, select **Messenger > Preferences**.



2. Configure the following features:
 - a. Click **Connection**.
 - b. Select **Use proxies**.
 - c. Select **Enable SOCKS proxy**; select **Ver 5**.
 - d. Enter the SG appliance IP address. If the default port is **1080**, accept it; if not, change it to port **1080**.
 - e. If authentication is required on the SG appliance, enter the authentication user name and password.
 - f. Click **Apply** and **OK**. Result: the Yahoo client now sends traffic to the SG appliance.

Notes

If Yahoo Messenger is configured for explicit proxy (SOCKS) through the SG appliance, the IM voice chat feature is disabled. Any client attempting a voice chat with a client behind the SG appliance firewall receives an error message. The voice data stream is carried by default on port 5001; therefore, you can create and open this port and configure Yahoo IM to use transparent proxy. However, the SG appliance only supports the voice data in pass-through mode.

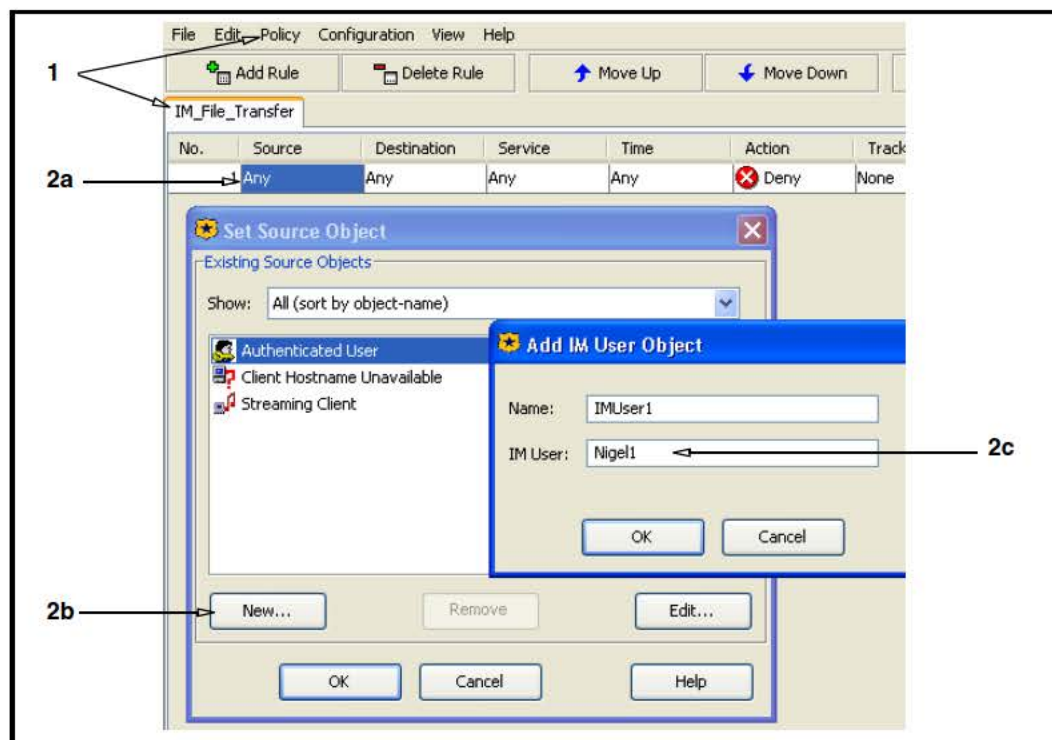
Policy Examples

After the IM clients are configured to send traffic through the SG appliance, you can control and limit IM activity. The Visual Policy Manager (VPM) allows you to create rules that control and track IM communications, including IM activities based on users and groups, IM handle, chat room handle, file name, and other triggers.

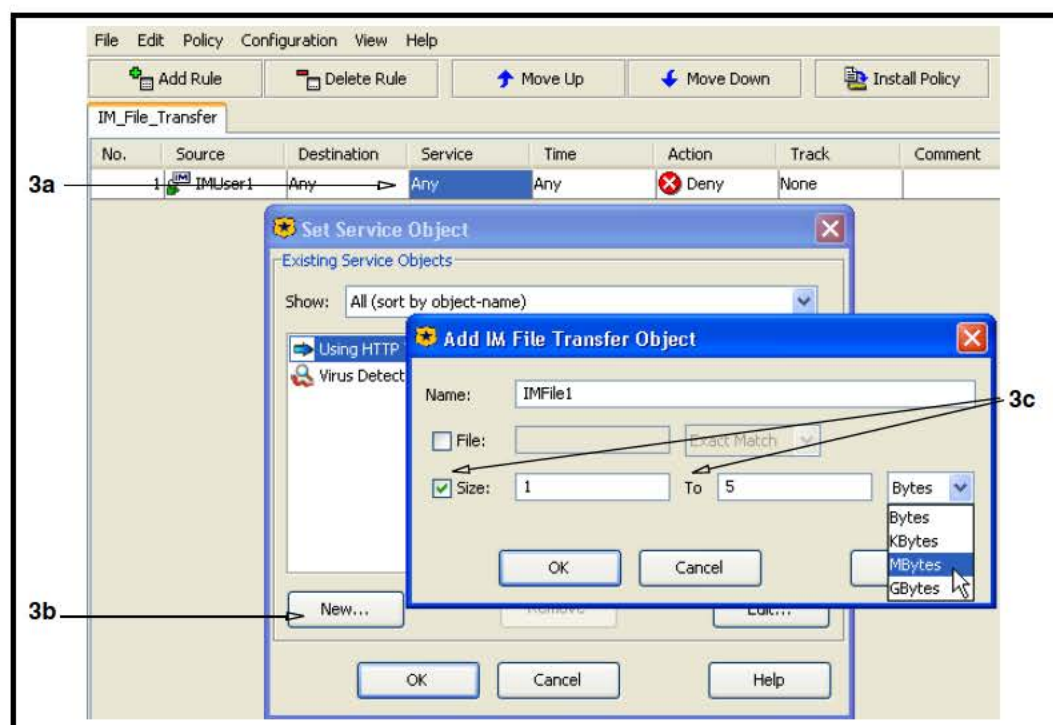
To learn about the VPM, refer to *Volume 7: VPM and Advanced Policy*.

Example 1: File Transfer

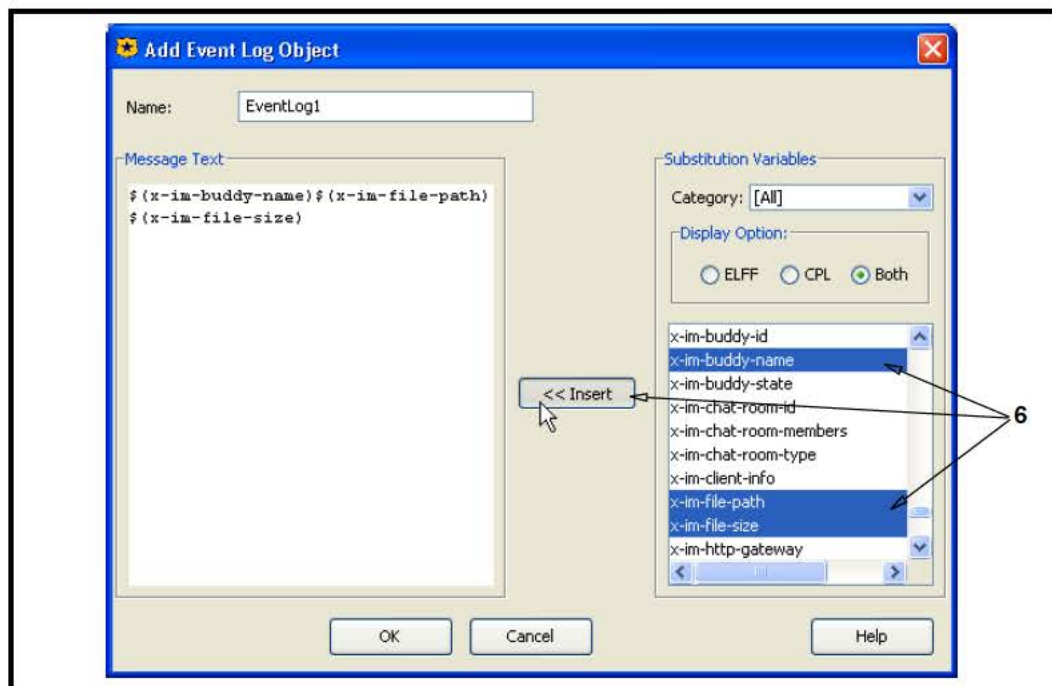
The following example demonstrates an IM rule created with the VPM that IM handle **Nigel1** can perform a file transfer at any time, but the file must be between 1 and 5 MB in size, and the handle, the file path, and file size are logged.



1. In the VPM, select **Policy > Add Web Access Layer**; name it **IM_File_Transfer**.
2. Create a new IM user object:
 - a. Right-click the **Source** field; select **Set**. The Set Source Object dialog appears.
 - b. Click **New**; select **IM User**. The Add IM User Object dialog appears.
 - c. In the **IM User** field, enter **Nigel1**; click **OK** in each dialog.



3. Create a File Transfer object:
 - a. Right-click the **Service** field; select **Set**. The Set Service Object dialog appears.
 - b. Click **New**; select **IM File Transfer**. The Add IM File Transfer dialog appears.
 - c. Select **Size** and enter a range 1 and 5.
 - d. Select **MBytes** from the drop-down list; click **OK** in each dialog.
4. Right-click the **Track** field; select **Set**. The Add Track Object dialog appears.
5. Click **New**; select **Event Log**. The Add Event Log Object dialog appears.



6. From the **Substitution Variables** list, select **x-im-buddy-name** and click insert. Repeat for **x-im-file-path** and **x-im-file-size**. Click **OK** in each dialog.

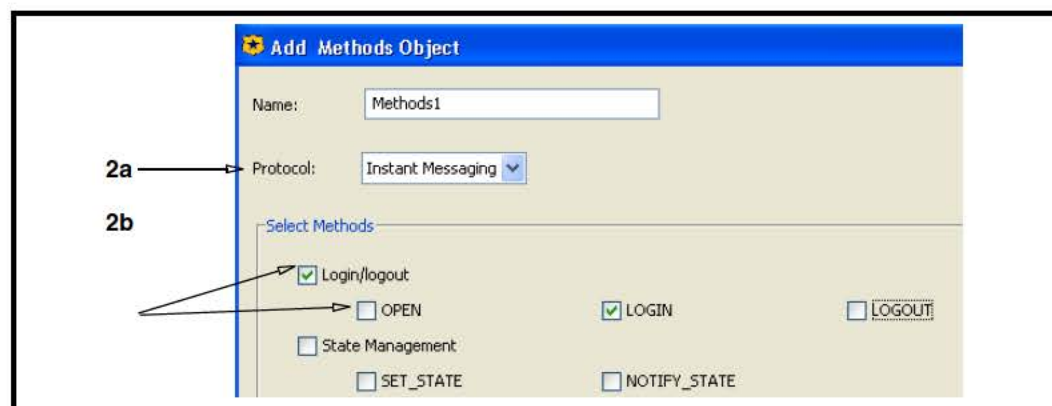


7. In the VPM, click **Install Policy**.

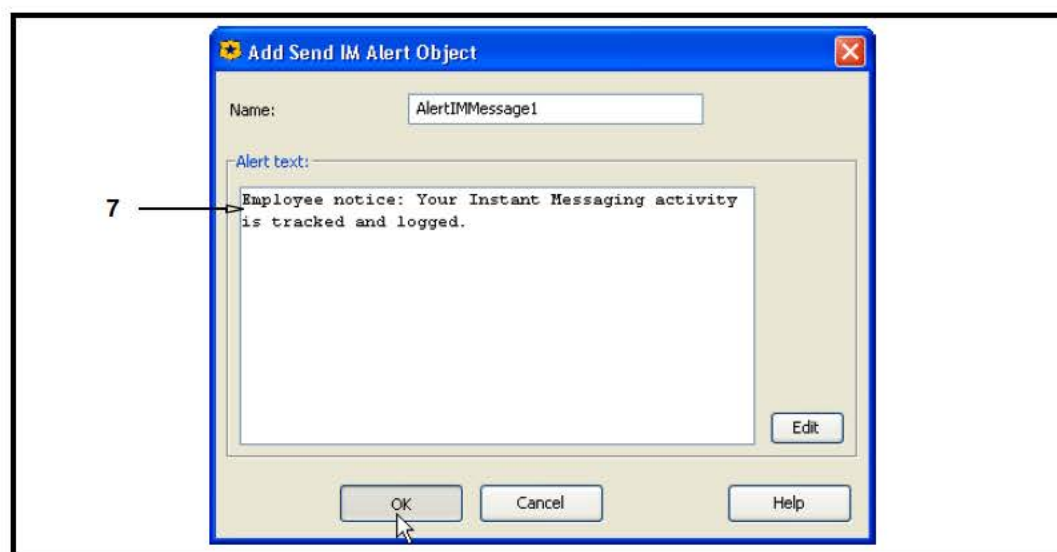
Example 2: Send an IM Alert Message

The following example demonstrates a rule created with the VPM that informs all IM users when they login that their IM activity is tracked and logged.

1. In the VPM, select **Policy > Add Web Access Layer**; name it **IM_NotifyMessage**.
2. Right-click the **Service** field; select **Set**. The Set Service Object dialog appears.
3. Click **New**; select **Protocol Methods**. The Add Methods Object dialog appears.



4. Configure protocol method options:
 - a. From the **Protocol** drop-down list, select **Instant Messaging**.
 - b. Click **Login/Logout**; **LOGIN**; click **OK** to close the dialog; click **OK** to insert the object in the rule.
 - c. Click **OK** in each dialog.
5. Right-click the **Action** field; select **Set**. The Set Action Object dialog appears.
6. Click **New**; select **Send IM Alert**. The Add Send IM Alert Object dialog appears.



7. In the **Alert Text** field, enter a message that appears to users. For example, **Employee notice: Your Instant Messaging activity is tracked and logged**.
8. Click **OK** to close the dialog; click **OK** to insert the object in the rule.
9. Click **Install Policy**.

Reference: Equivalent IM CLI Commands

The configuration tasks describes in this chapter can also be accomplished through the SG appliance CLI. The following are the equivalent CLI command syntaxes:

- ❑ To enter configuration mode:

```
SGOS#(config) proxy-services
```

```
SGOS#(config proxy-services) create {aol-im | msn-im | yahoo-im}  
service_name
```

- ❑ The following submodes are available:

```
SGOS#(config proxy-services) edit service_name
```

```
SGOS#(config service_name) add all | ip_address | ip_address/subnet-  
mask {port | first_port-last_port} [intercept | bypass]
```

```
SGOS#(config service_name) attribute reflect-client-ip {enable |  
disable}
```

```
SGOS#(config service_name) bypass all | ip_address | ip_address/  
subnet-mask {port | first_port-last_port}
```

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

```
SGOS#(config service_name) intercept all | ip_address | ip_address/  
subnet-mask {port | first_port-last_port}
```

```
SGOS#(config service_name) remove all | ip_address | ip_address/  
subnet-mask {port | first_port-last_port}
```

```
SGOS#(config service_name) view
```

Reference: Access Log Fields

The default Blue Coat IM fields are (only IM-specific or relative are listed and described):

- ❑ `cs-protocol`: Protocol used in the client's request.
- ❑ `x-im-method`: The method associated with the instant message.
- ❑ `x-im-user-id`: Instant messaging user identifier.
- ❑ `x-im-user-name`: Display name of the client.
- ❑ `x-im-user-state`: Instant messaging user state.
- ❑ `x-im-client-info`: The instant messaging client information.
- ❑ `x-im-buddy-id`: Instant messaging buddy ID.
- ❑ `x-im-buddy-name`: Instant messaging buddy display name.
- ❑ `x-im-buddy-state`: Instant messaging buddy state
- ❑ `x-im-chat-room-id`: Instant messaging identifier of the chat room in use.
- ❑ `x-im-chat-room-type`: The chat room type, one of public or public, and possibly `invite_only`, voice and/or conference.
- ❑ `x-im-chat-room-members`: The list of chat room member IDs.
- ❑ `x-im-message-text`: Text of the instant message.
- ❑ `x-im-message-size`: Length of the instant message
- ❑ `x-im-message-route`: The route of the instance message.
- ❑ `x-im-message-type`: The type of the instant message.
- ❑ `x-im-file-path`: Path of the file associated with an instant message.

