

# ProxySG Web Visual Policy Manager Reference

Version 7.2.x

Guide Revision:  
12/10/2020



## **Symantec: A Division of Broadcom**

### **Legal Notice**

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2020 Broadcom. All Rights Reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit [www.broadcom.com](http://www.broadcom.com).

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Thursday, December 10, 2020

# Table of Contents

"About the ProxySG Web Visual Policy Manager Reference" on page 5

"Managing Policy Files" on page 6

- "Creating and Editing Policy Files" on page 7
- "Unloading Policy Files" on page 11
- "Configuring Policy Options" on page 12
- "Managing the Central Policy File" on page 14
- "Viewing Policy Files" on page 16

"Visual Policy Manager" on page 18

- "VPM Overview" on page 19
- " Layers" on page 23
- "Policy Rules " on page 25
- "Enforcement Domains" on page 26
- "About Code Sharing With the Management Console" on page 29
- "Policy Layer and Rule Object Reference" on page 30
- "VPM Object Reference" on page 52
- "Managing Policy Layers, Rules, and Files" on page 149
- "Tutorials" on page 160
- "Composing CPL Directly in the VPM" on page 173

"Advanced Policy Tasks" on page 174

- "Blocking Pop-Up Windows" on page 175
- "Exempting Non-Contiguous IP Addresses" on page 177
- "Stripping or Replacing Active Content" on page 179
- "Modifying Headers" on page 182
- "Defining Exceptions" on page 183
- "Managing Peer-to-Peer Services" on page 196

## **Symantec: A Division of Broadcom**

- "Managing QoS and Differentiated Services" on page 200
- "Providing Read-Only Access in the Management Console" on page 206
- "Setting Policy for Content and Content-Type Filtering" on page 208

Additional SGOS Documentation

# About the ProxySG Web Visual Policy Manager Reference

Creating policy is the core task of implementing ProxySG appliances in the enterprise. After the basic ProxySG configurations are complete, defined policy is what controls user activities and implements company authentication and network resource allocation goals.

The Visual Policy Manager is a user interface that creates underlying Content Policy Language (CPL). In the VPM, you create policy layers by selecting and customizing policy objects. This document discusses the facets of the VPM, including layer interactions and summary object descriptions. When appropriate, cross references are provided to other Symantec documents that describe the conceptual information of the feature. It also contains a chapter that discusses some common tasks that are only achieved through policy, not the Management Console.

This document discusses creating and implementing policy using the Web Visual Policy Manager.

# Managing Policy Files

Policy files contain the policies (triggers and actions) that manage every aspect of the ProxySG appliance, from controlling user authentication and privileges to disabling access logging or determining the version of SOCKS.

The policy for a given system can contain several files with many layers and rules in each. Policies can be defined through the Visual Policy Manager (VPM) or composed in Content Policy Language (CPL). (Some advanced policy features are not available in and can only be configured through CPL.)

Policies are managed through four files:

- **Central**—Contains global settings to improve performance and behavior and filters for important and emerging viruses. This file is managed by Symantec, but you can point the ProxySG appliance to a custom Central policy file instead.
- **Forward**—Usually used to supplement any policy created in the other three policy files. The Forward policy file contains Forwarding rules, for example, when the system is upgraded from a previous version of SGOS.
- **Local**—A file you create yourself. When the is not the primary tool used to define policy, the Local file contains the majority of the policy rules for a system. If the is the primary tool, this file is either empty or includes rules for advanced policy features that are not available in.
- **Visual Policy Manager**—The policy created by the can either supplement or override the policies created in the other policy files.

**Caution:** If you import policy that was created externally (for example, by a third-party tool) into a policy file, the ProxySG appliance validates the policy file's contents for syntax errors but cannot check for formatting or typographical mistakes. Such errors may result in unintended behavior after the policy is loaded. Symantec strongly recommends that you review the CPL in imported policy for correctness before installing the file.

# Creating and Editing Policy Files

You can create and edit policy files using either the Management Console or the `inline policy` CLI command. Symantec recommends using the Management Console for its ease of use and ability to keep layers separate while editing, whereas using `inline policy` overwrites any existing policy on the appliance.

## Creating and Editing Policy Files Using the Management Console

Compose CPL in the CPL Layer using one of the following methods:

- Use the appliance Text Editor, which allows you to enter directives (or copy and paste the contents of an already-created file) directly onto the appliance.
- Create a file on your local system; the appliance can browse to the file and install it.
- Use a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the appliance.

The appliance compiles the new policy from all source files and installs the policy, if the compilation is successful.

If errors or warnings are produced when you load the policy file, a summary of the errors and/or warnings is displayed automatically. If errors are present, the policy file is not installed. If warnings are present, the policy file is installed, but the warnings should be examined.

Define and install policy files directly:

1. Select **Configuration > Policy > Policy Files > Policy Files**.

The screenshot shows the 'Policy Files' tab in the Management Console. It contains two main sections: 'Install Policy' and 'View Policy'.

**Install Policy Section:**

- Three rows for installing files from a 'Remote URL':
  - 'Install Local File from:' with a dropdown menu and an 'Install' button.
  - 'Install Forward File from:' with a dropdown menu and an 'Install' button.
  - 'Install Central File from:' with a dropdown menu and an 'Install' button.
- Two checked checkboxes:
  - ☒ Automatically install new Policy when central file changes
  - ☒ Send me email when central file changes

**View Policy Section:**

- A 'View File:' dropdown menu currently set to 'Current Policy' and a 'View' button.

2. From the Install Local/Forward/Central File from drop-down list, select the method used to install the local, forward, or central policy configuration; click Install and complete one of the three procedures below:

**Tip:** A message is written to the event log when you install a list through the appliance.

- Installing a policy file using a Remote URL.

In the Install Local/Forward/Central File dialog that displays, enter the fully-qualified URL, including the filename, where the policy configuration is located. To view the file before installing it, click View. Click Install. The Installation Status field summarizes the results; click Results to open the policy installation results window. Close the window when you are finished viewing the results; click OK in the Install Local/Forward/Central File dialog.

If you install a Central policy file, the default is already entered; change this field only if you want to create a custom Central policy file.

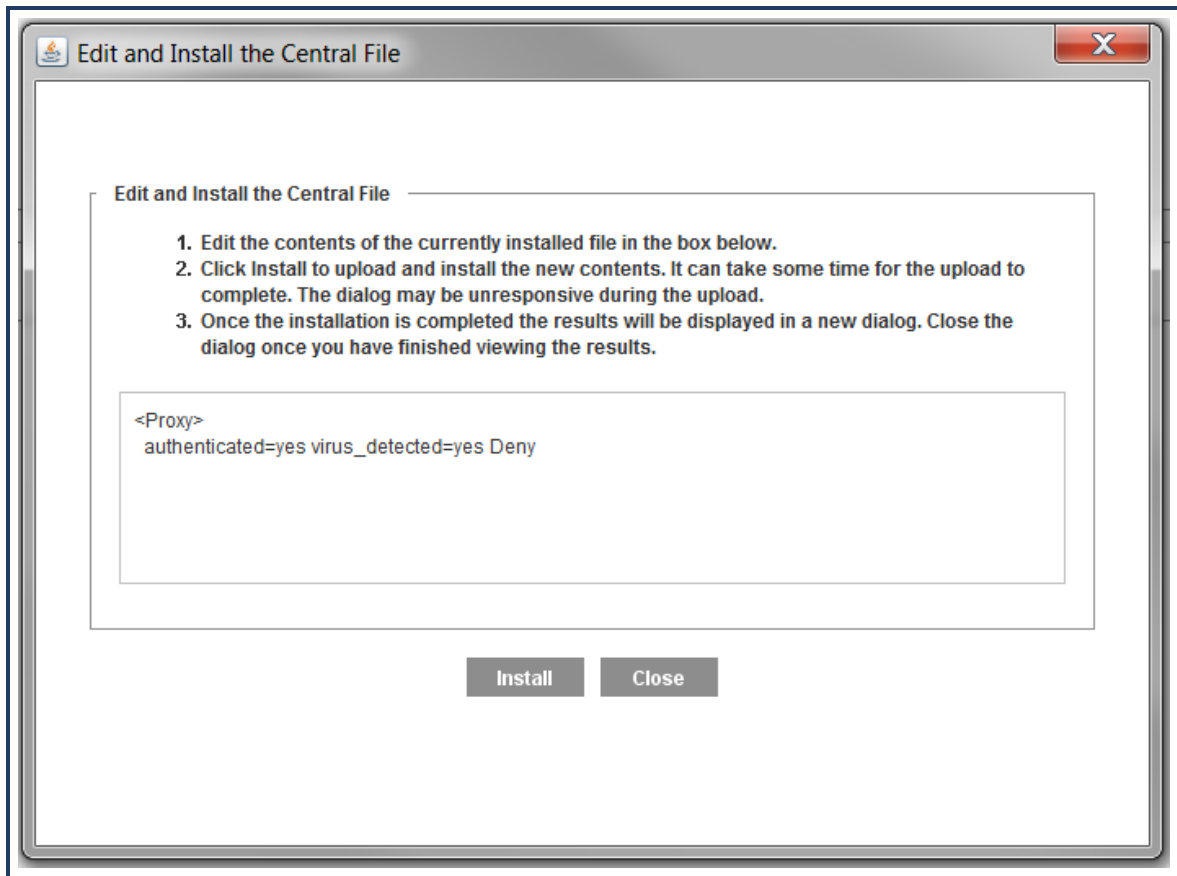
To load a Forward, Local, or a custom Central policy file, move it to an HTTP or FTP server, and then use that URL to download the file to the appliance.

- Installing a policy file using a Local File.

In the dialog that opens, browse to the file on the local system and open it. Click Install. When the installation is complete, the installation results display. You can view the results and close the window.



- Installing a policy file using the Text Editor.



The current configuration is displayed in installable list format. Define the policy rules using CPL in the Edit and Install File window that opens (refer to the Content Policy Language Reference); click Install. When the installation is complete, a results window opens. View the results, close the results window and click OK in the Edit and Install File window.

3. Click **Apply**.

There are other management-related tasks regarding the Central Policy File. See "Managing the Central Policy File" on page 14.

## Using the CLI Inline Command

To create policies using the CLI, you can use the inline policy command. This command either creates a new policy file or, if the specified file already exists, overwrites an existing policy file. You cannot edit an existing policy file using this command.

**Tip:** If you are not sure whether a policy file is already defined, check before using the inline policy command. For more information, see "Viewing Policy Source Files" on page 16.