- ❑ `x-im-file-size`: Size of the file (in...?) associated with an instant message.

Reference: CPL Triggers, Properties, and Actions

The following Blue Coat CPL is supported for IM:

Triggers

- ❑ `im.buddy=`
- ❑ `im.chat_room.conference=`
- ❑ `im.chat_room.id=`
- ❑ `im.chat_room.invite_only=`
- ❑ `im.chat_room.type=`
- ❑ `im.chat_room.member=`
- ❑ `im.chat_room.voice_enabled=`
- ❑ `im.client=`
- ❑ `im.file.extension=`
- ❑ `im.file.name=`
- ❑ `im.file.path=`
- ❑ `im.file.size=`
- ❑ `im.message.opcode=`
- ❑ `im.message.reflected=`
- ❑ `im.message.route=`
- ❑ `im.message.size=`
- ❑ `im.message.text=`
- ❑ `im.message.type=`
- ❑ `im.method=`
- ❑ `im.user_agent=`
- ❑ `im.user_id=`

Properties and Actions

- ❑ `im.block_encryptions()`
- ❑ `im.reflect()`
- ❑ `im.strip_attachments()`
- ❑ `im.transport()`
- ❑ `im.alert()`

IM History Statistics

The IM statistics allow you to track IM connections, file transfers, and messages that are currently in use and in total, or have been allowed and denied. The information can be displayed for each IM client type or combined.

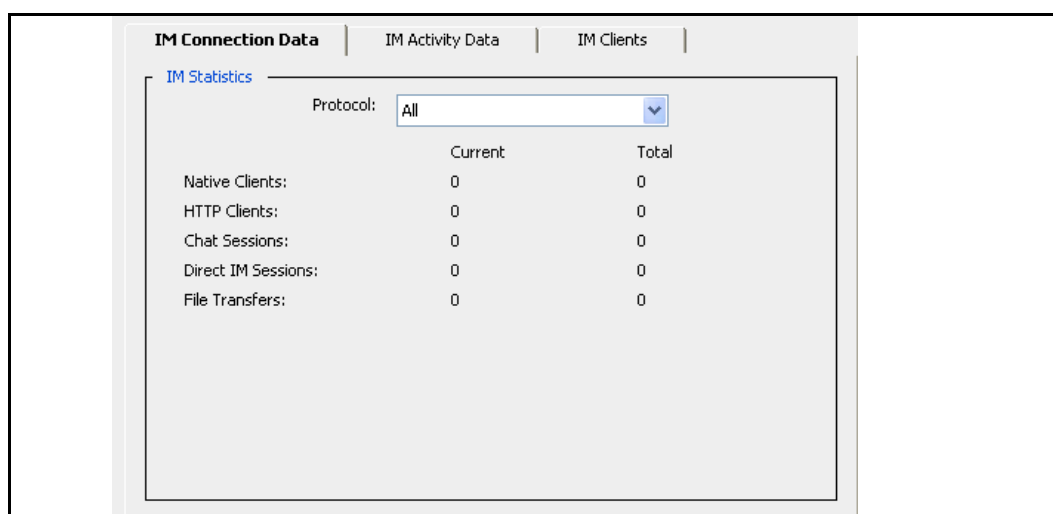
IM Connection Data Tab

The following IM Connection Data statistics indicate current and overall connection data since the last statistics clear:

- ❑ **Native Clients**—The number of native IM clients connected.
- ❑ **HTTP Clients**—The number of HTTP IM clients connected.
- ❑ **Chat Sessions**—The number of IM chats occurring.
- ❑ **Direct IM Sessions**—The number of chats using direct connections.
- ❑ **File Transfers**—The number of file transfers sent through IM clients.

To view the connection data statistics:

1. Select **Statistics > Protocol Details > IM History > IM Connection Data**.



IM Connection Data		
IM Statistics		
Protocol:	Current	Total
All	0	0
Native Clients:	0	0
HTTP Clients:	0	0
Chat Sessions:	0	0
Direct IM Sessions:	0	0
File Transfers:	0	0

2. The default protocol is **All**. To select a specific protocol, select **AOL**, **MSN**, or **Yahoo** from the drop-down list.

IM Activity Data Tab

The following IM Activity Data statistics indicate allowed and denied connections since the last statistics clear:

- ❑ **Logins**—The number of times IM clients have logged in.
- ❑ **Messages**—The number of IM messages.
- ❑ **File Transfers**—The number of file transfers sent through IM clients.
- ❑ **Voice Chats**—The number of voice conversations through IM clients.
- ❑ **Messages**—The number of IM messages reflected or not reflected (if IM Reflection policy is enabled).

Note: The IM activity data statistics are available only through the Management Console.

To view the activity data statistics:

1. Select **Statistics > Protocol Details > IM History > IM Activity Data**.

IM Statistics		
	Allowed	Denied
Logins:	0	0
Messages:	0	0
File Transfers:	0	0
Voice Chats:	0	0
	Reflected:	Not Reflected:
Messages:	0	0

- The default protocol is **All**. To select a specific protocol, select **AOL**, **MSN**, or **Yahoo** from the drop-down list.

IM Clients Tab

The IM Clients tab displays dynamic graphical statistics for connections over 60 minutes, 24 hours and 30 days. The page displays all values in the graph or clip a percentage of peak values. When peak values are clipped by a percentage, that percentage is allowed to fall off the top of the scale.

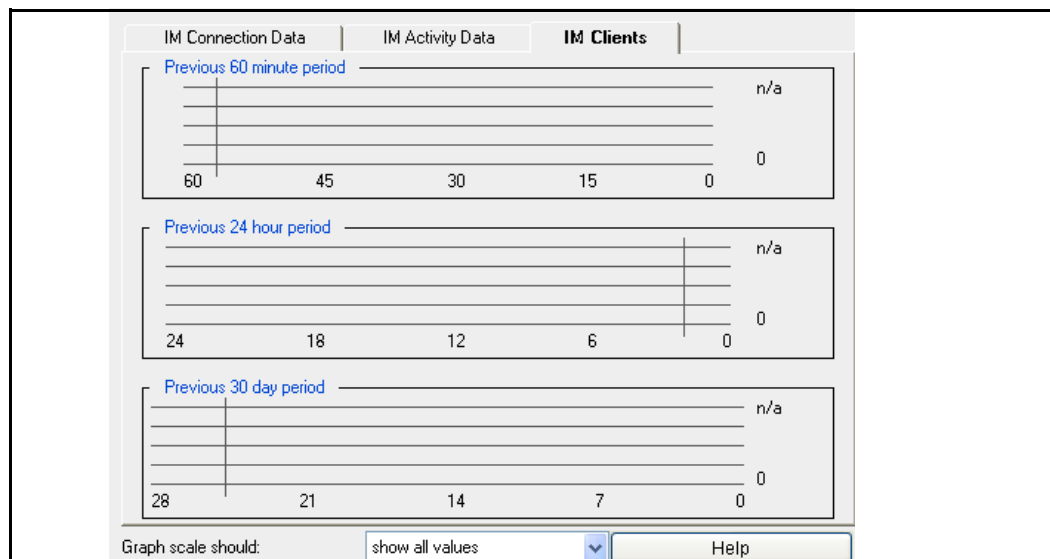
For example, if you clip 25% of the peaks, the top 25% of the values are allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values.

Move the cursor over the graphs to dynamically display the color-coded AOL, MSN, Yahoo, and total statistics.

Note: The IM clients statistics are available only through the Management Console.

To view the client connection statistics:

- Select **Statistics > Protocol Details > IM History > IM Clients**.



2. (Optional) To set the graph scale to a different value, select a value from the **Graph scale should** drop-down list.

Chapter 3: Managing Streaming Media

This chapter contains the following sections:

- ❑ "Section A: Concepts: Streaming Media"—Provides streaming media terminology and Blue Coat streaming solution concepts.
- ❑ "Section B: Configuring Streaming Media"—Provides feature-related concepts and procedures for configuring the SG to manage streaming media applications and bandwidth.
- ❑ "Section C: Additional Configuration Tasks—Windows Media (CLI)" —Provides procedures that can only be performed through the CLI, not the Management Console.
- ❑ "Section D: Windows Media Player"—Describes how to configure the Windows Media client and describes associated interactivities and access log conventions.
- ❑ "Section E: RealPlayer"—Describes how to configure the Real Media client and describes associated interactivities and access log conventions.
- ❑ "Section F: QuickTime Player"—Describes how to configure the QuickTime client and describes associated interactivities and access log conventions.

Section A: Concepts: Streaming Media

Section A: Concepts: Streaming Media

This section contains the following topics:

- ❑ ["About Streaming Media"](#) on page 34
- ❑ ["Supported Streaming Media Clients and Protocols"](#) on page 34
- ❑ ["About Processing Streaming Media Content"](#) on page 38
- ❑ ["About Streaming Media Authentication"](#) on page 47

About Streaming Media

Streaming is a method of content delivery. With media streaming, video and audio are delivered over the Internet rather than the user having to wait for an entire file to be downloaded before it can be played.

Streaming media support on the SG appliance provides the following features:

- ❑ Streaming media files can be live or prerecorded.
- ❑ Employs flexible delivery methods: unicast, multicast, HTTP, TCP, and UDP.
- ❑ Ability to seek, fast-forward, reverse, and pause.
- ❑ Ability to play entire file and control media playback, even before it is downloaded.
- ❑ Adjust media delivery to available bandwidth, including multi-bit-rate and thinning support.

Supported Streaming Media Clients and Protocols

This section describes the vendor-specific streaming protocols supported by the SG appliance.

Supported Streaming Media Clients and Servers

The SG appliance supports Microsoft Windows Media, RealNetworks RealPlayer, and Apple QuickTime; however, the various players might experience unexpected behavior dependent upon certain SGOS configurations and features. Feature sections list such interactivities, as necessary. For a list of the most current versions of each supported client, refer to the Blue Coat *SGOS Release Notes* for this release.

Supported Windows Media Players and Servers

The SG appliance supports the following versions and formats:

- ❑ Windows Media Player
- ❑ Windows Media Server

Section A: Concepts: Streaming Media

Supported Real Media Players and Servers

The SG appliance supports the following versions:

- ❑ RealOne Player
- ❑ RealPlayer
- ❑ RealServer
- ❑ Helix Universal Server

Note: Blue Coat recommends not deploying a Helix proxy between the SG appliance and a Helix server where the Helix proxy is the parent to the SG appliance. This causes errors with the Helix server. The reverse is acceptable (using a Helix proxy as a child to the SG appliance).

Supported QuickTime Players and Servers

The SG appliance supports the following versions, but in pass-through mode only:

- ❑ QuickTime Player
- ❑ Darwin Streaming Server
- ❑ Helix Universal Server

Supported Streaming Protocols

Each streaming media platform supports their own set of protocols. This section describes the protocols the SG appliance supports.

Windows Media Protocols

The SG appliance supports the following protocols:

- ❑ MMS-UDP (Microsoft Media Streaming—User Data Protocol)
- ❑ MMS-TCP (Microsoft Media Streaming—Transmission Control Protocol)
- ❑ HTTP streaming.
- ❑ All protocols between the client and the SG appliance for video-on-demand and live unicast content.
- ❑ MMS-TCP and HTTP streaming between the SG appliance and origin server for video-on-demand and live unicast content.
- ❑ Multicast-UDP is the only delivery protocol supported for multicast. No TCP control connection exists for multicast delivery.

The following briefly describes each of the supported delivery protocols:

- ❑ MMS-UDP—UDP provides the most efficient network throughput from server to client. The disadvantage to UDP is that many network administrators close their firewalls to UDP traffic, limiting the potential audience for Multicast-UDP-based streams.

Section A: Concepts: Streaming Media

The Windows Media Player attempts to connect in the following order:

- Multicast session. Multicast-UDP uses a TCP connection for control messages and UDP for streaming data. TCP provides packet receipt acknowledgement back to the sender. This insures control message delivery.
- MMS-TCP session. If an MMS-UDP session cannot be established, the client falls back to MMS-TCP automatically.

The SG appliance then establishes a connection to the origin server running the Microsoft Windows Media service.

- ❑ MMS-TCP—TCP provides a reliable protocol for delivering streaming media content from a server to a client. At the expense of less efficiency compared to MMS-UDP data transfer, MMS-TCP provides a reliable method for streaming content from the origin server to the SG appliance.

Note: The MMS protocol is usually referred to as either MMS-TCP or MMS-UDP depending on whether TCP or UDP is used as the transport layer for sending streaming data packets. MMS-UDP uses a TCP connection for sending and receiving media control messages, and a UDP connection for streaming the actual media data. MMS-TCP uses TCP connections to send both control and data messages.

- ❑ HTTP Streaming—The Windows Media server also supports HTTP-based media control commands along with TCP-based streaming data delivery. This combination has the benefit of working with all firewalls that let only Web traffic through (port 80).

Depending on the configuration, if MMS-UDP is used between the SG appliance and the client, the appliance can use MMS-TCP, HTTP, or multicast-UDP as the connection to the media server. No protocol relationship exists between the SG appliance and the media server, or between the SG appliance and the client.

Windows Media Over RTSP

The SG appliance supports Windows Media content streamed over RTSP. The following Windows Media RTSP transports are supported:

Client-side

- ❑ RTP over unicast UDP (RTSP over TCP, RTP over unicast UDP)
- ❑ Interleaved RTSP (RTSP over TCP, RTP over TCP on the same connection)
- ❑ RTP over multicast UDP (RTP over multicast UDP; for live content only)

Server-side

- ❑ Interleaved RTSP

Server-side RTP over UDP is not supported. If policy directs the RTSP proxy to use HTTP as server-side transport, the proxy denies the client request. The client then rolls over to MMS or HTTP.

Section A: Concepts: Streaming Media

Real Media Protocols

The SG appliance supports the following Real Media protocols:

Client-Side

- ❑ RDT over unicast UDP (RTSP over TCP, RDT over unicast UDP)
- ❑ Interleaved RTSP (RTSP over TCP, RDT over TCP on the same connection)
- ❑ RDT over multicast UDP (RTSP over TCP, RDT over multicast UDP; for live content only)
- ❑ HTTP streaming (RTSP and RDT over TCP tunneled through HTTP)—HTTP streaming is supported through a handoff process from HTTP to RTSP. HTTP accepts the connection and, based on the headers, hands off to RTSP. The headers identify an RTSP URL.

Server-Side

- ❑ Interleaved RTSP
- ❑ HTTP streaming

Unsupported Protocols

The following Real Media protocols are not supported in this version of SGOS:

- ❑ PNA.
- ❑ Server-side RDT/UDP (both unicast and multicast).

QuickTime Protocols

The SG appliance supports the following protocols:

- ❑ RTP over unicast UDP (RTSP over TCP, RDT over unicast UDP)
- ❑ Interleaved RTSP (RTSP over TCP, RDT over TCP on the same connection)
- ❑ HTTP streaming (RTSP and RDT over TCP tunneled through HTTP)—HTTP streaming is supported through a handoff process from HTTP to RTSP. HTTP accepts the connection and, based on the headers, hands off to RTSP. The headers identify an RTSP URL.

Server-Side

- ❑ Interleaved RTSP
- ❑ HTTP streaming

Unsupported Protocols

The following QuickTime protocols are not supported in this version of SGOS:

- ❑ Server-side RTP/UDP, both unicast and multicast, is not supported.
- ❑ Client-side multicast is not supported.