## Symantec: A Division of Broadcom

Create policy files:

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

```
#(config) inline policy file eof-marker
```

where:

- *file* specifies the type of policy you want to define: Central (Central policy file), Forward (Forward policy file), or local (local policy file).

Do not use the inline policy command with files created using the module.

- *eof-marker* specifies the string that marks the end of the current inline command input; eof usually works as a string. The CLI buffers all input until you enter the marker string.

2. Define the policy rules using CPL (refer to the *Content Policy Language Reference*).
3. Enter each line and press **Enter**. To correct mistakes on the current line, use **Backspace**. If a mistake has been made in a line that has already been terminated by **Enter**, exit the inline policy command by pressing CTRL+C to prevent the file from being saved.
4. Type the eof-marker to save the policies and exit the inline mode.

For more information on the inline command, refer to the *Command Line Interface Reference*.

Load policy files:

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

```
#(config) policy {forward-path | local-path | central-path} url  
#(config) load policy {forward | local | central}
```

The appliance compiles and installs the new policy. A warning might occur if the new policy causes conflicts. If a syntax error is found, the appliance displays an error message. For information about these messages, refer to the *Content Policy Language Reference*. Correct the error, and then reload the file.

# Unloading Policy Files

To disable policies, perform the following procedure to unload the compiled policy file from memory. These steps describe how to replace a current policy file with an empty policy file.

To keep a current policy file, either make a backup copy or rename the file before unloading it. By renaming the file, you can later reload the original policy file. If you use multiple policy files, back up or rename files as necessary. Alternatively, rather than use an empty policy file, you can delete the entire contents of the file, then reload it.

To unload policies:

1. Select **Configuration > Policy > Policy Files > Policy Files**.
2. Select Text Editor in the **Install Local/Forward/Central File** from drop-down list and click the appropriate Install button. The Edit and Install the Local/Forward/Central Policy File appears.
3. Delete the text and click **Install**.
4. View the results in the results page that opens; close the page.
5. Click **Close**.

# Configuring Policy Options

This section describes policy options, which allow you re-order policy evaluation, change the default transaction setting, and enable policy tracing.

## Policy File Evaluation

The order in which the appliance evaluates policy rules is important. Changes to the evaluation order can result in different effective policy, as the order of policy evaluation defines general rules and exceptions.

On a new appliance, default evaluation order is Local, Central, and Forward. The default prevents policies in the Central file that block virus signatures from being inadvertently overridden by allow (access-granting) policy rules in the and Local files.

On an upgraded appliance, default evaluation order is the order on the appliance before the upgrade.

When changing the policy file evaluation order, remember that final decisions can differ because decisions from files later in the order can override decisions from earlier files.

To change policy order:

1. Select **Configuration > Policy > Policy Options**.

2. Select the file to move and click **Move Up** or **Move Down**. Remember that the last file in the list overwrites decisions in files evaluated earlier.

## Transaction Settings: Deny and Allow

The default proxy transaction policy is to either deny proxy transactions or to allow proxy transactions. A default proxy transaction policy of Deny prohibits proxy-type access to the appliance; you must then create policies to explicitly grant access on a case-by-case basis.

A default proxy transaction policy of Allow permits most proxy transactions. However, if protocol detection is enabled, the appliance allows HTTP CONNECT for both port 443 and other ports—provided the appliance detects a known protocol. If protocol detection is disabled, HTTP CONNECT is only allowed on port 443. If your policy is set to Allow, you must create policies to explicitly deny access on a case-by-case basis.

The default proxy policy does not apply to admin transactions. By default, admin transactions are denied unless you log in using console account credentials or if explicit policy is written to grant read-only or read-write privileges.

Also keep in mind that:

- Changing the default proxy transaction policy affects the basic environment in which the overall policy is evaluated. It is likely that you must revise policies to retain expected behavior after such a change.
- Changes to the evaluation order might result in different effective policy, because the order of policy evaluation defines general rules and exceptions.
- Changing the default proxy transaction policy does not affect the evaluation of cache and admin transactions.

To configure Deny or Allow default proxy policy:

1. Select **Configuration > Policy > Policy Options**.
2. Under Default Proxy Policy, select either **Deny** or **Allow**.
3. Click **Apply**.

## Policy Tracing

Tracing enabled with the Management Console or CLI is global; that is, it records every policy-related event in every layer. It should be used only while troubleshooting. For information on troubleshooting policy, refer to the *Content Policy Language Reference*. Turning on policy tracing of any kind is expensive in terms of system resource usage and slows down the appliance's ability to handle traffic.

To enable policy tracing:

1. Select **Configuration > Policy > Policy Options**.
2. Select **Trace all policy execution**.
3. Click **Apply**.

# Managing the Central Policy File

The Central policy file is updated when needed by Symantec. The file can be updated automatically or you can request e-mail notification. Alternatively, you can configure the path to point to your own custom Central policy file.

**Caution:** If you import policy that was created externally (for example, by a third-party tool) into a policy file, the ProxySG appliance validates the policy file's contents for syntax errors but cannot check for formatting or typographical mistakes. Such errors may result in unintended behavior after the policy is loaded. Symantec strongly recommends that you review the CPL in imported policy for correctness before installing the file.

## Configuring Automatic Installation

You can specify whether the appliance checks for a new version of the Central policy file. If a new version exists, the appliance can install it automatically.

Perform the following procedure to configure the appliance to check for and install a new version of the Central policy file.

To configure automatic installation:

1. Select **Configuration > Policy > Policy Files > Policy Files**.
2. Select **Automatically install new Policy when central file changes**.
3. Click **Apply**.

## Configuring a Custom Central Policy File for Automatic Installation

If you define your own Central policy file, you can configure the appliance to automatically install any subsequent updated version of the file. To use this capability, you must change the Central policy file's first line with each version update. With automatic installation, the appliance checks for a change to the first line of the file. In defining a custom Central policy file, add an item, such as a comment, to the first line of the Central policy file that changes with each update. The following is a sample first line, containing date information that is routinely updated with each version:

```
; Central policy file Month, Date, Year version
```

When you update and save the file in the original location, the appliance automatically loads the updated version.

## Configuring E-mail Notification

You can specify whether the appliance sends e-mail when the Central policy file changes. The e-mail address used is the same as that used in diagnostic reporting: the event recipient for the custom heartbeat e-mail.

To configure e-mail notification:

1. Select **Configuration > Policy > Policy Files > Policy Files**.
2. Select **Send me email when central file changes**.
3. Click **Apply**.

## Configuring the Update Interval

You can specify how frequently the appliance checks for a new version of the Central policy file. By default, the appliance checks for an updated Central policy file once every 24 hours (1440 minutes). You must use the CLI to configure the update interval. You cannot configure the update interval through the Management Console.

To configure the update interval, type the following command:

```
 #(config) policy poll-interval minute
```

## Checking for an Updated Central Policy File

You can manually check whether the Central policy file has changed. You must use the CLI. You cannot check for updates through the Management Console.

To check for an updated central file, enter the following command:

```
 #(config) policy poll-now
```

## Resetting the Policy Files

To clear all the policy files automatically, enter the following command:

```
 #(config) policy reset
WARNING: This will clear local, central, forward and VPM policy. Are you sure you want to reset ALL
policy files? (y or n)
```

The appliance displays a warning that you are resetting all of your policy files.

Type **y** to continue or **n** to cancel.

This command does not change the default proxy policy settings.

## Moving Policy Files from One Appliance to Another

Policy files are specific to the appliance where they were created. But just as you can use the same Central, Local, and Forward policy files on multiple appliances, you can use policies created on one appliance on other appliances.

For detailed information on moving policy files, see "Installing Policies" on page 155.

# Viewing Policy Files

You can view either the compiled policy or the source policy files. Use these procedures to view policies defined in a single policy file (for example, using the Visual Policy Manager) or in multiple policy files (for example, using the Central policy file and the VPM).

## Viewing the Installed Policy

Use the Management Console or a browser to display installed Central, Local, or Forward policy files.

To view installed policy files in the VPM:

1. Select **Configuration > Policy > Policy Files > Policy Files**.
2. In the View File drop-down list, select **Current Policy** to view the installed and running policy, as assembled from all policy source files. You can also select **Results of Policy Load** to view any warnings or errors resulting from the last attempt (successful or not) to install policy.
3. Click **View**. The appliance opens a separate browser window and displays the installed policy file.

To view the currently installed policy through a browser:

1. Enter a URL in one of the following formats:
  - If an HTTPS console is configured, use `https://IP_address:HTTPS-Console_port/Policy/current` (the default port is 8082).
  - If an HTTP console is configured, use `http://IP_address:HTTP-Console_port/Policy/current` (the default port is 8081).
2. The appliance opens a separate browser window and displays the policy.
3. Review the policy, then close the browser.

## Viewing Policy Source Files

To display source (uncompiled) policy files on the appliance:

1. Select **Configuration > Policy > Policy Files > Policy Files**.
2. To view a policy source file, select the file you want to view (Local, Forward, or Central) from the **View File** drop-down list and click **View**.
3. The appliance opens a separate browser window and displays the appropriate source policy file.

## Viewing Policy Statistics

To view policy statistics on all requests processed by the appliance:



1. Select **Statistics > Advanced**.
2. Click the **Policy** link.
3. Click the **Show policy statistics** link.
4. A separate browser window opens and displays the statistics.
5. Examine the statistics, then close the browser.
6. To review policy statistics through a browser:
7. Enter a URL in one of the following formats:
  - If an HTTPS-Console is configured, use `https://IP_address:HTTPS-Console_port/Policy/statistics` (the default port is 8082).
  - If an HTTP-Console is configured, use `http://IP_address:HTTP-Console_port/Policy/statistics` (the default port is 8081).
8. The appliance opens a separate browser window and displays the statistics. Examine the statistics and close the browser when you are done.

# Visual Policy Manager

The Visual Policy Manager (VPM) is a graphical policy editor included with the ProxySG appliance. The VPM allows you to define web access and resource control policies without having an in-depth knowledge of Symantec Content Policy Language (CPL) and without the need to manually edit policy files.

This chapter serves as a VPM object reference, and assumes that you are familiar with basic concepts of appliance policy functionality as described in "Managing Policy Files" on page 6.

While VPM creates only a subset of everything you can achieve by writing policies directly in CPL, it is sufficient for most purposes. If your needs require more advanced policies, consult the *Content Policy Language Reference*.

## Launch the VPM




1. Select the **Configuration > Policy > Visual Policy Manager** tab.
2. Click **Launch Web VPM**. The web VPM launches in a new browser tab.

Alternatively, click **Launch Legacy Java VPM**. The Java VPM launches in a separate window. Refer to the *Visual Policy Manager Reference* for details on using the legacy VPM.