Section A: Concepts: Streaming Media

About Processing Streaming Media Content

The following sections describe how the SG appliance processes, stores, and serves streaming media requests. Using the SG appliance for streaming delivery minimizes bandwidth use by allowing the SG appliance to handle the broadcast and allows for policy enforcement over streaming use. The delivery method depends on if the content is live or video-on-demand.

Delivery Methods

The SG appliance supports the following streaming delivery methods:

- ❑ **Unicast**—A one-to-one transmission, where each client connects individually to the source, and a separate copy of data is delivered from the source to each client that requests it. Unicast supports both TCP- and UDP-based protocols. The majority of streaming media traffic on the Internet is unicast.
- ❑ **Multicast**—Allows efficient delivery of streaming content to a large number of users. Multicast enables hundreds or thousands of clients to play a single stream, thus minimizing bandwidth use.

The SG appliance provides caching, splitting, and multicast functionality.

Serving Content: Live Unicast

An SG appliance can serve many clients through one unicast connection by receiving the content from the origin server and then splitting that stream to the clients that request it. This method saves server-side bandwidth and reduces the server load. You cannot pause or rewind live broadcasts. A live broadcast can be of prerecorded content. A common example is a company president making a speech to all employees.

Serving Content: Video-on-Demand Unicast

An SG appliance can store frequently requested data and distribute it upon client requests. Because the SG appliance is closer to the client than the origin server, the data is served locally, which saves firewall bandwidth and increases quality of service by reducing pauses or buffering during playback. The SG appliance provides higher quality streams (also dependent on the client connection rate) than the origin server because of its closer proximity to the end user. VOD content can be paused, rewound, and played back. Common examples include training videos or news broadcasts.

Serving Content: Multicast Streaming

This section describes multicast streaming and how to configure the SG appliance to manage multicast broadcasts.

About Multicast Content

The SG appliance can take a unicast stream from the OCS and deliver it as a multicast broadcast. This enables the SG appliance to take a one-to-one stream and split it into a one-to-many stream, saving bandwidth and reducing the server load. It also produces a higher quality broadcast.

For Windows Media multicast, an NSC file is downloaded through HTTP to acquire the control information required to set up content delivery.

Section A: Concepts: Streaming Media

For Real Media and QuickTime (through RTSP), multicasting maintains a TCP control (accounting) channel between the client and media server. The multicast data stream is broadcast using UDP from the SG appliance to streaming clients, who join the multicast.

About Serving Multicast Content

The SG appliance takes a multicast stream from the origin server and delivers it as a unicast stream. This avoids the main disadvantage of multicasting—that all of the routers on the network must be multicast-enabled to accept a multicast stream. Unicast-to-multicast, multicast-to-multicast, and broadcast alias-(scheduled live from stored content)-to-multicast are also supported.

Multicast to Unicast Live Conversion at the SG Appliance

The SG appliance supports converting multicast streams from an origin content server to unicast streams. The stream at the SG appliance is given the appropriate unicast headers to allow the appliance to direct one copy of the content to each user on the network.

Multicast streaming only uses UDP protocol and does not know about the control channel, which transfers essential file information. The `.nsc` file (a file created off-line that contains this essential information) is retrieved at the beginning of a multicast session from an HTTP server. The `multicast-alias` command specifies an alias to the URL to receive this `.nsc` file.

The converted unicast stream can use any of the protocols supported by Windows Media and Real Media, including HTTP streaming.

When a client requests the alias content, the SG uses the URL specified in the `multicast-alias` command to fetch the `.nsc` file from the HTTP server. The `.nsc` file contains all of the multicast-related information, such as addresses and `.asf` file header information that is normally exchanged through the control connection for unicast-delivered content.

Note: For Windows Media steaming clients, additional multicast information is provided in “[Managing Multicast Streaming for Windows Media](#)” on page 63.

About HTTP Handoff

When a Windows Media, Real Media, or QuickTime client requests a stream from the SG appliance over port 80, which in common deployments is the only port allowing traffic through a firewall, the HTTP module passes control to the streaming module so HTTP streaming can be supported through the HTTP proxy port.

Limiting Bandwidth

The following sections describe bandwidth limitation and how to configure the SG to limit global and protocol-specific media bandwidth.

Streaming media bandwidth management is achieved by configuring the SG appliance to restrict the total number of bits per second the appliance receives from the origin media servers and delivers to clients. The configuration options are flexible to allow you to configure streaming bandwidth limits for the SG appliance, as well as for each streaming protocol (Windows Media, Real Media, and QuickTime).

Section A: Concepts: Streaming Media

Note: Bandwidth claimed by HTTP, non-streaming protocols, and network infrastructure is not constrained by this limit. Transient bursts that occur on the network can exceed the hard limits established by the bandwidth limit options.

After it has been configured, the SG appliance limits streaming access to the specified threshold. If a client tries to make a request after a limit has been reached, the client receives an error message.

Note: If a maximum bandwidth limitation has been specified for the SG appliance, the following condition can occur. If a Real Media client, followed by a Windows Media client, requests streams through the same SG appliance and total bandwidth exceeds the maximum allowance, the Real Media client enters the rebuffering state. The Windows Media client continues to stream.

Section A: Concepts: Streaming Media

Consider the following features when planning to limit streaming media bandwidth:

- ❑ SG appliance to server (all protocols)—The total kilobits per second allowed between the appliance and any origin content server or upstream proxy for all streaming protocols. Setting this option to 0 effectively prevents the SG appliance from initiating any connections to the media server. The SG appliance supports partial caching in that no bandwidth is consumed if portions of the media content are stored in the SG appliance.
- ❑ Client to SG appliance (all protocols)—The total kilobits per second allowed between streaming clients and the SG. Setting this option to 0 effectively prevents any streaming clients from initiating connections through the SG appliance.
- ❑ SG appliance to server—The total kilobits per second allowed between the Appliance and the media server. Setting this option to 0 effectively prevents the SG appliance from accepting media content.

Limiting SG appliance bandwidth restricts the following streaming media-related functions:

- Live and video-on-demand media, the sum of all bit rates
 - Limits the ability to fetch new data for an object that is partially cached
 - Reception of multicast streams
- ❑ Client to SG appliance—The total kilobits per second allowed between Windows Media streaming media clients and the SG appliance. Setting this option to 0 effectively prevents streaming clients from making connections to the SG appliance.

Limiting server bandwidth restricts the following streaming media-related functions:

- MBR is supported; the SG appliance assumes the client is using the maximum bit rate
 - Limits the transmission of multicast streams
- ❑ Client connections—The total number of clients that can connect concurrently. When this limit is reached, clients attempting to connect receive an error message and are not allowed to connect until other clients disconnect. Setting this variable to 0 effectively prevents any streaming media clients from connecting.

Selecting a Method to Limit Streaming Bandwidth

You can control streaming bandwidth using two different methods: you can use the streaming features described in [“Limiting Bandwidth”](#) on page 39, or you can use the bandwidth management features described in *Volume 6: Advanced Networking*. Do not, however, use both methods to control streaming bandwidth. The way that each method controls bandwidth differs—read the information below to decide which method best suits your deployment requirements.

Limiting streaming bandwidth using the streaming features (described in this chapter) works this way: if a new stream comes in that pushes above the specified bandwidth limit, that new stream is denied. This allows existing streams to continue to get the same level of quality they currently receive.

Limiting streaming bandwidth using the bandwidth management features works this way: all streaming traffic for which you have configured a bandwidth limit shares that limit. If a new stream comes in that pushes above the specified bandwidth limit, that stream is allowed, and the amount of bandwidth available for existing streams is reduced.

Section A: Concepts: Streaming Media

This causes streaming players to drop to a lower bandwidth version of the stream. If a lower bandwidth version of the stream is not available, players that are not receiving enough bandwidth can behave in an unpredictable fashion. In other words, if the amount of bandwidth is insufficient to service all of the streams, some or all of the media players experience a reduction in stream quality.

For most circumstances, Blue Coat recommends that you use the streaming features to control streaming bandwidth rather than the bandwidth management features.

Caching Behavior: Protocol Specific

This section describes what is cached for each supported protocol.

Windows Media

The SG appliance caches Windows Media-encoded video and audio files. The standard extensions for these file types are: `.wmv`, `.wma`, and `.asf`.

Real Media

The SG appliance caches Real Media-encoded files, such as RealVideo and RealAudio. The standard extensions for these file types are: `.ra`, `.rm`, and `.rmvb`. Other content served from a Real Media server through RTSP is also supported, but it is not cached. This content is served in pass-through mode only.

QuickTime

The SG appliance does not cache QuickTime content (`.mov` files). All QuickTime content is served in *pass-through* mode only.

Caching Behavior: Video on Demand

The SG appliance supports the caching of files for VOD streaming. First, the client connects to the SG appliance, which in turn connects to the origin server and pulls the content, storing it locally. Subsequent requests are served from the SG appliance. This provides bandwidth savings, as every *hit* to the SG appliance means less network traffic. Blue Coat also supports partial caching of streams

Note: On-demand files must be unicast.

Caching Behavior: Live Splitting

The SG appliance supports splitting of live content, but behavior varies depending upon the media type.

For live streams, the SG appliance can split streams for clients that request the same stream. First, the client connects to the SG appliance, which then connects to the origin server and requests the live stream. Subsequent requests are split from the appliance.

Two streams are considered identical by the SG appliance if they share the following characteristics:

- ❑ The stream is a live or broadcast stream.
- ❑ The URL of the stream requested by client is identical.
- ❑ MMS, MMSU, MMST, and HTTP are considered as identical.

Section A: Concepts: Streaming Media

Note: If the URL is composed of host names instead of IP addresses, splitting does not occur across WMP 7.0 clients.

Splitting of live unicast streams provides bandwidth savings, since subsequent requests do not increase network traffic.

Multiple Bit Rate Support

The SG appliance supports multiple bit rate (MBR), which is the capability of a single stream to deliver multiple bit rates to clients requesting content from caches from within varying levels of network conditions (such as different connecting bandwidths and traffic). This allows the SG appliance and the client to negotiate the optimal stream quality for the available bandwidth even when the network conditions are bad. MBR increases client-side streaming quality, especially when the requested content is not cached.

Only the requested bitrate is cached. Therefore, a media client that requests a 50Kbps stream receives that stream, and the SG appliance caches only the 50Kbps bitrate content.

Bitrate Thinning

Thinning support is closely related to MBR, but different in that thinning allows for data rate optimizations even for single data-rate media files. If the media client detects that there is network congestion, it requests a subset of the single data rate stream. For example, depending on how congested the network is, the client requests only the *key video frames* or audio-only instead of the complete video stream.

Pre-Populating Content

The SG appliance supports pre-population of streaming files from HTTP servers and origin content servers. Downloading streaming files from HTTP servers reduces the time required to pre-populate the file.

Note: QuickTime content is not supported. Windows Media RTSP only supports pre-population of streaming files from origin content servers. However, whenever origin content server allows faster caching of streaming content, Windows Media RTSP pre-populates the content much faster.

Pre-population can be accomplished through streaming from the media server. The required download time was equivalent to the file length; for example, a two-hour movie required two hours to download. Now, if the media file is hosted on a HTTP server, the download time occurs at normal transfer speeds of an HTTP object, and is independent of the play length of the media file.

Note: Content must be hosted on a HTTP server in addition to the media server.

Using the content distribute CLI command, content is downloaded from the HTTP server and renamed with a given URL argument. A client requesting the content perceives that the file originated from a media server. If the file on the origin media server experiences changes (such as naming convention), SGOS bypasses the cached mirrored version and fetches the updated version.

Section A: Concepts: Streaming Media

About Fast Streaming (Windows Media)

Note: This feature applies to Windows Media only.

Windows Media Server version 9 contains a feature called Fast Streaming that allows clients to provide streams with extremely low buffering time.

SGOS 4.x supports the following functionality for both cached and uncached content:

- ❑ Fast Start
- ❑ Fast Cache

Fast Recovery and Fast Reconnect are currently not supported.

About QoS Support

The SG appliance supports Quality of Service (QoS), which allows you to create policy to examine the Type of Service fields in IP headers and perform an action based on that information. For streaming protocols, managing the QoS assists with managing bandwidth classes.

For detailed information about managing QoS, see the Advanced Policy chapter in *Volume 6: Advanced Networking*.

About Windows Media Over RTSP

This section provides inter-activity notes for Windows Media over RTSP deployments.

License Requirements

The Windows Media RTSP functionality is included in the existing Windows Media license.

Standard License

When a standard Windows Media license is installed, only pass-through streaming mode and full policy control are available. Advanced features, for example, live splitting, VOD caching, or multicast-station are not available.

Premium License

When a premium Windows Media license is installed, the full functionality for Windows Media RTSP is available.

If a Windows Media license is not installed, or the license has expired, client connections are denied.

Upgrade/Downgrade Issues

There are no software upgrade/downgrade requirements associated with Windows Media RTSP.

If the SG appliance is downgraded to a release prior to SGOS 4.2.3, RTSP connections from a Windows Media Player are denied. However, the client will fail over to MMS or HTTP, which are handled by the MMS proxy.

Management Console and CLI Changes

No Management Console or CLI changes are related to the Windows Media RTSP feature.

Supported Streaming Features

The following table describes the supported Windows Media streaming features.

Live Support

Table 3-1. Windows Media live RTSP streaming feature support

Feature	Live Support
Multi-Bit Rate and Thinning	Yes
UDP Retransmission	No
Server-Side Playlists	Yes
Stream Change	Yes
Splitting Server-Authenticated Data	Yes
Splitting Proxy-Authenticated Data	Yes
Adherence to RTSP Cache Directives	Yes

On Demand Support

Table 3-2. Windows Media on demand RTSP streaming feature support

Feature	On Demand Support
Multi-Bit Rate and Thinning	Yes
Fast Forward and Rewind	Yes
Fast Streaming	Yes
UDP Retransmission	No
Server-Side Playlists	No Caching
Stream Change	No
Caching Server-Authenticated Data	Yes
Caching Proxy-Authenticated Data	Yes
Adherence to RTSP Cache Directives	Yes
Partial File Caching	Yes
File Invalidation/Freshness checking for Cached Files	Yes

Section A: Concepts: Streaming Media

Multicast Support

Table 3-3. Windows Media Multicast UDP streaming feature support

Feature	Multicast
Multi-Bit Rate and Thinning	Yes
Server-Side Playlists	No
Stream Change	No
Multicasting Server-Authenticated Data	No
Multicasting Proxy-Authenticated Data	No

Other Supported Features

The Windows Media RTSP streaming feature also supports the following features:

- ❑ Access logging for unicast clients
- ❑ Summary statistics in the Management Console
- ❑ Detailed statistics

Supported VPM Properties and Actions

Windows Media RTSP supports the following policy properties and actions:

- ❑ `allow, deny, force_deny`
- ❑ `access_server(yes|no)`. Forces the SG appliance to deliver content only from the cache. Requests for live streams are denied.
- ❑ `authenticate(realm)`
- ❑ `forward(alias_list|no)`
- ❑ `forward.fail_open(yes|no)`
- ❑ `reflect_ip(auto|no|client|vip|<ip address>)`
- ❑ `bypass_cache(yes|no)`. Forces the SG appliance to deliver content in pass-through mode.
- ❑ `limit_bandwidth()`
- ❑ `rewrite()`. One-way URL rewrite of server-side URLs is supported.

Windows Media RTSP also supports the following streaming-relevant properties:

- ❑ `max_bitrate(bitrate|no)`. Sets the maximum bit rate that can be served to the client. (This property does not apply to the bit rate consumed on the gateway connection.) If the bit rate of a client-side session exceeds the maximum bit rate set by policy, that client session is denied.
- ❑ `force_cache(yes|no)`. Causes the SG appliance to ignore RTSP cache directives and cache VOD content while serving it to clients.

Note: Windows Media RTSP does not support policy-based streaming transport selection.