# VPM Overview

The following table provides an overview of VPM operations and functions.

Area	Action	Instructions
Configuring settings for use in policy objects	Configure recipient lists for email notifications. See "E-mail" on page 138 for details on the <b>E-mail</b> track object.	Select <b>Configuration &gt; Email Lists</b> .
	Manage file extensions. See "File Extensions" on page 75 for details on the <b>File Extensions</b> destination object.	Select <b>Configuration &gt; File Extensions</b> .
	Restrict DNS lookups during policy evaluation.	Select <b>Configuration &gt; DNS Lookup Restrictions</b> .
	Restrict reverse DNS lookups during policy evaluation.	Select <b>Configuration &gt; Reverse DNS Lookup Restrictions</b> .
	Configure the order in which the group information is logged.	Select <b>Configuration &gt; Group Log Order</b> .
	Edit policy categories. See "Request URL Category" on page 77 for details.	Select <b>Configuration &gt; Categories</b> .
	Manage Subject Directory Attribute objects.	Select <b>Configuration &gt; Subject Directory Attributes</b> .
Locating specific policy items	Search for a text string in layer names and rule names.	See "Searching Policy" on page 156.
	View all condition definitions (define condition gestures).	Select <b>Operations &gt; View Generated CPL</b> . In the Generated CPL pane, look in the <b>Condition Definition</b> section.
	View all action definitions (define action gestures).	Select <b>Operations &gt; View Generated CPL</b> . In the Generated CPL pane, look in the <b>Action Definition</b> section.
Installing policy	Manage enforcement of policies.	See "Enforcement Domains" on page 26.
	Apply all changes to policy since the last save.	Click <b>Apply Policy</b> .
	Ignore all changes to policy since the last save and reload installed policy rules.	Select <b>Operations &gt; Revert to Existing Policy</b> .

Area	Action	Instructions
Configuring layers	Disable or enable the selected layer.	Click the toggle button.  Disabled layers are grayed out in the VPM.
	Rename a selected layer. Symantec recommends renaming layers to make for easy identification.	Go to the layer name and click to edit.
	Delete a layer if it is no longer needed in policy.	Go to  and click <b>Delete Layer</b> .
	Add a layer guard to specify a common condition to all rules within the layer.	Go to  and click <b>Add Layer Guard</b> .  Not applicable to the CPL layer, which is solely for composing CPL. Layer guards are written in the CPL itself. To compose CPL, click the down arrow to expand the field for text entry.  Not applicable to the Access Security and Content Security Policy layers.
	Duplicate the selected layer. Useful for layers that have similar configurations.	Go to  and click <b>Duplicate Layer</b> .  Not applicable to the CPL layer or the Default Security Policy layer.
	Change layer evaluation order.	Drag and drop layers to move them.
	Add policy layers.	Select <b>Add Layer</b> .
	View the rules within a layer.	Click the down arrow to expand the rule.  Not applicable to CPL layers, which are solely for composing CPL. Rules are written in the CPL itself. To compose CPL, click the down arrow to expand the field for text entry.

Area	Action	Instructions
Configuring objects	Determine which rules contain a specific policy object and how many times the object is used in policy.  Useful for removing or making changes to all instances of an object in policy.	Go to a rule that includes the object you are looking for. On the drop-down menu, select <b>View Occurrences</b> . The VPM displays a dialog that shows which layers and rules include the object.  Available for all policy objects except <b>Any</b> and <b>None</b> , and for all layers except the CPL layer and the Default Security Policy layer
	Displays a dialog that lists current static and user-defined VPM objects. See "View and Manage All Objects" on page 143.	Select <b>Operations &gt; View All Objects</b> .
Determining unsupported conditions	Displays a list of unsupported conditions that were removed from policy at load time.  Conditions might be removed for reasons such as: <ul style="list-style-type: none"> <li>■ Downgrade to a version that does not support the conditions</li> <li>■ VPM-XML file contains policy objects that are no longer supported</li> <li>■ Policy contains deprecated conditions</li> </ul>	Select <b>Operations &gt; Removed Conditions</b> .
Working with policy files	View generated CPL of installed VPM policy, including default security policy.	Select <b>Operations &gt; View Generated CPL</b> .

Area	Action	Instructions
Configuring rules	Add a blank rule to the end of the current policy layer.  See "Policy Rules " on page 25.	In the layer heading, select <b>Add rule</b> .
	Add a blank rule below the current policy layer.  See "Policy Rules " on page 25.	In the current rule, go to  and click <b>Insert Rule</b> .
	Duplicate the selected rule. Useful for rules that have similar configurations.	Go to  and click <b>Duplicate</b> .
	Delete a rule if it is no longer needed in policy.	Go to  and click <b>Delete</b> .
	Disable or enable the selected rule.	Click the toggle button.  Disabled rules are grayed out in the VPM.
	Copy and paste a rule.	Go to  and click <b>Copy</b> .  In another rule, go to  and click <b>Paste</b> . The rule is inserted below.
	Cut and paste a rule.	Go to  and click <b>Cut</b> .  In another rule, go to  and click <b>Paste</b> . The rule is inserted below.
	Include notes and clarifying information to a rule.	Click the comment icon to add a comment. If a rule has a comment, the icon is gray (filled in).  Comments do not affect operation of policy.
	Change rule evaluation order.	Drag and drop rules to move them.

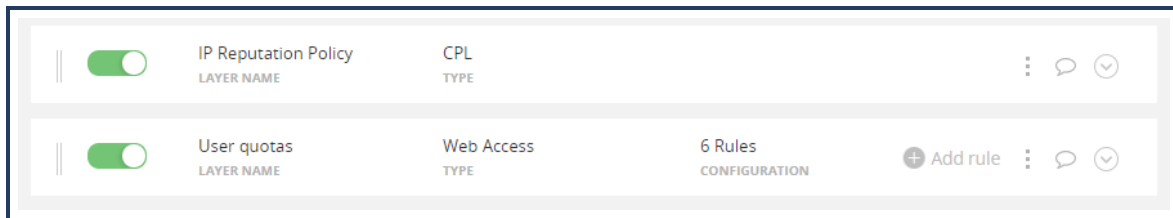
# Layers

Add policy layers:

1. Click **Add Layer**. The **Add a Layer** dialog displays the supported layer types. See "VPM Policy Layers" below for a list of supported layers.
2. To add a pre-defined security policy, under "Add A Pre-configured Policy", select **Access Policy** or **Content Policy**.

For details on security policy, refer to the following documentation:

- Access Security policy rules: <https://knowledge.broadcom.com/external/article/174668>
  - Content Security policy rules: <https://knowledge.broadcom.com/external/article/174669>
  - "Using Policy Services" chapter in the [SGOS Administration Guide](#)
  - [ProxySG Security Best Practices](#)
3. To create your own policy, under "Add A Policy Layer - Build your own policy", select a layer type. Enter a new layer name and then click **OK**. The VPM displays the layer name, layer type, and details about rules, as follows:



4. Refer to "VPM Overview" on page 19 for actions you can perform on layers.
5. When you are done with your changes, add policy rules (see "Policy Rules " on page 25). Otherwise, click **Apply Policy** to save current changes.

## VPM Policy Layers

You can add the following layers in the VPM:

VPM Layer	Policy Purpose	CPL Layer
Access Security Policy	Pre-configured policy that allows you to block or monitor transactions based on Symantec's URL Threat Risk Levels and URL categories.  For details on the Access Policy, refer to the <i>SGOS Administration Guide</i> and the <i>ProxySG Security Best Practices</i> document.	<Proxy>
Admin Access	Determines who can access the appliance to perform administration tasks.	<Admin>

## Symantec: A Division of Broadcom

VPM Layer	Policy Purpose	CPL Layer
Admin Authentication	Determines how administrators accessing ProxySG appliance must authenticate.	<Admin>
Admin Login Banner	Configure a notice and consent banner for the Management Console.	<Admin>
Content Security Policy	Pre-configured policy that allows you to scan traffic based on Symantec's current content scanning recommendations and set failover and security options for the ICAP service.  For details on the Access Policy, refer to the <i>SGOS Administration Guide</i> and the <i>ProxySG Security Best Practices</i> document.	<Proxy>, <Cache>
DNS Access	Determines how the appliance processes DNS requests.	<DNS>
Forwarding	Determine forwarding hosts and methods.	<Forward>
SOCKS Authentication	Determines the method of authentication for accessing the proxy through SOCKS.	<Proxy>
SSL Intercept	Determines whether to tunnel or intercept HTTPS traffic.	<SSL-Intercept>
SSL Access	Determines the allow/deny actions for HTTPS traffic.	<SSL>
Web Access	Determines what clients can and cannot access on the Web and specifies any restrictions that apply.	<Proxy>
Web Authentication	Determines whether user clients that access the proxy or the Web must authenticate.	<Proxy>
Web Content	Determines caching behavior, such as verification and Content Analysis redirection.	<Cache>
Web Request	Determine if a request is denied before reaching the OCS.	<Proxy>




# Policy Rules

Policy evaluates rules in a layer from top to bottom until there is a match. When the appliance evaluates a rule, it tests the conditions for the current transaction. If all of the conditions evaluate to true, the rule is said to match. When there is a match, all of the listed actions are executed (though later layers can potentially override the action) and evaluation of the current layer ends. If one or more of the conditions evaluate to false for that transaction, it is a miss, and policy evaluation continues to the next rule in the layer.

A policy layer (other than CPL layers) contains one or more rules. Each rule consists of at least one trigger and an action, such as a source condition and an **Allow** action.

To add a rule:

1. Click **Add rule**; the new rule is appended to the layer.

Alternatively, to add a rule below the current rule, go to  and click **Insert Rule**.

New layers automatically include one rule, with default settings such as **Any** (any source, destination, service, or time can match) and **None** (no action or tracking method is set). Some layers have other defaults, such as **Use Default Caching** in the Web Content Layer and **Deny** in the Web Access Layer.

2. Refer to "VPM Overview" on page 19 for actions you can perform on rules.
3. You can configure the source, destination, service, time, action, and track objects in a rule; see "Policy Layer and Rule Object Reference" on page 30. Otherwise, click **Apply Policy** to save current changes.

# Enforcement Domains

As part of your cloud migration strategy, Symantec recommends using enforcement domains in conjunction with Symantec Management Center to specify whether to enforce policy rules in Symantec Web Security Service, in any on-premises appliances, or both. If your deployment does not include Management Center, you can designate enforcement domains manually.

For instructions on deploying universal policy, refer to Universal Policy documentation:

<https://techdocs.broadcom.com/content/broadcom/techdocs.html>

To migrate policy to the cloud, or to facilitate managing policy in a mixed environment with the cloud and on-premises appliances, specify an enforcement domain for each applicable policy rule.

When you install VPM policy that includes enforcement domains, the generated CPL guards the appliance-specific rules and cloud-specific rules with the enforcement preprocessor variable; refer to “Conditional Compilation” in the *Content Policy Language Reference* for details.

The following layers support enforcement domains:

- DNS Access Layer
- SSL Intercept Layer
- SSL Access Layer
- Web Authentication Layer
- Web Access Layer
- Web Content Layer
- Web Request Layer

## Enable Enforcement Domains

You must enable enforcement domains before you can specify and change them in policy rules. Select **Operations > Enable Enforcement Domains**. This adds an Enforcement column to supported VPM layers. You can then specify the enforcement domain for rules within these layers.

## Determine Where Rules are Enforced

Rules display an Enforcement column if enforcement domains are enabled (**Operations > Enable Enforcement Domains**) and the layer supports the feature. The Enforcement column value is Appliance by default until you make changes, whereas rules that do not support domains do not display the column.

Enforcement Domain	Description
Appliance	The rule is enforced on the appliance. Possibly, the enforcement domain was never changed from the default setting. Generated CPL displays enforcement=appliance for consecutive appliance rules.
WSS	The rule is enforced in cloud policy. Generated CPL displays enforcement=wss for consecutive cloud rules.
Universal	The rule is enforced in both cloud and appliance policy. Generated CPL does not include the enforcement variable for the rules because they are not specific to cloud or on-premises appliances.

## Change Enforcement Domains

By default, a rule's enforcement domain is set to **Appliance**. Depending on your requirements, specify a different enforcement for a single rule or change the domain for multiple rules at once.

Specify the enforcement domain for one rule:

1. Launch the VPM and select a rule. Select a drop-down menu option in the **Enforcement** column.
2. Select the appropriate option:
  - **Appliance**: Enforce the rule in on-premises appliance policy. This is the default setting.
  - **Universal**: Enforce the rule in policy in both on-premises appliances and the cloud.
  - **WSS**: Enforce the rule in Symantec Web Security Service cloud policy.
3. Configure policy as required.
4. Click **Apply Policy**.

Specify the enforcement domain for multiple rules in one or more layers:

1. Select **Operations > Change Enforcement**. The VPM opens a Change Enforcement dialog.  
The dialog lists all the layers in your VPM policy that support enforcement domains.
2. (Optional) To display all policy layers, clear **Show only applicable layers**. By default, only the layers that support enforcement domains are listed.
3. Change enforcement domains:
  - Toggle the layer selection using the checkbox beside **Layer**, or select and clear individual layers as needed.
  - From the **Change enforcement to** menu, select the target domain (Appliance, Universal, or WSS).
4. Click **Apply Policy** to save your changes.

## Identify Enforcement Errors and Warnings

When you change a rule's enforcement, the rule displays any errors and warnings that might occur. Look for an icon as shown below:

		Web Content Layer (1)	Web Content	1 Rule	0	1
		LAYER NAME	TYPE	CONFIGURATION	ERROR(S)	WARNING(S)
		Destination	Action	Track	Enforcement	
1		Any	Use Default Ca...	None	Universal	

Warnings do not prevent policy installation; in this example, WSS simply will not execute the rule with the warning. To find out more about the warning, hover over the message:

		Web Content Layer (1)	Web Content	1 Rule	0	1
		LAYER NAME	TYPE	CONFIGURATION	ERROR(S)	WARNING(S)
		Destination	Action	Track	Enforcement	
1		Any	Use Default Ca...	None	Universal	

Caching resources are managed by WSS. This property will be transparent to WSS. No action is required.

Errors prevent policy installation. When policy includes errors, the **Apply Policy** button is inactive. To determine which layers/rules have errors, look for a policy object with an icon as shown below:

<div><div></div><div></div></div>		<div><div></div><div></div></div>	Web Access Layer (1)	Web Access	2 Rules	1	0		
			LAYER NAME	TYPE	CONFIGURATION	ERROR(S)	WARNING(S)		
			Source	Destination	Service	Time	Action	Track	Enforcement
1	<div><div></div><div></div></div>		Any	Any	Any	Any	<div><div></div><div></div></div> Disable Fast-C...	None	Universal

To find out more about the error, hover over the message:

<div><div></div><div></div></div> <div><div></div></div>		Web Access Layer (1)	Web Access	2 Rules		1	0
		LAYER NAME	TYPE	CONFIGURATION			
		Source	Destination	Service	Time	Appliance gestures are not supported on WSS	
1	<div><div></div><div></div></div> <div><div></div></div>	Any	Any	Any	Any	<div><div></div><div>Disable Fast-C...</div></div>	None
							Enforcement
							Universal

When you resolve the error—by excluding the layer from conversion, changing or removing the rule, or another appropriate method—the **Apply Policy** button becomes available again.

# About Code Sharing With the Management Console

The VPM shares information in various lists from the current configuration in the Management Console, not the saved ProxySG configurations. When the VPM is launched, it inherits the state of the appliance from the Management Console and remains synchronous with that Management Console. This state might include configuration changes that have not yet been applied or reverted. This does not include any changes made through the CLI. When you click Apply in the Management Console, the configurations are sent to the appliance; the Management Console and the VPM become synchronous with the appliance.

For example, the appliance has two ICAP response services installed, A and B. In the Management Console, you remove service B, but do not click Apply. You then start the VPM and view the ICAP Response Services object. Only service A is viewable and selectable.

The VPM synchronizes the latest change from the Management Console when you do any of the following:

- Revert policy to the last-saved version (**Operations > Revert to Existing Policy**).
- Click **Apply Policy**.
- Restart the Management Console.
- Log out of the Management Console and log in again.

Any information the Management Console acquires from installable lists is immediately available in the VPM. The following are the lists the VPM obtains from the Management Console:

- Access log fields
- Authentication character sets
- Authentication realms
- Bandwidth gain classes
- Content filtering categories
- Exceptions
- Forwarding hosts
- ICAP request and response services
- Keyrings
- SOCKS gateways

# Policy Layer and Rule Object Reference

Refer to the following list of policy layers and the objects available in them. See "VPM Overview" on page 19 for some actions you can perform on objects.

## Admin Access Layer: Source Objects

- "Combined Source Object" on page 53
- "Attribute" on page 54
- "Client Address Login Count" on page 54
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- "Client IP Address/Subnet" on page 55
- "Group" on page 57
- "LDAP Attribute" on page 59
- "Proxy IP Address/Port" on page 60
- "User" on page 61
- "User Login Address" on page 64
- "User Login Count" on page 65
- "User Login Time" on page 65

## Admin Access Layer: Service Objects

- "Service Group" on page 88
- "Service Name" on page 89

## Admin Access Layer: Action Objects

- "Combined Action Object" on page 97
- Allow Read-Only Access (see "Static Objects" in "Action Column Objects" on page 93)
- Allow Read/Write Access (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Force Deny (see "Static Objects" in "Action Column Objects" on page 93)

- Log Out/Do Not Log Out Other Users With Same IP (see "Static Objects" in "Action Column Objects" on page 93)
- Log Out/Do Not Log Out User (see "Static Objects" in "Action Column Objects" on page 93)
- Log Out/Do Not Log Out User's Other Sessions (see "Static Objects" in "Action Column Objects" on page 93)
- "Set Authorization Refresh Time" on page 115
- "Set Credential Refresh Time" on page 118
- "Set Surrogate Refresh Time" on page 122

## Admin Access Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

## Admin Authentication Layer: Source Objects

- "Combined Source Object" on page 53
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- "Client IP Address/Subnet" on page 55
- "Proxy IP Address/Port" on page 60

## Admin Authentication Layer: Action Objects

- "Authenticate" on page 98
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Authenticate (see "Static Objects" in "Action Column Objects" on page 93)
- "Force Authenticate" on page 103

## Admin Authentication Layer: Track Objects

- "Combined Track Object" on page 138
- Email (see "SNMP " on page 139)

- "Policy ID" on page 139
- "Trace " on page 139

## Admin Login Banner Layer: Source Objects

- "Combined Source Object" on page 53
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- "Client IP Address/Subnet" on page 55
- "Proxy IP Address/Port" on page 60

## Admin Login Banner Layer: Service Objects

A service name is required.

- "Service Name" on page 89

## Admin Login Banner Layer: Action Objects

An action is required.

- "Combined Action Object" on page 97
- "Authenticate" on page 98
- "Force Authenticate" on page 103

## Admin Login Banner Layer: Banner Objects

A banner attribute is required.

- "Banner Attribute" on page 136

## CPL Layer

See "Composing CPL Directly in the VPM" on page 173.

## DNS Access Layer: Source Objects

- "Combined Source Object" on page 53
- "Client Connection DSCP " on page 54
- "Client Geolocation" on page 54



- "Client IP Address/Subnet" on page 55
- "DNS Request Class" on page 57
- "DNS Request Name" on page 57
- "DNS Request Opcode" on page 57
- "DNS Request Type" on page 57
- "Proxy IP Address/Port" on page 60

## DNS Access Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Category" on page 74
- "DNS CNAME " on page 74
- DNS Threat Risk Level (see "Threat Risk Level" on page 81)
- "DNS Response Code" on page 74
- DNS Response Contains No Data (see "Static Objects" in "Destination Column Objects " on page 69)
- "DNS Response IP Address/Subnet" on page 74
- "RDNS Request IP Address & Subnet" on page 60
- "Destination Column Objects " on page 69
- "Resolved Country" on page 79
- "Server Connection DSCP" on page 80

## DNS Access Layer: Time Objects

- "Combined Time Object" on page 91
- "Time" on page 91

## DNS Access Layer: Action Objects

- "Combined Action Object" on page 97
- Allow DNS From Upstream Server (see "Static Objects" in "Action Column Objects" on page 93)
- Bypass DNS Cache (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Bypass DNS Cache (see "Static Objects" in "Action Column Objects" on page 93)

## Symantec: A Division of Broadcom

- Enable/Disable DNS Imputing (see "Static Objects" in "Action Column Objects" on page 93)
- "Manage Bandwidth" on page 104
- "Reflect IP" on page 110
- "Send DNS/RDNS Response Code" on page 114
- "Send DNS Response" on page 114
- "Send Reverse DNS Response" on page 114
- Serve DNS Only From Cache (see "Static Objects" in "Action Column Objects" on page 93)
- "Set Client Connection DSCP " on page 116
- Set Effective DNS Request Threat Risk Level (see "Set Effective Threat Risk Level" on page 118)
- "Set Server Connection DSCP " on page 121