Section A: Concepts: Streaming Media

Bandwidth Management

Windows Media RTSP supports bandwidth management for both client-side and gateway-side streaming traffic. Bandwidth limiting is supported for both client-side and gateway-side streaming traffic. Bandwidth limits are also supported for pass-through streams.

About Streaming Media Authentication

The following sections discuss authentication between streaming media clients and SG appliances and between SG appliances and origin content servers (OCS).

Windows Media Server-Side Authentication

Windows Media server authentication for HTTP and MMS supports the following authentication types:

- ❑ HTTP—BASIC Authentication and Membership Service Account
- ❑ HTTP—BASIC Authentication and Microsoft Windows Integrated Windows Authentication (IWA) Account Database
- ❑ IWA Authentication and IWA Account Database

The SG appliance supports the caching and live-splitting of server-authenticated data. The functionality is also integrated with partial caching functionality so that multiple security challenges are not issued to the Windows Media Player when it accesses different portions of the same media file.

When Windows Media content on the server is accessed for the first time, the SG appliance caches the content along with the authentication type enabled on the server. The cached authentication type remains until the appliance learns that the server has changed the enabled authentication type, either through cache coherency (checking to be sure the cached contents reflect the original source) or until the SG appliance connects to the origin server (to verify access credentials).

Authentication type on the server refers to the authentication type enabled on the origin server at the time when the client sends a request for the content.

Windows Media Proxy Authentication

If proxy authentication is configured, Windows Media clients are authenticated based on the policy settings. The SG appliance evaluates the request from the client and verifies the accessibility against the set policies. The Windows Media player then prompts the client for the proper password. If the client is accepted, the Windows Media server might also require the client to provide a password for authentication. If a previously accepted client attempts to access the same Windows Media content again, the SG appliance verifies the user credentials using its own credential cache. If successful, the client request is forwarded to the Windows Media server for authentication.

Windows Media Player Authentication Interactivities

Consider the following proxy authentication interactivities with the Windows Media player (except when specified, these do not apply to HTTP streaming):

- ❑ If the proxy authentication type is configured as BASIC and the server authentication type is configured as IWA, the default is denial of service.

Section A: Concepts: Streaming Media

- ❑ If proxy authentication is configured as IWA and the server authentication is configured as BASIC, the proxy authentication type defaults to BASIC.
- ❑ The SG appliance does not support authentication based on `url_path` or `url_path_regex` conditions when using `mms` as the `url_scheme`.
- ❑ Transparent style HTTP proxy authentication fails to work with Windows Media players when the credential cache lifetime is set to 0 (independent of whether server-side authentication is involved).
- ❑ If proxy authentication is configured, a request for a stream through HTTP prompts the user to enter access credentials twice: once for the proxy authentication and once for the media server authentication.
- ❑ Additional scenarios involving HTTP streaming exist that do not work when the TTL is set to zero (0), even though only proxy authentication (with no server authentication) is involved. The SG appliance returning a 401-style proxy authentication challenge to the Windows Media Player 6.0 does not work because the Player cannot resolve inconsistencies between the authentication response code and the server type returned from the SG appliance. This results in an infinite loop of requests and challenges. Example scenarios include transparent authentication—resulting from either transparent request from player or hard-coded service specified in the SG appliance—and request of cache-local (ASX-rewritten or unicast alias) URLs.

Real Media Proxy Authentication

If proxy authentication is configured, Real Media clients are authenticated based on the policy settings. The proxy (the SG appliance) evaluates the request from the client and verifies the accessibility against the set policies. Next, RealPlayer prompts the client for the proper password. If the client is accepted, the Real Media server can also require the client to provide a password for authentication. If a previously accepted client attempts to access the same Real Media content again, the SG appliance verifies the user credentials using its own credential cache. If successful, the client request is forwarded to the Real Media server for authentication.

Real Media Player Authentication Limitation

Using RealPlayer 8.0 in transparent mode with both proxy and Real Media server authentication configured to BASIC, RealPlayer 8.0 always sends the same proxy credentials to the media server. This is regardless of whether a user enters in credentials for the media server. Therefore, the user is never authenticated and the content is not served.

QuickTime Proxy Authentication

BASIC is the only proxy authentication mode supported for QuickTime clients. If an IWA challenge is issued, the mode automatically downgrades to BASIC.

Section B: Configuring Streaming Media

Section B: Configuring Streaming Media

This section describes how to configure the various SG appliance streaming options. This section contains the following topics:

- ❑ ["Configuring Streaming Services" on page 49](#)
- ❑ ["Configuring Streaming Proxies" on page 52](#)
- ❑ ["Limiting Bandwidth" on page 53](#)
- ❑ ["Configuring the SG Appliance Multicast Network" on page 55](#)
- ❑ ["Configuring Media Server Authentication Type \(Windows Media\)" on page 56](#)
- ❑ ["Related CLI Syntax to Manage Streaming" on page 56](#)
- ❑ ["Reference: Access Log Fields" on page 57](#)
- ❑ ["Reference: CPL Triggers, Properties, and Actions" on page 58](#)
- ❑ ["Streaming History Statistics" on page 58](#)

Related Topics

You must also configure the network service (**Configuration > Network > Services**) to assign port numbers and modes (transparent or proxy). For more information, refer to *Volume 3: Proxies and Proxy Services*.

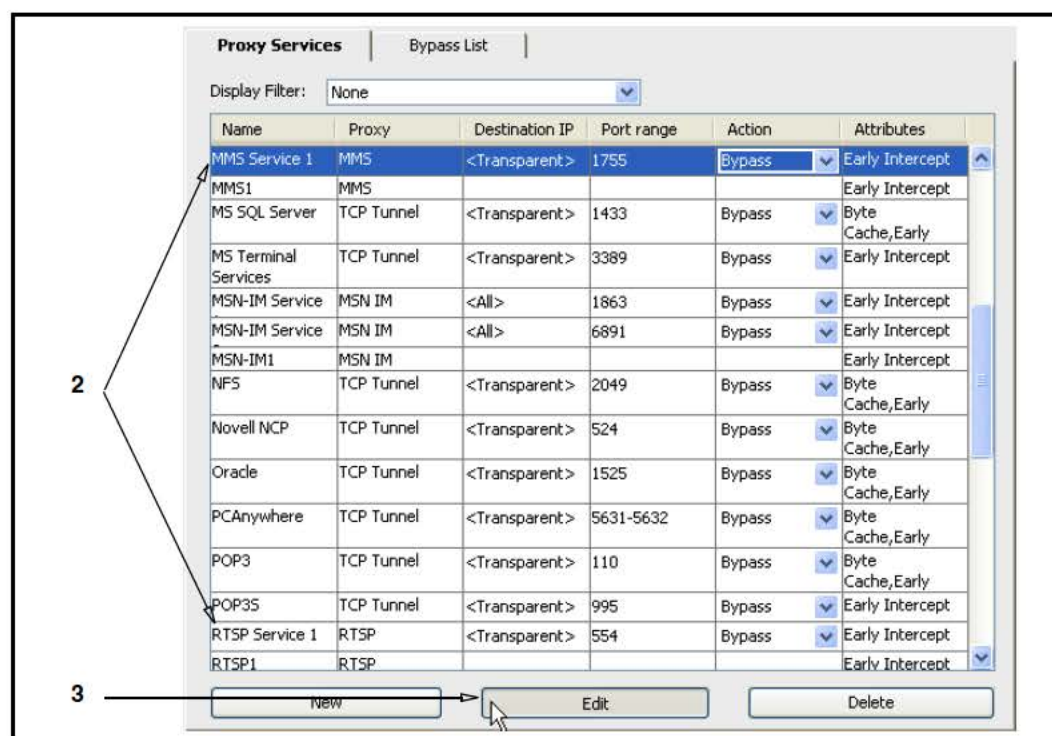
Configuring Streaming Services

By default, the streaming services (MMS and RTSP) are configured be **Transparent** and in **Bypass** mode. The following procedure describes how to change them to **Intercept** mode, and explains other attributes within the service.

To configure the MMS/RTSP proxy services attributes:

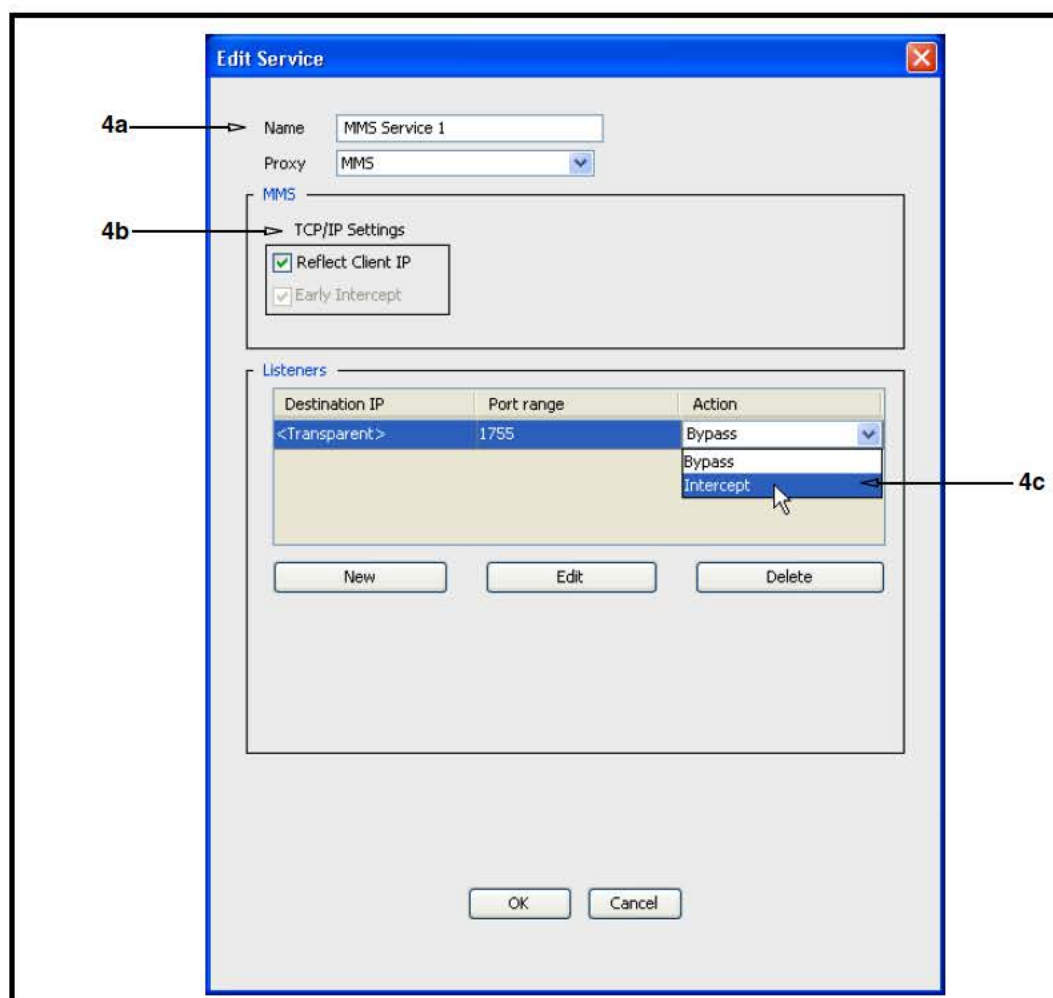
1. From the Management Console, select **Configuration > Services > Proxy Services**.

Section B: Configuring Streaming Media



2. Scroll the list of services to display the default one of the IM service lines (this example uses MMS). Notice the **Action** is **Bypass**. You can select **Intercept** from the drop-down list, but for the purposes of this procedure, select the service line to highlight it.
3. Click **Edit**. The Edit Service dialog appears with the default settings displays.

Section B: Configuring Streaming Media



4. Configure the service attributes:
 - a. In the **Name** field, enter a name that intuitively labels this service. This example accepts the default name.
 - b. The **TCP/IP Settings** options allow you to manage the data connections:
 - **Reflect Client IP:** If this is enabled, the connection to the origin content server appears to come from the client, not the SG.
 - **Early Intercept:** Not valid for this service.
 - c. In the **Listeners** field, select **Intercept** from the drop-down list; the SG must intercept the streaming connection.

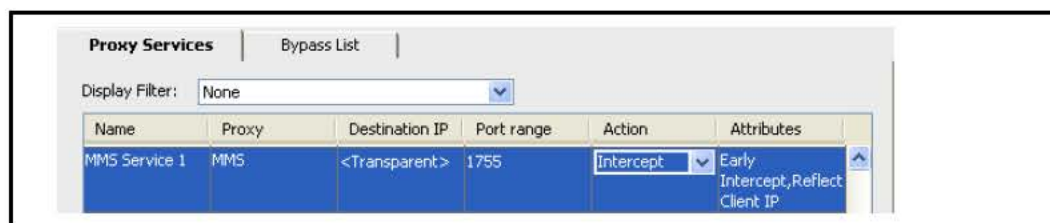
Note: You can also change the mode from **Bypass** to **Intercept** from the main services page.

d. Click **OK**

5. Click **Apply**.

Result: The streaming service is configured and appears in Management Console.

Section B: Configuring Streaming Media



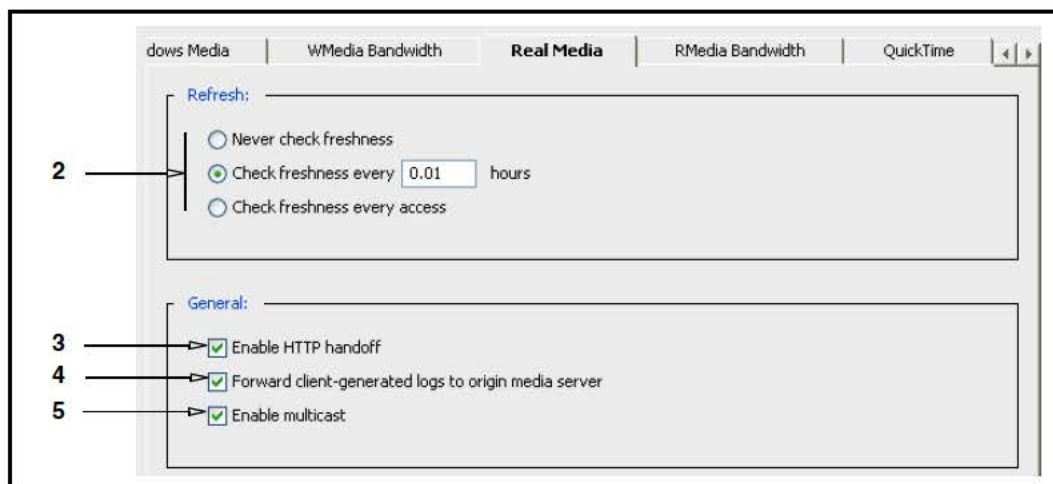
Now that the streaming listeners are configured, you can configure the streaming proxies.

Configuring Streaming Proxies

This section describes how to configure the Streaming Media proxies. The Windows Media and Real Media proxy options are identical except for one extra option for Real Media. As QuickTime is not cached but passed through the SG appliance, there is only one option.

To configure Windows Media, Real Media, and QuickTime streaming proxies:

1. From the Management Console, select **Configuration > Services > Streaming Proxies > Windows Media, Real Media, or QuickTime** (configures HTTP Handoff only).



2. Specify the when the SG appliance checks cached streaming content for freshness.
 - **Never check freshness:** The default, but Blue Coat recommends not using this option.
 - **Check freshness every *value* hours:** The SG appliance checks content freshness every *n.nn* hours.
 - **Check freshness every access:** Every time cached content is requested, it is checked for freshness.

Section B: Configuring Streaming Media

Note: A value of 0 requires the streaming content to always be checked for freshness.

3. **Enable HTTP handoff:** Enabled by default. Only disable if you do not want HTTP streams to be cached or split. See [“About HTTP Handoff”](#) on page 39.
4. **Forward client-generated logs to origin media server:** Enabled by default. The SG appliance logs information, such as client IP address, the date, and the time, to the origin server for Windows Media and Real Media content.

Note: For Real Media, the log is only forwarded before a streaming session is halted; QuickTime log forwarding is not supported.

5. **Enable multicast** (Real Media proxy only): The SG appliance receives a unicast stream from the origin RealServer and serves it as a multicast broadcast. This allows the SG to take a one-to-one stream and split it into a one-to-many stream, saving bandwidth and reducing the server load. It also produces a higher quality broadcast.

Multicasting maintains a TCP control (accounting) channel between the client and RealServer. The multicast data stream is broadcast using UDP from the SG appliance to RealPlayers that join the multicast. The SG appliance support for Real Media uses UDP port 554 (RTSP) for multicasting. This port number can be changed to any valid UDP port number.

6. Click **Apply**.

Note: For Multicast, additional configuration is required. See [“Configuring the SG Appliance Multicast Network”](#) on page 55.

Limiting Bandwidth

This section describes how to limit bandwidth from both the clients to the SG appliance and the SG appliance to origin content servers (OCS).

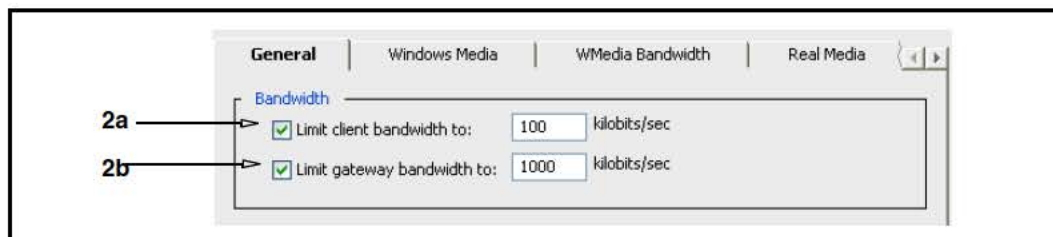
Section B: Configuring Streaming Media

Configuring Bandwidth Limits—Global

This section describes how to limit all bandwidth use through the SG appliance.

To specify the bandwidth limit for all streaming protocols:

1. Select **Configuration > Services > Streaming Proxies > General**.



2. To limit the client connection bandwidth:
 - a. In the **Bandwidth** field, select **Limit client bandwidth to**. In the **Kilobits/sec** field, enter the maximum number of kilobits per second that the SG appliance allows for all streaming client connections.

Note: This option is not based on individual clients.

- b. In the **Bandwidth** pane, select **Limit gateway bandwidth**. In the **Kilobits/sec** field, enter the maximum number of kilobits per second that the SG appliance allows for all streaming connections to origin media servers.
3. Click **Apply**.

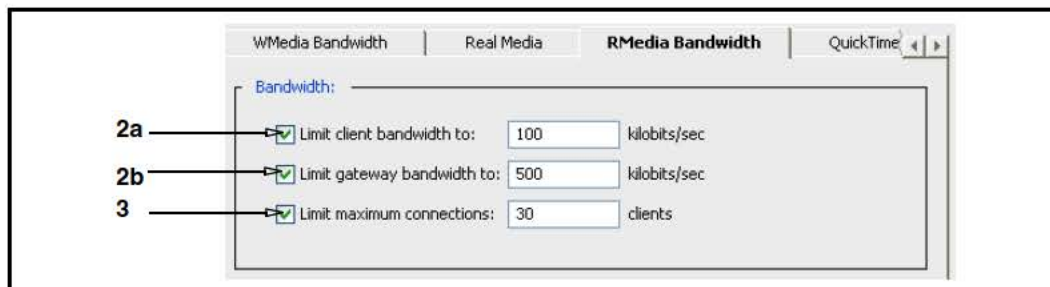
Configuring Bandwidth Limits—Protocol-Specific

This section describes how to limit bandwidth use per-protocol through the SG appliance. You can also limit the number of connections from the SG appliance to the OCS. The following example uses Real Media, but the Management Console screens are identical for all protocols.

Section B: Configuring Streaming Media

To specify the bandwidth limit for Windows Media, Real Media, or QuickTime:

1. Select **Configuration > Services > Streaming Proxies > WMedia Bandwidth -or- RMedia Bandwidth -or- QuickTime Bandwidth**.



2. Configure bandwidth limit options:
 - a. To limit the bandwidth for client connections to the SG appliance, select **Limit client bandwidth to**. In the **Kilobits/sec** field, enter the maximum number of kilobits per second that the SG appliance allows for all streaming client connections.
 - b. To limit the bandwidth for connections from the SG appliance to origin content servers, select **Limit gateway bandwidth to**. In the **Kilobits/sec** field, enter the maximum number of kilobits per second that the SG appliance allows for all streaming connections to origin media servers.
3. To limit the bandwidth for connections from the SG appliance to the OCS, select **Limit maximum connections**. In the **clients** field, enter the total number of clients that can connect concurrently.
4. Click **Apply**.

Configuring Bandwidth Limitation—Fast Start (WM)

Note: This section applies to Windows Media only and can only be accomplished through the CLI.

Upon connection to the SG appliance, Windows Media clients do not consume more bandwidth (in kilobits per second) than the defined value.

To specify the maximum starting bandwidth:

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

```
SGOS#(config) streaming windows-media max-fast-bandwidth kbps
```

Configuring the SG Appliance Multicast Network

This section describes how to configure the SG appliance multicast service. Additional steps are required to configure the SG appliance to serve multicast broadcasts to streaming clients (Windows Media and Real Media). Those procedures are provided in subsequent sections.

Section B: Configuring Streaming Media

To configure the multicast service:

1. Select **Configuration > Services > Streaming Proxies > General**.

2. Configure Multicast options:
 - a. In the **Maximum Hops** field, enter a time-to-live (TTL) value.
 - b. In the **IP Range** fields, enter the IP address range.
 - c. In the **Port Range** fields, enter the port range.
3. Click **Apply**.
4. Enable Windows and Real Media multicast:
 - Real Media: See [Step 5](#) on page 53.
 - Windows Media: See ["Managing Multicast Streaming for Windows Media"](#) on page 63.

Configuring Media Server Authentication Type (Windows Media)

Note: This section applies to Windows Media streaming only and can only be configured through the CLI.

Configure the SG appliance to recognize the type of authentication the origin content server is using: BASIC or NTLM/Kerberos.

To configure the media server authentication type:

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

```
SGOS#(config) streaming windows-media server-auth-type {basic | ntlm}
```

Related CLI Syntax to Manage Streaming

- ❑ To enter configuration mode:


```
SGOS#(config) proxy-services
SGOS#(config proxy-services) create {mms | rtsp} service_name
```
- ❑ The following submodes are available:


```
SGOS#(config) streaming max-client-bandwidth kbits_second
SGOS#(config) streaming max-gateway-bandwidth kbits_second
```


Section B: Configuring Streaming Media

```

SGOS#(config) streaming {windows-media | real-media | quicktime} {max-
client-bandwidth kbits_second | no max-client-bandwidth}
SGOS#(config) streaming {windows-media | real-media | quicktime} {max-
gateway-bandwidth kbits_second | no max-gateway-bandwidth}
SGOS#(config) streaming {windows-media | real-media | quicktime} {max-
connections number | no max-connection}
SGOS#(config) streaming {windows-media | real-media | quicktime} http-
handoff disable
SGOS#(config) streaming {windows-media | real-media} refresh-interval
number.number
SGOS#(config) streaming real-media multicast enable
SGOS#(config) streaming windows-media server-auth-type {basic | ntlm}
SGOS#(config) content-distribute url [from url]

```

Reference: Access Log Fields

The default Blue Coat streaming fields are (only Streaming-specific or relative are listed and described):

```

c-ip date time c-dns cs-uri-scheme cs-host cs-uri-port cs-uri-path cs-
uri-query c-starttime x-duration c-rate c-status c-playerid c-
playerversion c-playerlanguage cs(User-Agent) cs(Referer) c-hostexe c-
hostexeever c-os c-osversion c-cpu filelength filesize avgbandwidth
protocol transport audiocodec videocodec channelURL sc-bytes c-bytes
s-pkts-sent c-pkts-received c-pkts-lost-client c-pkts-lost-net c-pkts-
lost-cont-net c-resendreqs c-pkts-recovered-ECC c-pkts-recovered-
resent c-buffercount c-totalbuffertime c-quality s-ip s-dns s-
totalclients s-cpu-util x-cache-user x-cache-info x-client-address

```

- ❑ audiocodec: Audio codec used in stream.
- ❑ avgbandwidth: Average bandwidth (in bits per second) at which the client was connected to the server.
- ❑ channelURL: URL to the .nsc file.
- ❑ c-buffercount: Number of times the client buffered while playing the stream.
- ❑ c-bytes: An MMS-only value of the total number of bytes delivered to the client.
- ❑ c-cpu: Client computer CPU type.
- ❑ c-hostexe: Host application.
- ❑ c-os: Client computer operating system.
- ❑ c-osversion: Client computer operating system version number.
- ❑ c-playerid: Globally unique identifier (GUID) of the player.
- ❑ c-playerlanguage: Client language-country code.
- ❑ c-playerversion: Version number of the player.
- ❑ c-rate: Mode of Windows Media Player when the last command event was sent.
- ❑ c-starttime: Timestamp (in seconds) of the stream when an entry is generated in the log file.
- ❑ c-status: Codes that describe client status.

Section B: Configuring Streaming Media

- ❑ `c-totalbuffertime`: Time (in seconds) the client used to buffer the stream.
- ❑ `filelength`: Length of the file (in seconds).
- ❑ `filesize`: Size of the file (in bytes).
- ❑ `protocol`: Protocol used to access the stream: `mms`, `http`, or `asfm`.
- ❑ `s-totalclients`: Clients connected to the server (but not necessarily receiving streams).
- ❑ `transport`: Transport protocol used (UDP, TCP, multicast, and so on).
- ❑ `videocodec`: Video codec used to encode the stream.
- ❑ `x-cache-info`: Values: `UNKNOWN`, `DEMAND_MISS`, `DEMAND_PARTIAL_HIT`, `DEMAND_HIT`, `LIVE_FROM_ORIGIN`, `LIVE_PARTIAL_SPLIT`, `LIVE_SPLIT`.
- ❑ `x-duration`: Length of time a client played content prior to a client event (FF, REW, Pause, Stop, or jump to marker).
- ❑ `x-wm-c-dns`: Hostname of the client determined from the Windows Media protocol.
- ❑ `x-wm-c-ip`: The client IP address determined from the Windows Media protocol.
- ❑ `x-cs-streaming-client`: Type of streaming client in use (`windows_media`, `real_media`, or `quicktime`).
- ❑ `x-rs-streaming-content`: Type of streaming content served.
- ❑ `x-streaming-bitrate`: The reported client-side bitrate for the stream.

Reference: CPL Triggers, Properties, and Actions

The following Blue Coat CPL is supported in Streaming:

Triggers

- ❑ `streaming.client=`
- ❑ `streaming.content=`

Properties and Actions

`streaming.transport=`

Streaming History Statistics

The Streaming History tabs (Windows Media, Real Media, and QuickTime) display bar graphs that illustrate the number of active client connections over the last 60 minutes, 24 hours, and 30 days. These statistics are not available through the CLI. The Current Streaming Data and Total Streaming Data tabs display real-time values for current connection and live traffic activity on the SG appliance. Current and total streaming data statistics are available through the CLI.

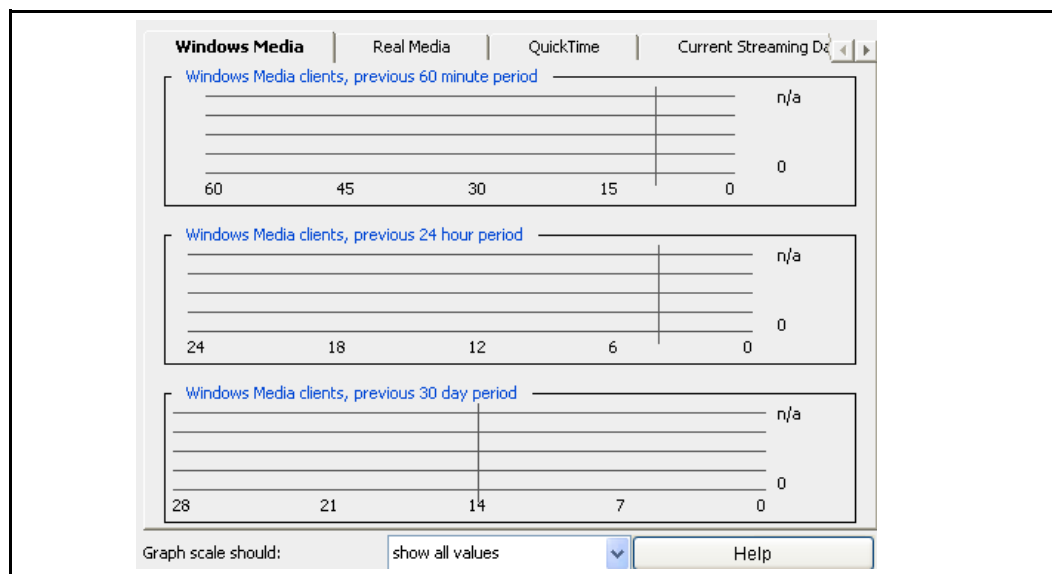
Viewing Windows Media Statistics

The Windows Media tab shows the number of active Windows Media client connections over the last 60 minutes, 24 hours, and 30 days.

Section B: Configuring Streaming Media

To view Windows Media client statistics:

1. Select **Statistics > Protocol Details > Streaming History > Windows Media**.



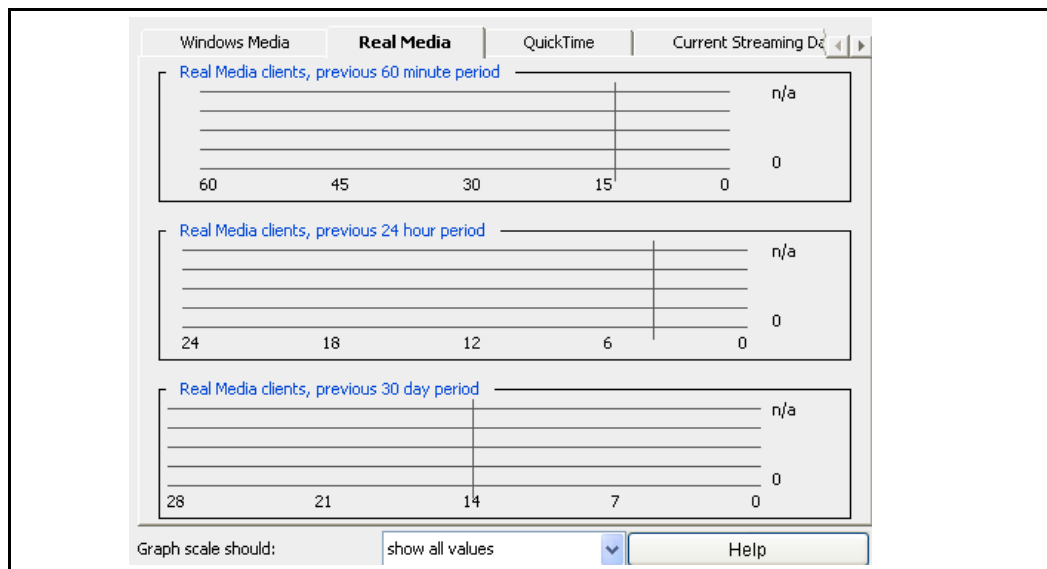
2. (Optional) To set the graph scale to a different value, select a value from the **Graph scale should** drop-down list.

Viewing Real Media Statistics

The Real Media tab shows the number of active Real Media client connections over the last 60-minutes, 24 hours, and 30 days.