## DNS Access Layer: Track Objects

- "Combined Track Object" on page 138
- SNMP (see "SNMP " on page 139)
- "Trace " on page 139

## Forwarding Layer: Source Objects

- "Combined Source Object" on page 53
- "Attribute" on page 54
- Authenticated User (see "Static Objects" in "Source Column Objects" on page 53)
- "Client Address Login Count" on page 54
- "Client Connection DSCP " on page 54
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client IP Address/Subnet" on page 55
- "Group" on page 57
- Guest User (see "Static Objects" in "Source Column Objects" on page 53)
- "LDAP Attribute" on page 59

- "P2P Client" on page 60
- "Proxy IP Address/Port" on page 60
- "SAML Attribute" on page 60
- "SOCKS Version" on page 61
- Streaming Client (see "Static Objects" in "Source Column Objects" on page 53)
- "User" on page 61
- "User Agent" on page 63
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64
- "User Login Address" on page 64
- "User Login Count" on page 65
- "User Login Time" on page 65

## SOCKS Authentication Layer: Source Objects

- "Combined Source Object" on page 53
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- "Client IP Address/Subnet" on page 55
- "Proxy IP Address/Port" on page 60
- "SOCKS Version" on page 61

## SOCKS Authentication Layer: Action Objects

- Do Not SOCKS Authenticate (see "Static Objects" in "Action Column Objects" on page 93)
- Force SOCKS Authenticate (see "Force Authenticate" on page 103)
- SOCKS Authenticate (see "Authenticate" on page 98)

## SOCKS Authentication Layer: Track Objects

- "Combined Track Object" on page 138
- Email (see "SNMP " on page 139)

- "Policy ID" on page 139
- "Trace " on page 139

## SSL Access Layer: Source Objects

- "Combined Source Object" on page 53
- "Attribute" on page 54
- Authenticated User (see "Static Objects" in "Source Column Objects" on page 53)
- "Client Certificate" on page 54
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client IP Address/Subnet" on page 55
- "Client Negotiated Cipher" on page 56
- "Client Negotiated Cipher Strength" on page 56
- "Client Negotiated SSL Version" on page 56
- "Group" on page 57
- Guest User (see "Static Objects" in "Source Column Objects" on page 53)
- "LDAP Attribute" on page 59
- "Proxy IP Address/Port" on page 60
- "SAML Attribute" on page 60
- "User" on page 61
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64
- "User Login Address" on page 64

## SSL Access Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Application Attributes" on page 69
- "Destination Column Objects " on page 69

- "Application Name" on page 72
- "Application Operation" on page 73
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "Request URL" on page 76
- "Request URL Category" on page 77
- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)
- "Resolved Country" on page 79
- "Server Certificate" on page 80
- "Server Certificate Category" on page 80
- Server Certificate Hostname Threat Risk Level (see "Threat Risk Level" on page 81)
- "Server Negotiated Cipher" on page 80
- "Server Negotiated Cipher Strength" on page 81
- "Server Negotiated SSL Version" on page 81
- "Server URL" on page 81

## SSL Access Layer: Service Objects

- "Combined Service Object" on page 87
- "Client Protocol" on page 87
- "Health Check" on page 88
- "SSL Proxy Mode" on page 89
- Request Forwarded (see "Service Column Objects " on page 87)

## SSL Access Layer: Action Objects

- "Combined Action Object" on page 97
- Allow (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (Content Filter) (see "Static Objects" in "Action Column Objects" on page 93)
- "Enable Encrypted Tap" on page 102

## Symantec: A Division of Broadcom

- Force Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Force Deny (Content Filter) (see "Static Objects" in "Action Column Objects" on page 93)
- Require/Do Not Require Client Certificate (see "Static Objects" in "Action Column Objects" on page 93)
- "Return Exception" on page 111
- "Set Client Certificate Validation" on page 115
- "Set Client Keyring" on page 117
- "Set Geolocation Restriction" on page 119
- "Set Server Certificate Validation" on page 120

## SSL Access Layer: Track Objects

- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139
- "Combined Track Object" on page 138

## SSL Intercept Layer: Source Objects

- "Combined Source Object" on page 53
- "Attribute" on page 54
- Authenticated User (see "Static Objects" in "Source Column Objects" on page 53)
- "Client Address Login Count" on page 54
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client IP Address/Subnet" on page 55
- "Group" on page 57
- Guest User (see "Static Objects" in "Source Column Objects" on page 53)
- "HTTP CONNECT User Agent" on page 59
- "LDAP Attribute" on page 59

- "Proxy IP Address/Port" on page 60
- "SAML Attribute" on page 60
- "Source Column Objects" on page 53
- "User" on page 61
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64
- "User Login Address" on page 64
- "User Login Count" on page 65
- "User Login Time" on page 65

## SSL Intercept Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Application Attributes" on page 69
- "Destination Column Objects " on page 69
- "Application Name" on page 72
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "Request URL" on page 76
- "Request URL Category" on page 77
- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)
- "Resolved Country" on page 79
- "Server Certificate" on page 80
- "Server Certificate Category" on page 80
- Server Certificate Hostname Threat Risk Level (see "Threat Risk Level" on page 81)
- "Server URL" on page 81

## SSL Intercept Layer: Service Objects

- Client Certificate Requested (see "Service Column Objects " on page 87)
- "Health Status" on page 88

## SSL Intercept Layer: Action Objects

- "Combined Action Object" on page 97
- Disable SSL Interception (see "Action Column Objects" on page 93)
- Do not Preserve Untrusted Issuer (see "Action Column Objects" on page 93)
- "Action Column Objects" on page 93
- Preserve Untrusted Issuer (see "Action Column Objects" on page 93)
- Set Effective Server Certificate Hostname Threat Risk Level (see "Set Effective Threat Risk Level" on page 118)
- Use Default Setting for Preserve Untrusted Issuer (see "Action Column Objects" on page 93)

## SSL Intercept Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

## Web Access Layer: Source Objects

- "Combined Source Object" on page 53
- "Apparent Data Type Source" on page 53
- "Attribute" on page 54
- Authenticated User (see "Static Objects" in "Source Column Objects" on page 53)
- "Client Address Login Count" on page 54
- "Client Certificate" on page 54
- "Client Connection DSCP " on page 54
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client IP Address/Subnet" on page 55
- "Group" on page 57
- Guest User (see "Static Objects" in "Source Column Objects" on page 53)



- "HTTP Request Body" on page 59
- "LDAP Attribute" on page 59
- "P2P Client" on page 60
- "Proxy IP Address/Port" on page 60
- "ICAP Reqmod Header" on page 59
- "Request Header" on page 60
- "SAML Attribute" on page 60
- "User" on page 61
- "User Agent" on page 63
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64
- "User Login Address" on page 64
- "User Login Count" on page 65
- "User Login Time" on page 65

## Web Access Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Apparent Data Type Destination" on page 69
- "Application Attributes" on page 69
- "Destination Column Objects " on page 69
- "Application Name" on page 72
- "Application Operation" on page 73
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "File Extensions" on page 75
- "HTTP MIME Types" on page 76
- "Request URL" on page 76
- "Request URL Category" on page 77

- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)
- "Respmod Header" on page 76
- "Response Code" on page 79
- "Response Header" on page 79
- "Server Certificate" on page 80
- "Server Connection DSCP" on page 80
- "WebEx Site" on page 83

## Web Access Layer: Service Objects

- "Combined Service Object" on page 87
- "Client Protocol" on page 87
- "Health Status" on page 88
- "ICAP REQMOD/RESPMOD Error Code" on page 88
- "Protocol Methods" on page 88
- "Service Group" on page 88
- "Service Name" on page 89
- "Streaming Content Type" on page 89
- Using HTTP Transparent Authentication (see "Service Column Objects " on page 87)
- Virus Detected (see "Service Column Objects " on page 87)

## Web Access Layer: Time Objects

- "Combined Time Object" on page 91
- "Time" on page 91

## Web Access Layer: Action Objects

- "Combined Action Object" on page 97
- Accept/Do Not Accept HTTP/2 Client-Side Connections (see "Static Objects" in "Action Column Objects" on page 93)
- "Add Attack Detection Failure Weight" on page 97
- Allow (see "Static Objects" in "Action Column Objects" on page 93)
- Always Verify (see "Static Objects" in "Action Column Objects" on page 93)

- Block/Do not Block Popup Ads (see "Static Objects" in "Action Column Objects" on page 93)
- Bypass/Do not Bypass Cache (see "Static Objects" in "Action Column Objects" on page 93)
- Check/Do not Check Authorization (see "Static Objects" in "Action Column Objects" on page 93)
- "Control Request/Response Header" on page 100
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (Content Filter) (see "Static Objects" in "Action Column Objects" on page 93)
- Disable Fast-Caching in Windows Media Client (see "Static Objects" in "Action Column Objects" on page 93)
- Disable/Enable ICAP Mirroring for response modification (see "Static Objects" in "Action Column Objects" on page 93)
- "Disable SSL Detection" on page 101
- "Enable Encrypted Tap" on page 102
- Force Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Force Deny (Content Filter) (see "Static Objects" in "Action Column Objects" on page 93)
- Force/Do Not Force IWA for Server Auth (see "Static Objects" in "Action Column Objects" on page 93)
- "Manage Bandwidth" on page 104
- "Modify Access Logging" on page 104
- "Notify User" on page 104
- "Action Column Objects" on page 93
- "Perform Request Analysis" on page 109
- "Reflect IP" on page 110
- "Action Column Objects" on page 93
- Require/Do Not Require Client Certificate (see "Static Objects" in "Action Column Objects" on page 93)
- "Return Exception" on page 111
- "Return ICAP Feedback" on page 111
- "Return Redirect" on page 112
- "Rewrite Host" on page 113
- "Set Apparent Data Type Action" on page 115
- "Set Authorization Refresh Time" on page 115
- "Set Client Certificate Validation" on page 115