To view Real Media data statistics:

1. Select **Statistics > Protocol Details > Streaming History > Real Media**.



2. (Optional) To set the graph scale to a different value, select a value from the **Graph scale should** drop-down list.

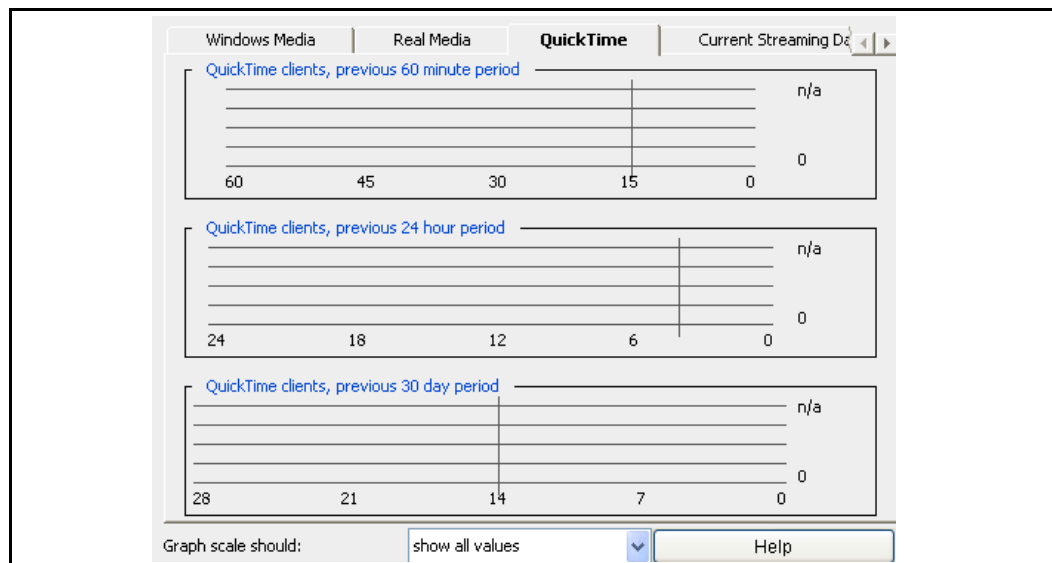
Section B: Configuring Streaming Media

Viewing QuickTime Statistics

The QuickTime tab shows the number of active QuickTime client connections over the last 60 minutes, 24 hours and 30 days.

To view QuickTime data statistics:

1. Select **Statistics > Protocol Details > Streaming History > QuickTime**.



2. (Optional) To set the graph scale to a different value, select a value from the **Graph scale should** drop-down list.

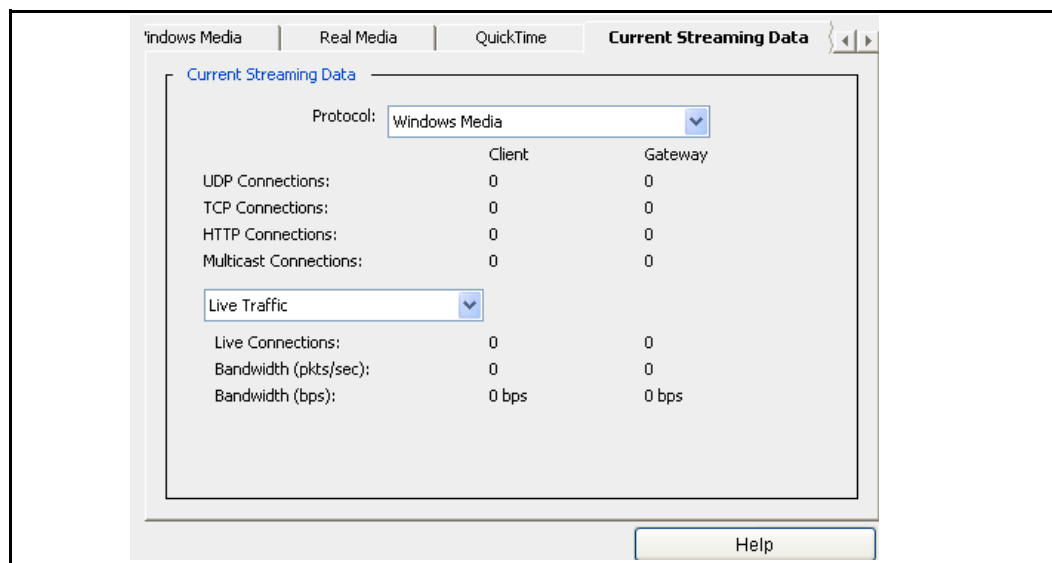
Viewing Current and Total Streaming Data Statistics

The Management Console **Current Streaming Data** tab and the **Total Streaming Data** tab show real-time values for Windows Media, Real Media, and QuickTime activity on the SG appliance. These statistics can also viewed through the CLI.

To view current streaming data statistics:

1. Select **Statistics > Protocol Details > Streaming History > Current Streaming Data**.

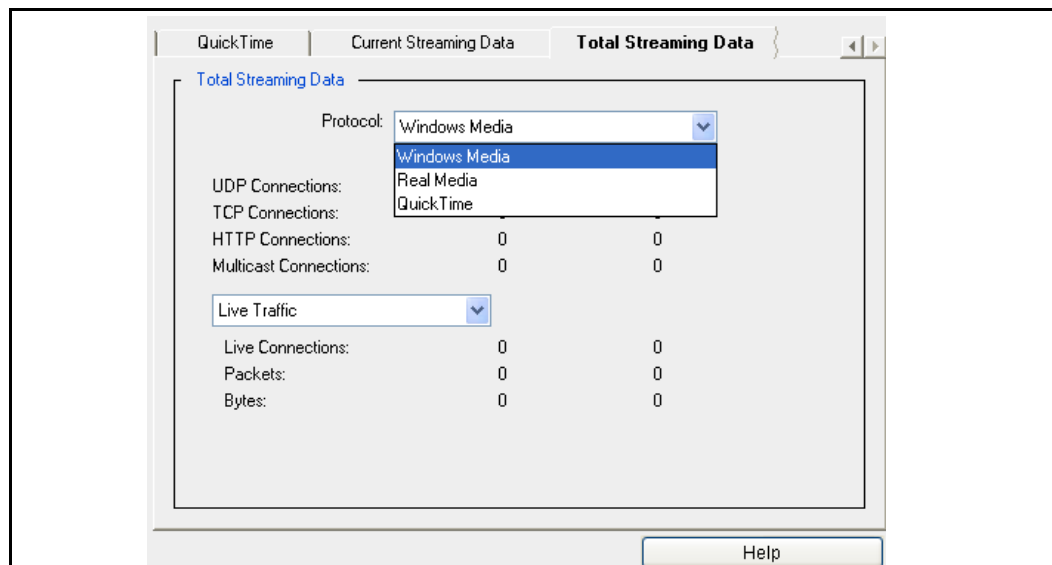
Section B: Configuring Streaming Media



2. Select a streaming protocol from the **Protocol** drop-down list.
3. Select a traffic connection type (**Live**, **On-Demand**, or **Pass-thru**) from the drop-down list.

To view total streaming data statistics:

1. Select **Statistics > Streaming History > Total Streaming Data**.



2. Select a streaming protocol from the **Protocol** drop-down list.
3. Select a traffic connection type (**Live**, **On-Demand**, or **Passthru**) from the drop-down list.

To clear streaming statistics:

Enter the following command at the prompt:

```
SGOS# clear-statistics {quicktime | real-media | windows-media}
```

Section B: Configuring Streaming Media

Viewing Streaming Bandwidth Gain

The Management Console **Streaming Bandwidth Gain** tab show real-time statistics for bandwidth gained when you employ

Section C: Additional Configuration Tasks—Windows Media (CLI)

Section C: Additional Configuration Tasks—Windows Media (CLI)

This section provides Windows Media configuration tasks that cannot be accomplished through the Management Console, but can be accomplished through the CLI.

This section contains the following topics:

- ❑ "Managing Multicast Streaming for Windows Media" on page 63
- ❑ "Managing Simulated Live Content (Windows Media)" on page 67
- ❑ "ASX Rewriting (Windows Media)" on page 69

Managing Multicast Streaming for Windows Media

This section describes multicast station and `.nsc` files, and describes how to configure the SG appliance to send multicast broadcasts to Windows Media clients.

About Multicast Stations

A multicast station is a defined location from where the Windows Media player retrieves live streams. This defined location allows `.asf` streams to be delivered to many clients using only the bandwidth of a single stream. Without a multicast station, streams must be delivered to clients through unicast.

A multicast station contains all of the information needed to deliver `.asf` content to a Windows Media player or to another SG appliance, including:

- ❑ IP address
- ❑ Port
- ❑ Stream format
- ❑ TTL value (time-to-live, expressed hops)

The information is stored in an `.nsc` file, which the Window Media Player must be able to access to locate the IP address.

If Windows Media Player fails to find proper streaming packets on the network for multicast, the player can roll over to a unicast URL. Reasons for this include lack of a multicast-enabled router on the network or if the player is outside the multicast station's TTL. If the player fails to receive streaming data packets, it uses the unicast URL specified in the `.nsc` file that is created from the multicast station configuration. All `.nsc` files contain a unicast URL to allow rollover.

Unicast to Multicast

Unicast to multicast streaming requires converting a unicast stream on the server-side connection to a multicast station on the SG appliance. The unicast stream must contain live content before the multicast station works properly. If the unicast stream is a video-on-demand file, the multicast station is created but is not able to send packets to the network. For video-on-demand files, use the `broadcast-alias` command, discussed below.

Multicast to Multicast

Use the `multicast-alias` command to get the source stream for the multicast station.

Section C: Additional Configuration Tasks—Windows Media (CLI)

About Broadcast Aliases

A broadcast alias defines a playlist, specify a starting time, date, and the number of times the content is repeated.

Creating a Multicast Station

To create a multicast station, you must perform the following:

- ❑ Define a name for the multicast station.
- ❑ Define the source of the multicast stream.
- ❑ The port range to be used.
- ❑ Define the address range of the multicast stream.
- ❑ Define the TTL value.
- ❑ Create the multicast alias, unicast alias, and broadcast alias commands to enable the functionality.

Syntax

```
multicast-station name {alias | url} [address | port | ttl]
```

where

- *name* specifies the name of the multicast station, such as *station1*.
- {*alias* | *url*} defines the source of the multicast stream. The source can be a URL or it can be a multicast alias, a unicast alias, or simulated live. (The source commands must be set up before the functionality is enabled within the multicast station.)
- [*address* | *port* | *ttl*] are optional commands that you can use to override the default ranges of these values. (Defaults and permissible values are discussed below.)

Example 1: Create a Multicast Station

This example:

- ❑ Creates a multicast station, named *station1*, on SG 10.25.36.47.
- ❑ Defines the source as `mms://10.25.36.47/tenchi`.
- ❑ Accepts the address, port, and TTL default values.

```
SGOS#(config) streaming windows-media multicast-station station1 mms://10.25.36.47/tenchi.
```

To delete multicast *station1*:

```
SGOS#(config) streaming no multicast-station station1
```

Example 2: Create a Broadcast Alias and Direct a Multicast Station to use It

This example:

- ❑ To allow unicast clients to connect through multicast, creates a broadcast alias named *array1*; defines the source as `mms://10.25.36.48/tenchi2`.
- ❑ Instructs the multicast station from Example 1, *station1*, to use the broadcast alias, *array1*, as the source.

Section C: Additional Configuration Tasks—Windows Media (CLI)

```
SGOS#(config) streaming windows-media broadcast-alias array1 mms://  
10.25.36.48/tenchi2 0 today noon  
SGOS#(config) streaming windows-media multicast-station station1  
array1
```

Changing Address, Port, and TTL Values

Specific commands allow you to change the address range, the port range, and the default TTL value. To leave the defaults as they are for most multicast stations and change it only for specified station definitions, use the `multicast-station` command.

The `multicast-station` command randomly creates an IP address and port from the specified ranges.

- ❑ Address-range: the default ranges from 224.2.128.0 to 224.2.255.255; the permissible range is 224.0.0.2 and 239.255.255.255.
- ❑ Port-range: the default ranges from 32768 to 65535; the permissible range is between 1 and 65535.
- ❑ TTL value: the default is 5 hops; the permissible range is from 1 to 255.

Syntax, with Defaults Set

```
multicast address-range <224.2.128.0>-<224.2.255.255>  
multicast port-range <32768>-<65535>  
multicast ttl <5>
```

Getting the .nsc File

The `.nsc` file is 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.

To get an `.nsc` file from newly created `station1`, open the file by navigating through the browser to the multicast station's location (where it was created) and save the file as `station1.nsc`.

The file location, based on the streaming configuration above:

```
http://10.25.36.47/MMS/nsc/station1.nsc
```

Save the file as `station1.nsc`.

Note: You can also enter the URL in the Windows Media Player to start the stream.

The newly created file is not editable; the settings come from streaming configuration file. In that file, you have already defined the following pertinent information for the file:

- ❑ The address, which includes TTL, IP Address, IP Port, Unicast URL, and the NSC URL. All created `.nsc` files contain a unicast URL for rollover in case the Windows Media Player cannot find the streaming packets.
- ❑ The description, which references the MMS URL that you defined.
- ❑ The format, which contains important ASF header information. All streams delivered by the multicast station definition have their ASF headers defined here.

Section C: Additional Configuration Tasks—Windows Media (CLI)

Monitoring the Multicast Station

You can determine the multicast station definitions by viewing the streaming windows configuration. To determine the current client connections and current SG appliance connections, use the `show streaming windows-media statistics` command.

To view the multicast station setup:

```
SGOS#(config) show streaming windows config
; Windows Media Configuration
license:      1XXXXXXX-7XXXXXXX-7XXXXX
logging:      enable
logging       enable
http-handoff: enable
live-retransmit: enable
transparent-port (1755): enable
explicit proxy: 0
refresh-interval:          no refresh interval (Never check freshness)
max connections:          no max-connections (Allow maximum
connections)
max-bandwidth:            no max-bandwidth (Allow maximum bandwidth)
max-gateway-bandwidth:    no max-gateway-bandwidth (Allow maximum
bandwidth)
multicast address:        224.2.128.0 - 224.2.255.255
multicast port:           32768 - 65535
multicast TTL:            5
asx-rewrite:              No rules
multicast-alias:          No rules
unicast-alias:            No rules
broadcast-alias:          No rules
multicast-station:        station1 mms://10.25.36.47/tenchi
224.2.207.0 40465 5 (playing)
```

Note: *Playing* at the end of the multicast station definition indicates that the station is currently sending packets onto the network. The IP address and port ranges have been randomly assigned from among the default ranges allowed.

To view the multicast station statistics:

```
SGOS#(config) show streaming windows stat
;Windows Media Statistics
Current client connections:
  by transport: 0 UDP, 0 TCP, 0 HTTP, 1 multicast
  by type: 1 live, 0 on-demand
Current gateway connections:
  by transport: 0 UDP, 1 TCP, 0 HTTP, 0 multicast
  by type: 1 live, 0 on-demand
```

Section C: Additional Configuration Tasks—Windows Media (CLI)

Managing Simulated Live Content (Windows Media)

This section describes simulated live content and how to configure the SG appliance to manage and serve simulated live content.

About Simulated Live Content

The simulated live content feature 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. If used in conjunction with the `multicast-alias` command, the live content is multicast; otherwise, live content is accessible as live-splitting sources. The feature does *not* require the content to be cached.

When a starting date and time for the simulated live content have been set, the broadcast of the content starts when there is at least one client requesting the file. Clients requesting the simulated live content before the scheduled time are put into wait mode. Clients requesting the content after all of the contents have played receive an error message. Video-on-demand content does not need to be on the SG appliance before the scheduled start time, but prepopulating the content on the appliance provides better streaming quality.

Before configuring simulated live, consider the following:

- ❑ The simulated live content name must be unique. Aliases are not case sensitive.
- ❑ The name cannot be used for both a unicast and a multicast alias name.
- ❑ After simulated live content is referenced by one or more multicast stations, the simulated live content cannot be deleted until all multicast stations referencing the simulated live content are first deleted.

The multicast station appears as another client of simulated live content, just like a Windows Media Player.

Note: This note applies to HTTP only. If a client opens Windows Media player and requests an alias before the starting time specified in the `broadcast-alias` option, the HTTP connection closes after a short time period. When the specified time arrives, the player fails to reconnect to the stream and remains in waiting mode.

Three scenarios can occur when a client requests the simulated live content:

- ❑ Clients connect before the scheduled start time of the simulated live content: clients are put into *wait* mode.
- ❑ Clients connect during the scheduled playback time of the simulated live content: clients receive cached content for playback.
- ❑ Clients connect after the scheduled playback time of the simulated live: the client receives an error message.

The SG Appliance computes the starting playtime of the broadcast stream based on the time difference between the client request time and the simulated live starting time.

Section C: Additional Configuration Tasks—Windows Media (CLI)

Creating a Broadcast Alias for Simulated Live Content

Syntax

```
streaming windows-media broadcast-alias alias url loops date time
```

where:

- *alias* is the name of the simulated live content.
- *url* is the URL for the video-on-demand stream. Up to 128 URLs can be specified for simulated live content.
- *loops* is the number of times you want the content to be played back. Set to 0 (zero) to allow the content to be viewed an indefinite number of times.
- *date* is the simulated live content starting date. Valid date strings are in the format *yyyy-mm-dd* or *today*. You can specify up to seven start dates by using the comma as a separator (no spaces).
- *time* is the simulated live content starting time. Valid time strings are in the format *hh:mm* (on a 24-hour clock) or one of the following strings:
 - midnight, noon
 - 1am, 2am, ...
 - 1pm, 2pm, ...

Specify up to 24 different start times within a single date by using the comma as a separator (no spaces).

Example 1

This example creates a playlist for simulated live content. The order of playback is dependent on the order you enter the URLs. Up to 128 URLs can be added.

```
SGOS#(config) streaming windows-media broadcast-alias alias url
```

Example 2

This example demonstrates the following:

- ❑ creates a simulated live file called *bca*.
- ❑ plays back `mms://ocs.bca.com/bca1.asf` and `mms://ocs.bca.com/bca2.asf`.
- ❑ configures the SG appliance to play back the content twice.
- ❑ sets a starting date and time of today at 4 p.m., 6 p.m., and 8 p.m.

```
SGOS#(config) streaming windows-media broadcast-alias bca mms://  
ocs.bca.com/bca1.asf 2 today 4pm,6pm,8pm  
SGOS#(config) streaming windows-media broadcast-alias bca mms://  
ocs.bca.com/bca2.asf
```

To delete simulated live content:

```
SGOS#(config) streaming windows-media no broadcast-alias alias
```

Section C: Additional Configuration Tasks—Windows Media (CLI)

ASX Rewriting (Windows Media)

This section describes ASX rewriting and applies to Windows Media only.

About ASX Rewrite

If your environment does not use a Layer 4 switch or the Cisco Web Cache Control Protocol (WCCP), the SG appliance can operate as a proxy for Windows Media Player clients by rewriting the Windows Media metafile (which contains entries with URL links to the actual location of the streaming content) to point to the appliance rather than the Windows Media server. The metadata files can have `.asx`, `.wvx`, or `.wax` extensions, but are commonly referred to as `.asx` files. The `.asx` file refers to the actual media files (with `.asf`, `.wmv`, and `.wma` extensions). An `.asx` file can refer to other `.asx` files, although this is not a recommended practice. If the file does not have one of the metafile extensions and the Web server that is serving the metadata file does not set the correct MIME type, it is not processed by the Windows Media module. Also, the `.asx` file with the appropriate syntax must be located on an HTTP (not Windows Media) server.

The ASX rewrite module is triggered by either the appropriate file extension or the returned MIME type from the server (`x-video-asf`).

Note: If an `.asx` file syntax does not follow the standard `<ASX>` tag-based syntax, the ASX rewrite module is not triggered.

For the SG appliance to operate as a proxy for Windows Media Player requires the following:

- ❑ The client is explicitly proxied for HTTP content to the SG appliance that rewrites the `.asx` metafile.
- ❑ The streaming media SG appliance is configurable.

Note: Windows Media Player automatically tries to roll over to different protocols according to its Windows Media property settings before trying the rollover URLs in the `.asx` metafile.

With the `asx-rewrite` command, you can implement redirection of the streaming media to a SG appliance by specifying the rewrite protocol, the rewrite IP address, and the rewrite port.

The protocol specified in the ASX rewrite rule is the protocol the client uses to reach the SG. You can use forwarding and policy to change the default protocol specified in the original `.asx` file that connects to the origin media server.

When creating ASX rewrite rules, you need to determine the number priority. It is likely you will create multiple ASX rewrite rules that affect the `.asx` file; for example, rule 100 could redirect the IP address from `10.25.36.01` to `10.25.36.47`, while rule 300 could redirect the IP address from `10.25.36.01` to `10.25.36.58`. In this case, you are saying that the original IP address is redirected to the IP address in rule 100. If that IP address is not available, the SG looks for another rule matching the incoming IP address.

Section C: Additional Configuration Tasks—Windows Media (CLI)

Notes and Interactivities

Before creating rules, consider the following.

- ❑ Each rule you create must be checked for a match; therefore, performance might be affected if you create large amounts of rules.
- ❑ Lower numbers have a higher priority than high numbers.

Note: Rules can only be created through the CLI.

- ❑ ASX rewrite rules configured for multiple SG appliances configured in an HTTP proxy-chaining configuration can produce unexpected URL entries in access logs for the *downstream* SG appliance (the SG appliance that the client proxies to). The combination of proxy-chained SG appliances in the HTTP path coupled with ASX rewrite configured for multiple SG appliances in the chain can create a rewritten URL requested by the client in the example form of:

```
protocol1://downstream_SecApp/redirect?protocol2://<upstream_
SecApp>/redirect?protocol3://origin_host/origin_path
```

In this scenario, the URL used by the downstream SG for caching and access logging can be different than what is expected. Specifically, the downstream SG appliance creates an access log entry with `protocol2://upstream_SecApp/redirect` as the requested URL. Content is also cached using this truncated URL. Blue Coat recommends that the ASX rewrite rule be configured for only the downstream SG appliance, along with a proxy route rule that can forward the Windows Media streaming requests from the downstream to upstream SG appliances.

Syntax for the *asx-rewrite* Command:

```
asx-rewrite rule # in-addr cache-proto cache-addr [cache-port]
```

where:

- *in-addr*—Specifies the hostname or IP address delivering the content
- *cache-proto*—Specifies the rewrite protocol on the SG. Acceptable values for the rewrite protocol are:
 - `mmsu` specifies Microsoft Media Streaming UDP
 - `mmst` specifies Microsoft Media Streaming TCP
 - `http` specifies HTTP
 - `mms` specifies either MMS-UDP or MMS-TCP
 - `*` specifies the same protocol as in the `.asx` file

If the `.asx` file is referred from within another `.asx` file (not a recommended practice), use a `*` for the *cache-proto* value. This specifies that the protocol specified in the original URL is used. As a conservative, alternative approach, you could use HTTP for the *cache-proto* value.
- *cache-addr*—Specifies the rewrite address on the SG appliance.
- *cache-port*—Specifies the port on the SG appliance. This value is optional.

Section C: Additional Configuration Tasks—Windows Media (CLI)

To set up the .asx rewrite rules:

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

```
SGOS#(config) streaming windows-media asx-rewrite number in-addr  
cache-proto cache-addr cache-port
```

Note: To delete a specific rule, enter `streaming windows-media no asx-rewrite number`.

To ensure that an ASX rewrite rule has been modified immediately, clear the local browser cache.

Example

This example:

- ❑ Sets the priority rule to 200
- ❑ Sets the protocol to be whatever protocol was originally specified in the URL and directs the data stream to the appropriate default port.
- ❑ Provides the rewrite IP address of 10.9.44.53, the SG appliance.

```
SGOS#(config) streaming windows-media asx-rewrite 200 * * 10.9.44.53
```

Note: ASX files must be fetched from HTTP servers. If you are not sure of the network topology or the content being served on the network, use the asterisks to assure the protocol set is that specified in the URL.

ASX Rewrite Incompatibility With Server-side IWA Authentication

Server-side authentication (MMS only, not HTTP) is supported if the origin media server authentication type is BASIC or No Auth. However, if you know that a Windows Media server is configured for IWA authentication, the following procedure allows you to designate any virtual IP addresses to the IWA authentication type. If you know that all of the activity through the SG appliance requires IWA authentication, you can use the IP address of the appliance.

To designate an IP address to an authentication type:

1. If necessary, create a virtual IP address that is used to contact the Windows Media server.
2. At the (config) prompt, enter the following command:

```
SGOS#(config) streaming windows-media server-auth-type ntlm ip_address
```
3. Configure the ASX rewrite rule to use the IP address.
 - a. To remove the authentication type designation:

```
SGOS#(config) streaming windows-media no server-auth-type  
ip_address
```
 - b. To return the authentication type to BASIC:

```
SGOS#(config) streaming windows-media server-auth-type basic  
ip_address
```


Section D: Windows Media Player

Section D: Windows Media Player

This section describes how to configure the Windows Media Player to communicate through the SG appliance.

Configuring Windows Media Player

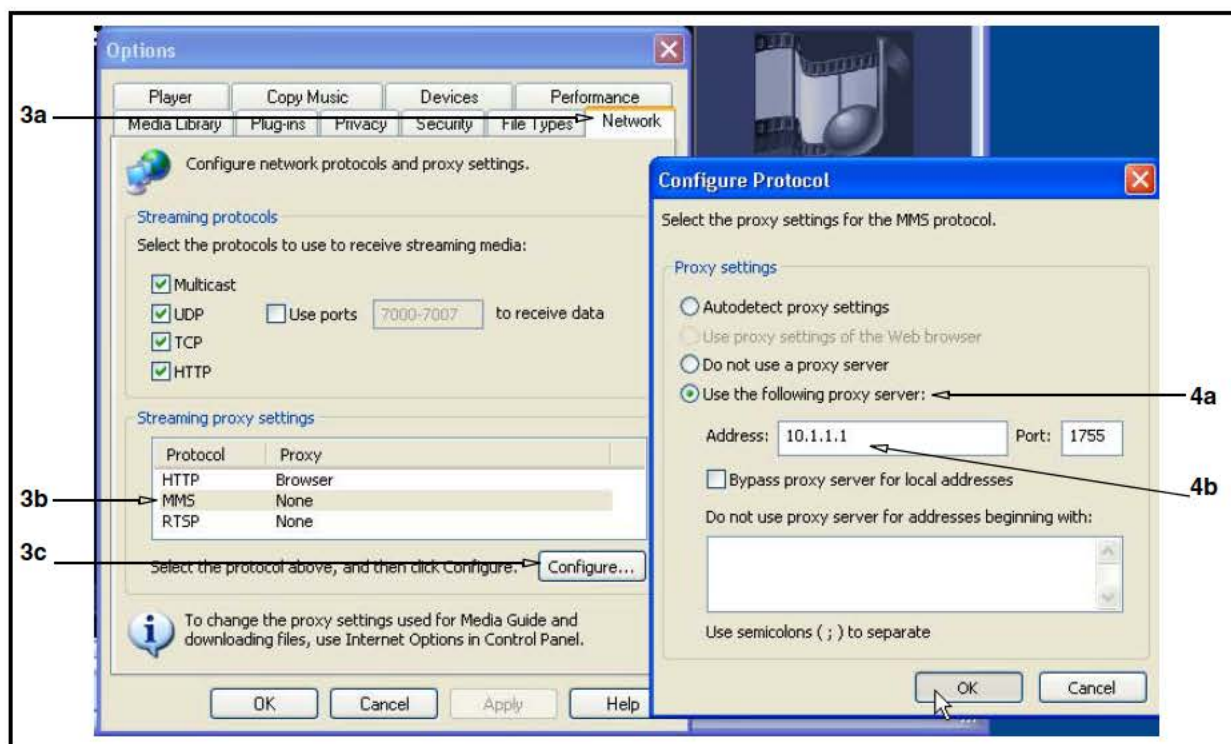
To apply the SG appliance Windows Media streaming services, Windows Media Player must be installed and configured to use explicit proxy.

MMS explicit proxy is defined with the `asx-rewrite` command (discussed earlier in this chapter) or with CPL (`url_host_rewrite`).

Note: The example below uses Windows Media Player 9.0. Installation and setup varies with different versions of Windows Media Player.

To configure Windows Media Player:

1. Start Windows Media Player.
2. Select **Tools > Options**.



Section D: Windows Media Player

3. Navigate to protocol configuration:
 - a. Select **Network**.
 - b. Select **MMS**.
 - c. Click **Configure**. The Configure Protocol Dialog appears.
4. Configure the proxy settings:
 - a. Select **Use the following proxy server**.
 - b. Enter the SG appliance IP address and the port number used for the explicit proxy (the default MMS port is 1755). These settings must match the settings configured in the SG appliance. If you change the SG appliance explicit proxy configuration, you must also reconfigure the Windows Media Player.
5. Click **OK** in both dialogs. Result: the Windows Media Player now proxies through the SG appliance and content is susceptible to streaming configurations and access policies.

Windows Media Player Inter-activity Notes

This section describes Windows Media Player interactivities that might affect performance.

Striding

When you use the Windows Media Player, consider the following interactivities in regard to using fast forward and reverse (referred to as *striding*):

- ❑ If you request a cached file and repeatedly attempt play and fast forward, the file freezes.
- ❑ If you attempt a fast reverse of a cached file that is just about to play, you receive an error message, depending on whether you have a proxy:
 - Without a proxy: A device attached to the system is not functioning.
 - With a proxy: The request is invalid in the current state.
- ❑ If Windows Media Player is in pause mode for more than ten minutes and you press fast reverse or fast forward, an error message displays: `The network connection has failed`.

Other Notes

- ❑ Applies to Versions 9: if a `url_host_rewrite` rule is configured to rewrite a host name that is a domain name instead of an IP address, a request through the MMS protocol fails and the host is not rewritten. As the connect message sent by the player at the initial connection does not contain the host name, a rewrite cannot occur. HTTP requests are not affected by this limitation.
- ❑ If explicit proxy is configured and the access policy on the SG appliance is set to `deny`, a requested stream using HTTP from Windows Media Player 9 serves the stream directly from the origin server even after the request is denied. The player sends a request to the OCS and plays the stream from there.

Section D: Windows Media Player

Blue Coat recommends the following policy:

```
<proxy>
  streaming.content=yes deny
-or-
<proxy>
  streaming.content=windows_media deny
```

The above rules force the HTTP module to hand-off HTTP requests to the MMS module. MMS returns the error properly to the player, and does not go directly to the origin server to try to server the content.

- ❑ If you request an un-cached file using the HTTP protocol, the file is likely to stop playing if the authentication type is set to BASIC or NTLM/Kerberos and you initiate rapid seeks before the buffering begins for a previous seek. The Windows Media Player, however, displays that the file is still playing.
- ❑ If a stream is scheduled to be accessible at a future time (using a simulated live rule), and the stream is requested before that time, the Windows Media Player enters a waiting stage. This is normal. However, if HTTP is used as the protocol, after a minute or two the Windows Media Player closes the HTTP connection, but remains in the waiting stage, even when the stream is broadcasting.

Notes:

For authentication-specific notes, see ["Windows Media Server-Side Authentication"](#) on page 47 and ["Windows Media Proxy Authentication"](#) on page 47.

Section E: RealPlayer

Section E: RealPlayer

This section describes how to configure the Windows Media Player to communicate through the SG appliance.