## Symantec: A Division of Broadcom

- "Set Client Connection DSCP " on page 116
- "Set Client HTTP Compression" on page 116
- "Set Credential Refresh Time" on page 118
- "Set Effective Client IP" on page 118
- "Set Effective Threat Risk Level" on page 118
- "Set FTP Connection" on page 119
- "Set Geolocation Restriction" on page 119
- "Set HTTP Compression Level" on page 119
- "Set HTTP Request Max Body Size" on page 120
- "Action Column Objects" on page 93
- "Set SOCKS Acceleration " on page 122
- "Set SOCKS Compression" on page 122
- "Set Server Certificate Validation" on page 120
- "Set Server Connection DSCP " on page 121
- "Set Server HTTP Compression" on page 121
- "Set Server URL DNS Lookup" on page 121
- "Set Streaming Max Bitrate" on page 122
- "Set Surrogate Refresh Time" on page 122
- "Strip Active Content" on page 123
- Support/Do not Support Persistent Client Requests (see "Static Objects" in "Action Column Objects" on page 93)
- Support/Do not Support Persistent Server Requests (see "Static Objects" in "Action Column Objects" on page 93)
- "Suppress Headers" on page 123
- "Time Quota" on page 124
- Trust/Do Not Trust Destination IP (see "Static Objects" in "Action Column Objects" on page 93)
- Use Default Verification (see "Static Objects" in "Action Column Objects" on page 93)
- "Volume Quota" on page 124
- "Action Column Objects" on page 93

## Web Access Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

## Web Authentication Layer: Source Objects

- "Combined Source Object" on page 53
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- Client Hostname Unavailable (see "Static Objects" in "Source Column Objects" on page 53)
- "Client IP Address/Subnet" on page 55
- "Proxy IP Address/Port" on page 60
- "Request Header" on page 60
- "User Agent" on page 63
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64

## Web Authentication Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Application Group " on page 72
- "Application Name" on page 72
- "Application Operation" on page 73
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "Request URL" on page 76
- "Request URL Category" on page 77
- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)

## Web Authentication Layer: Action Objects

- "Combined Action Object" on page 97
- "Authenticate" on page 98
- "Authenticate Guest" on page 99
- "Authentication Charset" on page 100
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- "Deny" on page 101
- Do Not Authenticate (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Authenticate (Forward Credentials) (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Duplicate Proxy Credentials Upstream (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Use Kerberos Constrained Delegation (see "Static Objects" in "Action Column Objects" on page 93)
- "Duplicate Proxy Credentials Upstream" on page 101
- "Force Authenticate" on page 103
- "Kerberos Constrained Delegation" on page 103
- "Permit Authentication Error" on page 110
- "Permit Authorization Error" on page 110
- "Set IP Address For Authentication " on page 120

## Web Authentication Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

## Web Content Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Apparent Data Type Destination" on page 69
- "Application Group " on page 72
- "Application Name" on page 72

- "Application Operation" on page 73
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "File Extensions" on page 75
- "Flash Application Name" on page 75
- "Flash Stream Name" on page 75
- "HTTP MIME Types" on page 76
- "Request URL" on page 76
- "Request URL Category" on page 77
- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)
- "Resolved Country" on page 79
- "Response Data" on page 79
- "Response Header" on page 79
- "Server Connection DSCP" on page 80

## Web Content Layer: Action Objects

- "Combined Action Object" on page 97
- Always Verify (see "Static Objects" in "Action Column Objects" on page 93)
- Check/Do Not Check Authorization (see "Static Objects" in "Action Column Objects" on page 93)
- Do Not Cache (see "Static Objects" in "Action Column Objects" on page 93)
- "Dynamic Categorization" on page 101
- Enable/Disable Pipelining (see "Static Objects" in "Action Column Objects" on page 93)
- "Manage Bandwidth" on page 104
- Mark/Do Not Mark as Advertisement (see "Static Objects" in "Action Column Objects" on page 93)
- "Modify Access Logging" on page 104
- "Action Column Objects" on page 93
- "Perform Request Analysis" on page 109
- "Perform Response Analysis " on page 109

## Symantec: A Division of Broadcom

- "Set Client HTTP Compression" on page 116
- "Set Force Cache Reasons" on page 119
- "Set Geolocation Restriction" on page 119
- "Set HTTP Compression Level" on page 119
- "Set Content Security Scanning" on page 117
- "Server Connection DSCP" on page 80
- "Set Server HTTP Compression" on page 121
- "Set TTL" on page 122
- Support/Do not Support Persistent Server Requests (see "Static Objects" in "Action Column Objects" on page 93)
- Use Default Caching (see "Static Objects" in "Action Column Objects" on page 93)
- Use Default Verification (see "Static Objects" in "Action Column Objects" on page 93)

## Web Content Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

## Web Request Layer: Source Objects

- "Combined Source Object" on page 53
- "Apparent Data Type Source" on page 53
- "Attribute" on page 54
- "Client Address Login Count" on page 54
- "Client Certificate" on page 54
- "Client Connection DSCP " on page 54
- "Client Geolocation" on page 54
- "Client Hostname" on page 55
- "Client IP Address/Subnet" on page 55
- "Client Negotiated Cipher Strength" on page 56



- "Group" on page 57
- "HTTP Request Body" on page 59
- "LDAP Attribute" on page 59
- "P2P Client" on page 60
- "Proxy IP Address/Port" on page 60
- "Request Header" on page 60
- "SOCKS Version" on page 61
- "User" on page 61
- "User Agent" on page 63
- "User Authentication Error" on page 63
- "User Authorization Error" on page 64
- "User Login Address" on page 64
- "User Login Count" on page 65
- "User Login Time" on page 65

## Web Request Layer: Destination Objects

- "Combined Destination Object" on page 69
- "Destination Column Objects " on page 69
- "Application Name" on page 72
- "Application Operation" on page 73
- "Destination Host/Port" on page 74
- "Destination IP Address/Subnet" on page 74
- "File Extensions" on page 75
- "Request URL" on page 76
- "Request URL Category" on page 77
- Request URL Threat Risk Level (see "Threat Risk Level" on page 81)
- "Server Certificate" on page 80
- "Server Connection DSCP" on page 80

## Web Request Layer: Service Objects

- "Combined Service Object" on page 87
- "Client Protocol" on page 87
- "Health Status" on page 88
- "Protocol Methods" on page 88
- "Service Group" on page 88
- "Service Name" on page 89

## Web Request Layer: Time Objects

- "Combined Time Object" on page 91
- "Time" on page 91

## Web Request Layer: Action Objects

- "Combined Action Object" on page 97
- Allow Access to Server (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (see "Static Objects" in "Action Column Objects" on page 93)
- Deny (Content Filter) (see "Static Objects" in "Action Column Objects" on page 93)
- "Disable SSL Detection" on page 101
- "Manage Bandwidth" on page 104
- "Modify Access Logging" on page 104
- "Action Column Objects" on page 93
- "Perform Request Analysis" on page 109
- "Reflect IP" on page 110
- "Return Redirect" on page 112
- "Rewrite Host" on page 113
- "Set Apparent Data Type Action" on page 115
- "Set Client Connection DSCP " on page 116
- "Set Effective Threat Risk Level" on page 118
- "Set FTP Connection" on page 119

- "Set Geolocation Restriction" on page 119
- "Set HTTP Request Max Body Size" on page 120
- "Set SOCKS Acceleration " on page 122
- "Set Server HTTP Compression" on page 121
- "Set Server URL DNS Lookup" on page 121
- "Set Streaming Max Bitrate" on page 122
- "Suppress Headers" on page 123
- "Action Column Objects" on page 93

## Web Request Layer: Track Objects

- "Combined Track Object" on page 138
- "SNMP " on page 139
- "Policy ID" on page 139
- "Trace " on page 139

# VPM Object Reference

This section contains the following topics:

- "Source Column Objects" on the facing page describes objects for policy layers that support the **Source** column.
- "Destination Column Objects " on page 69 describes objects supported in the **Destination** column.
- "Service Column Objects " on page 87 describes the policy objects available in the **Service** column.
- "Time Column Objects" on page 91 describes the policy objects available in the **Time** column.
- "Action Column Objects" on page 93 describes the policy objects available in the **Action** column.
- "Track Object " on page 138 describes the available objects in the **Track** column.
- "Combined Objects " on page 142 describes how to use combined policy objects.
- "Creating Categories" on page 145 describes how to create policy-based categories.

# Source Column Objects

A source object specifies the communication or Web transaction origin that is evaluated by the policy. Not all policy layers contain the same source objects; see the "Source Column/Policy Layer Matrix" on page 66 for details.

**Note:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define object names.

## Static Objects

Static VPM objects are listed by default on the **Set *object type* Object** dialog; you do not have to click **Add a new object** to display them. To add a static object, select it in the list and click **Set**. There is no further need to configure the object after it is added to a policy rule.

The following static objects are available:

- **Authenticated User:** This rule applies to any authenticated user.
- **Client Hostname Unavailable:** This rule applies if the client IP address could not be looked up with a reverse DNS query.
- **Guest User:** This rule applies to all guest users.
- **Streaming Client:** This rule applies to any request from a streaming client.

## Combined Source Object

An object that combines different source types. See "Combined Objects " on page 142.

**Note:** Symantec strongly recommends that combined objects with large lists of Client IP Address/Subnet values (see "Client IP Address/Subnet" on page 55) do not contain other source objects. If other source objects are present, the policy evaluation might experience a significant performance degradation.

## Apparent Data Type Source

This condition uses the first few bytes of files being transmitted to identify the Apparent Data Type of that content. When used in a deny policy, the purpose of this object is to prevent users from uploading files of the defined type.

In addition to the preceding list, this object can also be configured to leverage the internal Content Analysis service (on Advanced Secure Gateway appliances) or an external Content Analysis or ProxyAV appliance to examine the contents of

archive files, (such as .zip and .rar files). An ICAP service object (either through Malware Scanning or policy-based) must already exist for this option to function. Select the **Enable ICAP Scanning** to enable this functionality.

**Note:** Multi-part and form data cannot be identified with this policy. For that option, see "Set Apparent Data Type Action" on page 115.

## Attribute

Specify a RADIUS attribute:

1. Select **All RADIUS** or a specific realm.
2. Select an **Attribute Name**.
3. Enter an attribute value.

## Client Address Login Count

This condition matches and can limit the number of different users who are logged into the current IP address.

## Client Certificate

Allows for testing common name and subject fields in client certificates.

## Client Connection DSCP

Tests the inbound differentiated service code point (DSCP) value of primary client-to-proxy connections. After testing DSCP bits (in the IP header), additional policy dictates how to handle traffic associated with the type of service.

Specify DSCP values to test against inbound client connections:

- Under **DSCP Value Range**, set a range of values. The valid range is 0 to 63. Most applications fit into one of the defined values.
- (Recommended) Under **Select DSCP Names**, select specific names.

For conceptual information about configuring the ProxySG appliance to manipulate traffic based on type of service, see "Managing QoS and Differentiated Services" on page 200.

## Client Geolocation

Specifies conditions based on country. To have a full list of countries, you require a valid geolocation subscription and a valid geolocation license must be installed on the appliance.