Configuring RealPlayer

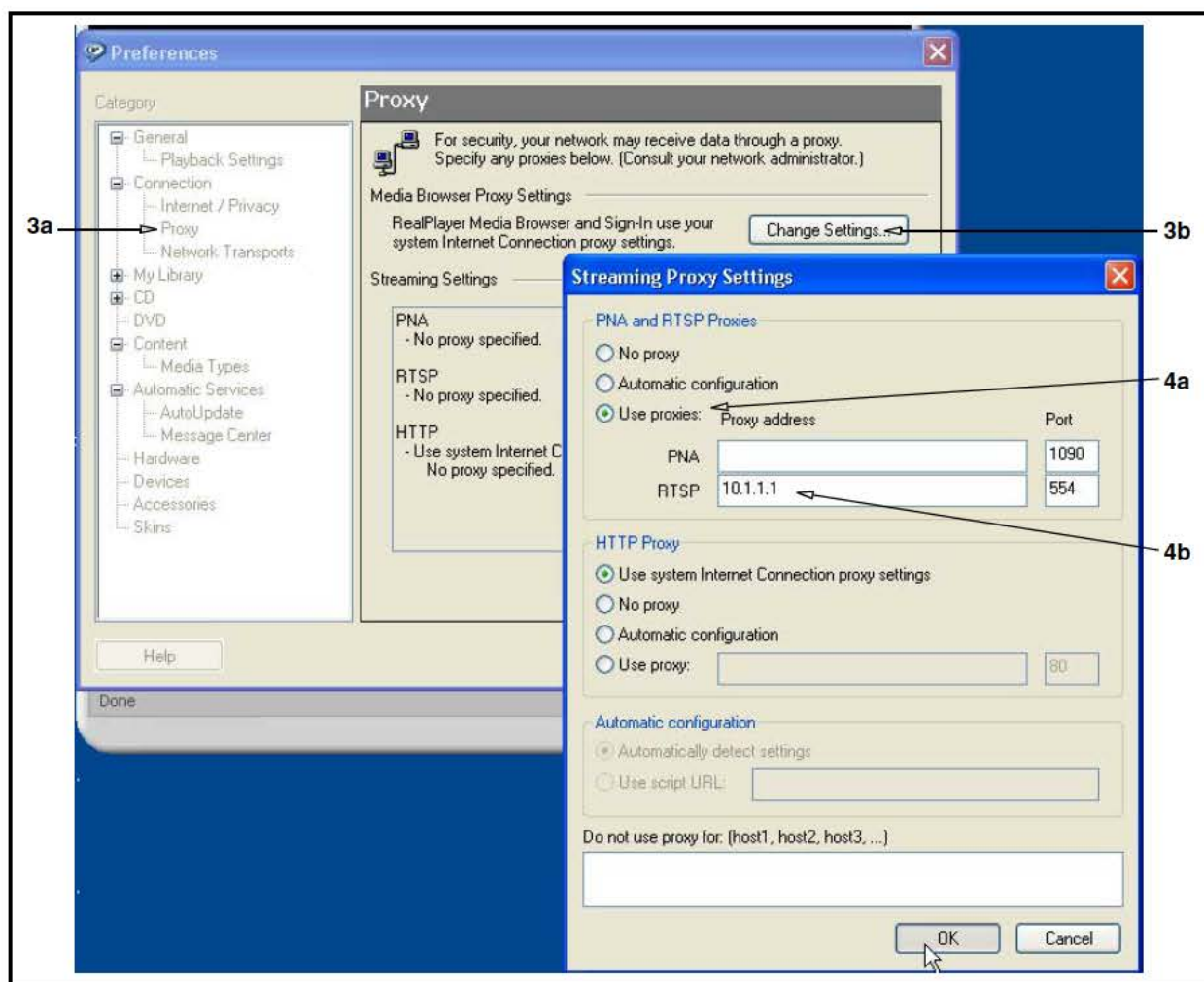
To use the SG appliance Real Media streaming services with an explicit proxy configuration, the client machine must have RealPlayer installed and configured to use RTSP streams. If you use transparent proxy, no changes need to be made to the RealPlayer.

Note: This procedure features RealPlayer, version 10.5. Installation and setup menus vary with different versions of RealPlayer. Refer to the RealPlayer documentation to configure earlier versions of RealPlayer.

To configure RealPlayer:

1. Start RealPlayer.
2. Select **Tools > Preferences**.

Section E: RealPlayer



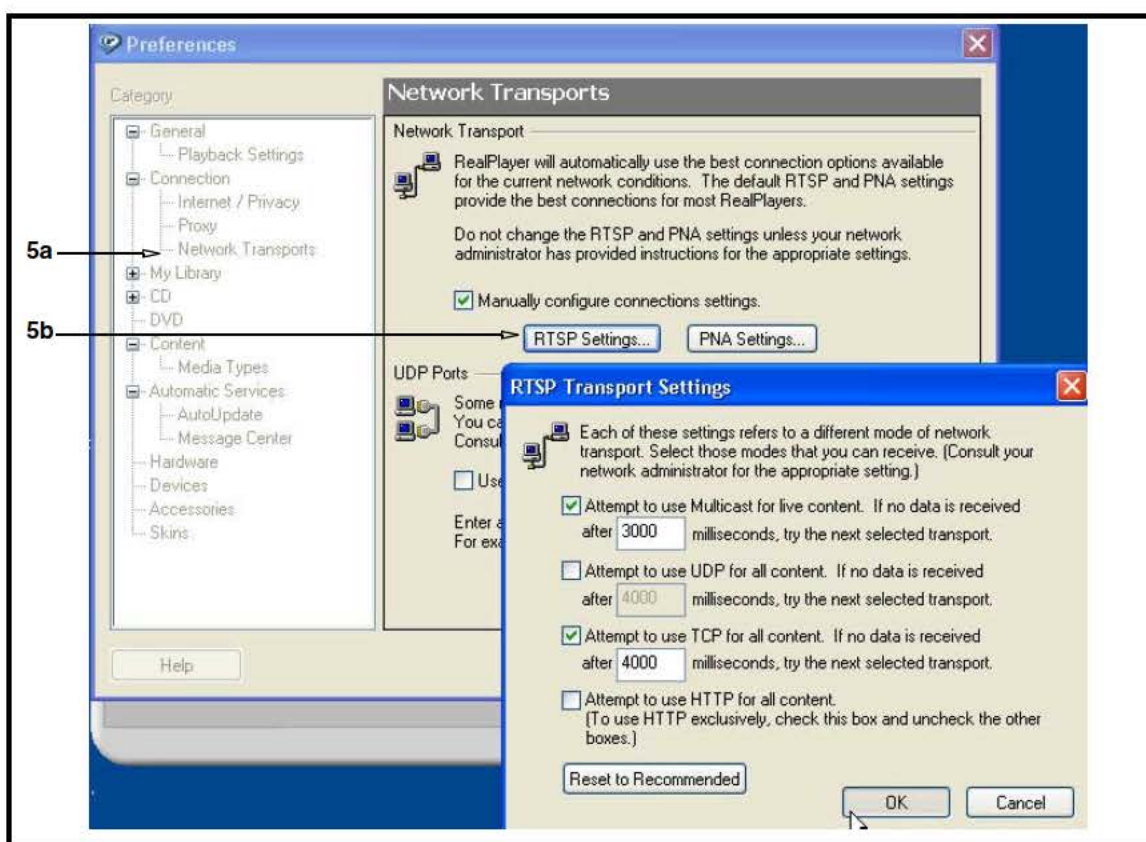
3. Navigate to proxy settings:
 - a. Select **Connection > Proxy**.
 - b. Click **Change Settings**. The Streaming Proxy Settings dialog appears.
4. Configure options:
 - a. In the **PNA and RTSP proxies:** field, select **Use proxies**.
 - b. Enter the SG IP address and the port number used for the explicit proxy (the default RTSP port is 544). These settings must match the settings configured in the SG appliance. If you change the SG appliance explicit proxy configuration, you must also reconfigure the RealPlayer. If using transparent proxy, RTSP port 554 is set by default and cannot be changed.

Note: For **HTTP Proxy**, if you have an HTTP proxy already configured in your browser, select **Use system Internet Connection proxy settings**.

- c. Optional: For **HTTP Proxy**, if you have an HTTP proxy already configured in your browser, select **Use system Internet Connection proxy settings**.
- d. Optional: In the **Do not use proxy for:** section, you can enter specific hosts and bypass the SG appliance.

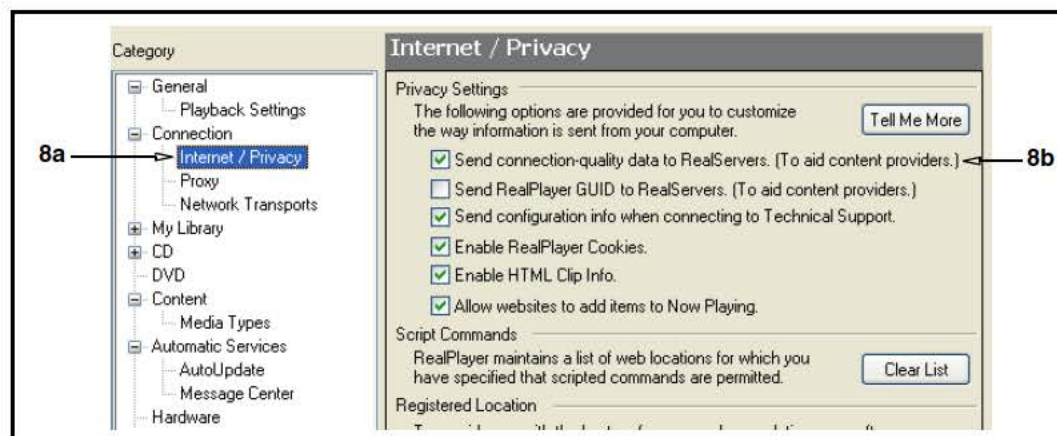
Note: This can also be accomplished with policy, which is the method Blue Coat recommends.

- e. Click **OK** to close the Streaming Proxy Settings dialog.



5. Configure RealPlayer transport settings:
 - a. Select **Connection > Network Transports**.
 - b. Click **RTSP Settings**. The RTSP Transport Settings dialog appears.
6. If required, deselect options, based on your network configuration. For example, if your firewall does not accept UDP, you can deselect **Attempt to use UDP for all content**, but leave the TCP option enabled. Blue Coat recommends using the default settings.
7. Click **OK**.

To allow the creation of access log entries, RealPlayer must be instructed to communicate with the RealServer.



8. Perform the following:

- a. **Select View > Preferences > Internet/Privacy.**
- b. In the **Privacy** field, select **Send connection-quality data to RealServers**; click **OK**.

Result: the RealPlayer now proxies through the SG appliance and content is susceptible to streaming configurations and access policies.

Notes:

For authentication-specific issues, see “[Real Media Proxy Authentication](#)” on page 48.

Section F: QuickTime Player

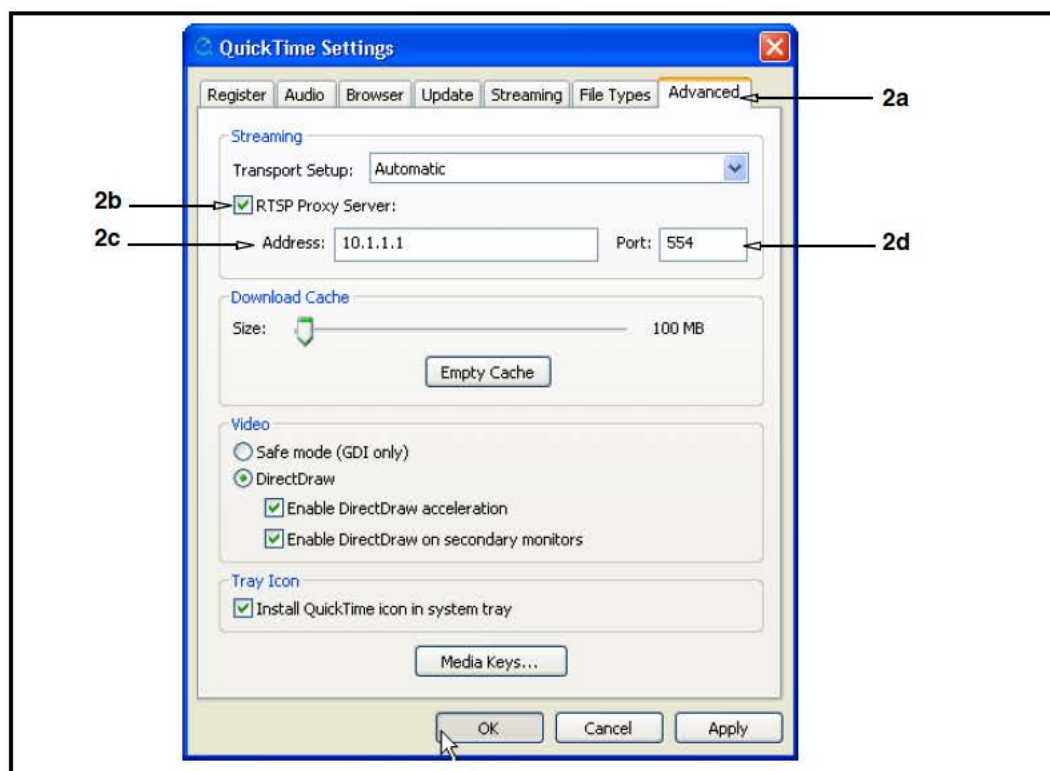
This section describes how to configure the QuickTime client.

Configuring QuickTime Player

This section describes how to configure the QuickTime player for explicit proxy to the SG appliance.

To configure QuickTime

1. Select **Edit > Preferences > QuickTime Preferences**.



2. Configure the protocol settings:
 - a. Click **Advanced**.
 - b. Select **RTSP Proxy Server**;
 - c. Enter the IP address of the SG appliance to connect to.
 - d. Enter the port number (554 is the default).

These settings must match the settings configured in the SG appliance. If you change the SG appliance explicit proxy settings, set similar settings in RealPlayer.

3. Close **OK**. Result: the QuickTime now proxies—in pass-through mode—through the SG appliance.

Notes:

For authentication-specific issues, see “[QuickTime Proxy Authentication](#)” on page 48.

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	<p>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.</p> <p>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.</p>
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</i> proxy service (d efault).
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>
O	
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.
P	
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	<i>See</i> 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. <i>See also</i> 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. <i>See also</i> 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 www.mycompany.com , the appliance is actually receiving the content from the server on 10.253.123.123. The client is unaware that mycompany.com 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 ftp:// 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.
Websense 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

- ASX rewrite
 - command syntax 69
 - rules 69
 - setting up for Windows Media 68

B

- Blue Coat SG
 - instant messaging
 - configuring clients 20
 - proxy authentication 9
 - securing 9
 - Yahoo Messenger client configuration 23
 - instant messaging, IM clients tab statistics 31
 - instant messaging, IM data tab statistics 30

D

- document
 - conventions 7

H

- HTTP
 - handoff, enabling 39

I

- instant messaging
 - configuring clients 20
 - proxy authentication 9
 - securing 9
 - statistics, IM clients tab 31
 - statistics, IM data tab 30
 - Yahoo Messenger client configuration 23

M

- multicast
 - defined 37
 - unicast, converting by Windows Media 38

P

- port services
 - instant messaging protocols 9
- proxies
 - definition 7

R

- RealMedia
 - proxy authentication 47
- RTSP over Windows Media, about 43

S

- streaming
 - WM over RTSP, about 43
- streaming media
 - delivery type 37
 - live content defined 38
 - multicast defined 37
 - prepopulating content, description 42
 - unicast defined 37

U

- unicast
 - defined 37
 - multicast, converting from by Windows Media 38

W

- Windows Media
 - .ASX-rewrite rules 69
 - .nsc file 64
 - ASX rewrite and NTLM incompatibility 70
 - authentication limitations 46
 - HTTP handoff enabling 39
 - multicast station monitoring 65
 - multicast to unicast 38
 - over RTSP 43
 - prepopulating content description 42
 - setting up ASX rewrite 68