The Locations list in the top left shows items that would be available without a license.

To find specific countries in the list, enter a search string in the **Filter** field or scroll through the list.

To add a country to your selected locations, do one of the following:

- In the Locations list, select the country's name.
- In the Locations list, select the check box beside its name.

The country appears in the Selected Locations list.

To remove a country from your selected locations:

1. Select the country in the 'Selected locations' list, right click, and select **Remove**.

To remove multiple countries, select them while holding the CTRL or SHIFT key. Then, right click and select **Remove**.

2. In the list of countries on the left, clear the check box beside the country's name.
3. In the 'Selected locations' list, select a country and press the DELETE key.

### What does the effective client IP selection do?

Policy can match an IP address to the effective client IP address.

- If you select Look up effective client IP (if configured), the appliance will match the IP address to the effective client IP address when the Effective Client IP object is configured and valid. Subsequent requests to the same IP address will use the effective IP address that was matched.
- If you select Look up effective client IP (if configured) and the effective client IP object is not configured or it extracts an invalid address, policy will use the client IP address.

## Client Hostname

Specifies a reverse DNS hostname resolved in the reverse lookup of a client IP address. Enter the host name and select matching criteria. This object is automatically named using the prefix Client, such as Client: host.com. If you select a matching qualifier, that attribute is appended to the object in parentheses, such as host.com (RegEx).

## Client IP Address/Subnet

Specifies the client IPv4 or IPv6 address, an IPv4 address with one or more wildcards, or a range of IP addresses in a network; an optional subnet mask (for IPv4) or prefix length (for IPv6); and an option to match the IP address to the effective client IP address if the effective client IP object is configured. If you select **Look up effective client IP (if configured)** and the object is not configured, policy will ignore your selection.

Policy defined in this rule applies only to this address or addresses on this subnet. This object is automatically named using the prefix Client, for example, Client: 1.2.0.0/255.255.0.0.

**Note:** When traffic is explicitly proxied, it arrives at the Administration layer (Administration Authentication Policy Layer and Administration Access Policy Layer) with the client IP address set to the ProxySG appliance's IP address; therefore, the Client IP Address/Subnet object is not useful for explicitly proxied traffic.

- For information on using an IP address range, refer to article:

<https://knowledge.broadcom.com/external/article/16627>

- For information on using wildcards, refer to article:

<https://knowledge.broadcom.com/external/article/165925>

- To configure the effective client IP address, set the **Effective Client IP** action object (in the **Action** column, right click and select **Set > New**). For information on the effective client IP address, refer to "Set Effective Client IP" on page 118 and the *Content Policy Language Reference*.

**Note:** See "Combined Source Object" on page 53 for related information regarding this source object.

## Client Negotiated Cipher

Allows the testing of the SSL cipher in use between the ProxySG appliance and the browser. Select one or more cipher suites valid for this rule.

**Note:** Refer to the list of supported cipher suites:

<https://knowledge.broadcom.com/external/article/170130>

## Client Negotiated Cipher Strength

Tests the cipher strength between a ProxySG-to-browser (client) HTTPS connection. Select one or more of the strength options valid for this rule: Export, High, Medium, or Low.

**Note:** Low, Medium, and High strength ciphers are not exportable.

## Client Negotiated SSL Version

Tests the SSL version between a proxy-to-browser (client) HTTPS connection. Select one or more of the version options valid for this rule: TLSv1.3, TLSv1.2, TLSv1.1, TLSv1, SSLv3.



## DNS Client Transport

Specifies the DNS client transport method: UDP or TCP.

## DNS Request Class

Specifies the DNS request class (QCLASS) properties.

## DNS Request Name

Specifies a DNS request. Enter the host name and select matching criteria. If you select a matching qualifier, that attribute is appended to the object name in parentheses, such as DNS: host.com (RegEx).

## DNS Request Opcode

Specifies one or more OPCODEs to represent in the DNS header.

## DNS Request Type

Specifies one or more DNS request types (QTYPE).

## Group

Specifies a verifiable group name. Enter a user group and an authentication realm. The dialog displays different information depending on the type of authentication realm specified.

- **Group** field—Replace the default with a verifiable group name.
- **Authentication Realm** field—Select the appropriate realm from the drop-down list. Items in the list are taken from the realms configured by the administrator on the appliance.
  - **LDAP**—Entries in the Group Base DN list come from those specified by the administrator on the appliance. You can also edit an entry selected in the list, or type a new one. Edited names and new names are retained in the list. Notice in the Full Name field that the VPM takes the User Attribute type specified by the administrator on the appliance (cn= in the following illustration), and conjoins it with the group name and Base DN entered here.

**Note:** When you create a group, the default attribute is cn= in the Full Name display field.

If the primary user attribute specified on the appliance differs from the primary user attribute specified in the directory server, you need to enter the latter here. Do that by typing it in the Group field with the appropriate value (in the format attribute=value). Doing so replaces the entry in the Full Name field. Unlike the comparable situation when creating a user (described immediately above), when creating a group, the Group Base DN does not need to be selected to enter the attribute=value pair in the Group field.

- **IWA**—Entries in this list are not prepopulated. You must enter a name in the Domain Name field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that the VPM displays the domain name and group name entered above.
- **Windows SSO**—Entries in this list are not prepopulated. You must enter a name in the Group field.
- **Novell SSO**—Entries in this list are not prepopulated. You must enter a name in the Group field.
- **RADIUS**—Entries in this list are not prepopulated. You must enter a name in the Group field.
- **Local**—Entries in this list are not prepopulated. You must enter a name in the Group field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the group name entered above.
- **Certificate**—If a Certificate realm is selected and that realm uses an LDAP realm as authentication realm, the Browse button is clickable. This option allows you to browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields. If the Certificate realm does not use an LDAP authentication realm, Browse is not displayed.
- **CA eTrust SiteMinder**—Entries in this list are not prepopulated. You must enter a name in the Group field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the group name entered above.
- **Oracle COREid**—Entries in this list are not prepopulated. You must enter a name in the Group field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the group name entered above.
- **SAML**—Entries in this list are not prepopulated. You must enter a name in the Group field.
- **XML**—Entries in this list are not prepopulated. You must enter a name in the Group field.
- **Policy Substitution**—Entries in this list are not prepopulated. You must enter a name in the Group field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the group name entered above.

- **Sequences**—Entries in this list are not prepopulated. You must enter a name in the Group field. An entered name is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays domain name and user name entered above. From the Member Realm drop-down list, select an authentication realm (already configured on the appliance). Depending on the realm type, new fields appear.

## HTTP CONNECT User Agent

Tests which user agent is used to initiate an explicit proxy HTTP CONNECT request. This object applies to explicitly proxied transactions.

Enter a text string and select one of the following:

- **Exact Match** - The User-Agent header matches the string exactly.
- **Contains** - The User-Agent header contains the string.
- **At Beginning** - The User-Agent header starts with the string
- **At End** - The User-Agent header ends with the string.

Alternatively, enter a regular expression and select RegEx.

## HTTP Request Body

Allows you to create a policy condition to inspect the first 65536 bytes of the body of an HTTP request object and match a specific substring, prefix, suffix, or other content:

1. From the **Request Body Match Type** menu, select the type of match to perform.
2. In the **Request Body Content** field, enter the pattern to match.
3. In the **Length of the Request Body to inspect (up to 65536 bytes)** field, specify how many object bytes are scanned for the match.

## ICAP Reqmod Header

Allows you to create a condition that inspects ICAP REQMOD response headers and perform a regular expression match:

1. From the **Header Name** menu, specify the name of the header to inspect. Before you add a header name, the menu is empty. Any header names you add are saved in the list so you can select them in the future.
2. In the **Header Regex** field, enter the pattern to match.

## LDAP Attribute

Specifies an LDAP attribute (and optional value).

1. From the **Authentication Realm** drop-down list, select All LDAP or a specific realm.
2. In the **Attribute Name** field, enter a valid LDAP attribute.

3. Perform one of the following:

- Select the **Attribute exists** option to set the policy match when the attribute name exists.
- Select **Attribute value match**, enter a value, and select a type of match.

## P2P Client

Specifies peer-to-peer (P2P) clients. Select **All P2P Clients** or one or more P2P protocols.

## Proxy IP Address/Port

Specifies the IPv4 or IPv6 address and, optionally, a port on the appliance. The policy defined in this rule applies only to this address or addresses with this subnet.

## RDNS Request IP Address & Subnet

Specifies the reverse DNS IPv4 address or range of addresses, IPv4 address with wildcards, or IPv6 address and, optionally, a subnet mask (for IPv4) or prefix length (for IPv6).

- For information on using an IP address range, refer to article:

<https://knowledge.broadcom.com/external/article/16627>

- For information on using wildcards, refer to article:

<https://knowledge.broadcom.com/external/article/165925>

The policy defined in this rule applies only to this address or addresses on this subnet. This object is automatically named using the prefix RDNS, such as RDNS: 5.6.0.0/255.255.0.0.

## Request Header

Specifies the rule applies to requests containing a specific header. The ProxySG appliance supplies a list of standard headers, but you can also select a custom header:

1. From the **Show** list, select **Standard** to displays only the default standard headers or **Custom** to display any admin-defined headers.
2. From the **Header Name** list, select a standard or custom header. Alternatively, enter a new custom header name.
3. In the **Header Regex** field, enter the header values to which this rule applies.

## SAML Attribute

The appliance processes SAML authentication responses from the SAML identity provider (IDP); these responses may contain assertion attributes that describe a SAML-authenticated user. For example, <saml:Attribute Name="mail"> is an assertion attribute that contains the user's email address inside the <saml:AttributeValue> element.

You can configure the appliance to use assertion attributes in authorization decisions. The SAML Attribute object allows you to forward SAML assertion attributes via custom headers to back-end or front-end servers.

For information on SAML realm configuration, refer to the “SAML Authentication” chapter in the *SGOS Administration Guide*.

Specify a SAML attribute:

1. Select **SAML Attribute** from the list of objects.
2. In the **Name** field, enter a name for the object or leave as is to accept the default.
3. From the **Authentication Realm** drop-down list, select <All> or a specific realm.
4. In the **Attribute Name** field, enter a valid SAML attribute.
5. Do one of the following:
  - Select the **Attribute Exists** option to set the policy match when the attribute name exists.
  - In the **Attribute Value Match > Value** field, enter a value for the specified SAML attribute or leave it empty to accept any value.

## SOCKS Version

Specifies the SOCKS version: 4 or 5.

## User

Specifies an individual user in the form of a verifiable username or login name. When you enter a user name and select an authentication realm from the list, the dialog displays information depending on the type of authentication realm specified. You can only choose authentication realms that the ProxySG administrator configured.

### IWA

Entries in this list are not prepopulated. You must enter a name in the Domain Name field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays domain name and user name entered above.

### Windows SSO

Entries in this list are not prepopulated. You must enter a name in the User field. Entries in the Domain Name list come from those specified by the administrator on the appliance. You can also edit an entry selected in the list, type a new one, or click Browse to manually select a name.

### LDAP

You can optionally select a User Base DN from a drop-down list. Entries in the User Base DN list come from those specified by the administrator on the appliance. You can also edit an entry selected in the list, type a new one, or click Browse to manually select a name. Edited names and new names are retained in the list. The Full Name field takes the User Attribute type specified by the administrator on the appliance (cn= in the following illustration), and associates it with the user name and Base DN specified.

**Note:** When you configure a realm, the appliance assumes a default primary user attribute (SAMAccountName for Active Directory; uid for Netscape/iPlanet Directory Server/SunOne; cn for Novell NDS). You can accept the default or change it. Whatever is entered there is what the VPM uses here, entering it in the Full Name display field after a Base DN is selected.

If the primary user attribute specified on the appliance differs from the primary user attribute specified in the directory server, enter the latter in the User field with the appropriate value (in the format attribute=value). This replaces the entry in the Full Name field.

## Novell SSO

Entries in this list are not prepopulated. You must enter a name in the User field. If a Novell SSO realm uses an LDAP realm for authorization, you can select a User Base DN. You can also browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields.

## RADIUS

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays domain name and user name specified.

## Local

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the domain name and user name specified.

## Certificate

If a Certificate realm uses an LDAP realm for authorization, you can select a User Base DN. You can also browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields. If the Certificate realm does not use an LDAP authentication realm, Browse is not displayed.

## CA eTrust SiteMinder

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays the domain name and user name specified.

## Oracle COREid

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays the domain name and user name specified.

## SAML

If a SAML realm uses an LDAP realm for authorization, you can select a User Base DN. You can also browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields. The Full Name field displays domain name and user name specified.

## XML

If an XML realm uses an LDAP realm for authorization, you can select a User Base DN. You can also browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields.

## Policy Substitution

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays domain name and user name specified.

## Sequences

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. The Full Name field displays domain name and user name specified. From the Member Realm drop-down list, select an authentication realm (already configured on the appliance). Depending on the realm type, new fields appear.

## User Agent

Specifies one or more agents a client might use to request content. The choices include specific versions of: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Netscape Communicator, Microsoft Windows Media Player and NetShow, Real Media RealPlayer and RealDownload, Apple QuickTime, Opera, and Wget as well as mobile devices including iPhone, iPad, iPod, Blackberry, Android, and Windows Mobile.

The policy defined in this rule applies to these selected agents. You can name this list and create other custom lists to use with other policy layer rules.

**Note:** If you require a user agent not contained in this list, use the "Request Header" on page 60 object, which can include a user agent specified as a header.

## User Authentication Error

Checks for a matches of specified user authentication errors:

1. Select one of the following:
  - **No errors:** Authentication was attempted and no user errors occurred.
  - **Any errors:** Authentication was attempted a user error occurred.
  - **Selected errors:** Authentication was attempted and one of the selected errors occurred; selecting this enables the Show drop-down list and selectable errors area.

2. If you selected **Selected errors**:

- Refine the error view from the **Show** drop-down list.
- Select one or more error types; select the groups to expand the lists. If you select a group-level error, all of the errors in that group are also selected by default.

**Note:** If authentication fails and no default groups are added through policy, the group conditions always evaluate to false. Verify group conditions if you permit authentication errors, especially in scenarios where users are denied based on group membership.

## User Authorization Error

Checks for a match of specified user authorization errors.

1. Select one of the following:

- **None:** Authorization was attempted and no user errors occurred.
- **Any:** Authorization was attempted a user error occurred.
- **Selected errors:** Authorization was attempted and one of the selected errors occurred.

2. If you selected **Selected errors**:

- a. Select one or more error types.
- b. Click **Add** to move the errors to the Selected field.

**Note:** If authorization fails and no default groups are added through policy, the group conditions always evaluate to false. Verify group conditions if you permit authorization errors, especially in scenarios where users are denied based on group membership.

## User Login Address

The condition matches the IPv4 or IPv6 address used to log in and serves as a request parameter for Windows Single Sign-On (SSO). You can also specify an IPv4 address range or IPv4 address with wildcards.

- For information on using an IP address range, refer to article:

<https://knowledge.broadcom.com/external/article/16627>

- For information on using wildcards, refer to article:

<https://knowledge.broadcom.com/external/article/165925>



## User Login Count

This condition matches the number of times that a specific user is logged in with the current realm.

## User Login Time

This condition matches the number of seconds since the current login started, and can limit the length of a login session.

# Source Column/Policy Layer Matrix

**Source** column objects are available in the following policy layers:

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Apparent Data Type									X		X	
Attribute		X					X		X		X	X
Authenticated User						X	X		X		X	X
Client Address Login Count		X					X		X		X	X
Client Certificate							X		X		X	
Client Connection DSCP Trigger				X					X		X	X
Client Geolocation	X	X	X	X	X	X	X	X	X		X	X
Client Hostname	X	X	X		X	X	X	X	X		X	X
Client Hostname Unavailable						X	X	X	X		X	
Client IP Address/Subnet				X		X	X	X	X		X	
Client Negotiated Cipher							X		X			

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Client Negotiated Cipher Strength							X		X		X	
Client Negotiated SSL Version							X					
Combined Source Object	X	X	X	X	X	X	X	X	X	X	X	X
DNS Client Transport				X								
DNS Request Class				X								
DNS Request Opcode				X								
DNS Request Type				X								
Group		X					X		X		X	X
Guest User							X		X		X	
HTTP Request Body									X		X	
ICAP Reqmod Header									X	X		
LDAP Attribute		X					X		X		X	X
DNS Request Name				X								
P2P Client									X		X	X

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Proxy IP Address/Port	X	X	X	X	X	X	X		X		X	X
RDNS Request IP Address/Subnet				X								
Request Header									X		X	X
SOCKS Version					X				X		X	X
Streaming Client									X		X	
User		X					X		X		X	X
User Agent								X	X		X	
User Authentication Error							X		X		X	X
User Authorization Error							X		X		X	X
User Login Address							X		X		X	X
User Login Count							X		X		X	X
User Login Time							X		X		X	X

# Destination Column Objects

A destination object specifies the communication or Web traffic destination that is evaluated by the policy. Not all policy layers contain the same Destination objects; see the "Destination Column/Policy Layer Matrix" on page 84 for details.

**Note:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define object names.

## Static Objects

Static VPM objects are listed by default on the **Set *object type* Object** dialog; you do not have to click **Add a new object** to display them. To add a static object, select it in the list and click **Set**. There is no further need to configure the object after it is added to a policy rule.

The following static objects are available:

- **DNS Response Contains No Data:** Rule applies when the DNS response does not contain any data.

## Combined Destination Object

An object that combines different destination types. See "Combined Objects " on page 142.

## Apparent Data Type Destination

This condition uses the first few bytes of files being transmitted to identify the Apparent Data Type of that content. When used in a deny policy, the purpose of this object is to prevent users from uploading files of the defined type.

In addition to the preceding list, this object can also be configured to leverage the internal Content Analysis service (on Advanced Secure Gateway appliances) or an external Content Analysis or ProxyAV appliance to examine the contents of archive files, (such as .zip and .rar files). An ICAP service object (either through Malware Scanning or policy-based) must already exist for this option to function. Check the **Enable ICAP Scanning** check box to enable this functionality.

**Note:** Multi-part and form data cannot be identified with this command. For that option, see [Set Apparent Data Type Action](#).

## Application Attributes

Specifies application attributes, which provide insight into a web application and its governance, risk management, and compliance.

**Tip:** To use this policy object, you must:

- Have a valid Application Classification subscription (included in an Intelligence Services bundle) that includes the CASB AppFeed attributes
- Enable the Application Classification and Application Attributes services

**Note:** When writing policy rules based on Business Readiness Rating (BRR), note that the CASB AppFeed applies its own Default BRR; it does not apply tenants' BRR modified from Symantec CloudSOC.

The **Add/Edit Application Attributes** object displays all attributes configured in the current rule. When multiple attributes are configured for a rule, they are logically ANDed in the condition. In the following example, four attributes are already configured for the current rule.

**Caution:** Matches are case-insensitive. To perform case-sensitive matching, use the following CPL condition with a modifier:

```
request.application.attribute_name.case_sensitive=  
For details, refer to the Content Policy Language Reference.
```

To add an attribute:

1. On the Add Application Attributes dialog, click **Add Attribute**. The VPM displays the list of all application attributes.
2. In the list of attributes, select the ones you want to add. Optionally, type a string in the Filter field to select from a smaller list.

Depending on the type of attribute you select, you can specify a string value, a boolean value, or a numeric value/range. Alternatively, you can specify one or more system-defined values; this is available for all attributes.

See the following table for details on the different values.

3. After you configure the attribute, click **OK** to save it. The Add Application Attributes dialog displays the attribute you added.
4. Repeat the previous steps to add more attributes. You can add an attribute to a rule only once; after you add it, it is no longer available on the list of attributes.

### Configure values for Application Attributes

Value Type	Description
String value	Enter a string and select an operation from the menu.

Value Type	Description
Boolean value	Select <b>True</b> or <b>False</b> .
Numeric value	Do one of the following: <ul style="list-style-type: none"> <li>■ Choose an operator and enter a numeric value.</li> <li>■ Specify a numeric range and whether the value should be inside (<b>Between</b>) or outside (<b>Not Between</b>) the range.</li> </ul>
System values	Specify one or more system-defined values: <ul style="list-style-type: none"> <li>■ <b>Attribute database is unlicensed:</b> You do not have a valid Application Attributes license.</li> <li>■ <b>Attribute database is unavailable:</b> A non-licensing problem exists with the Application Attributes database or with accessing the service, or the Application Attributes service is disabled.</li> <li>■ <b>Attribute is not defined for application:</b> The specified attribute is undefined or does not exist for the given application.</li> </ul>

## Renamed Attribute Warnings

If a policy rule includes an attribute that has been renamed in the currently downloaded database, policy warnings occur at compilation time. The following is an example of the warning:

Deprecation warning: 'Default\_BRR'; 'Default\_BRR' has been replaced by 'Office Temperature' due to Too obscure and will no longer be accepted after Sat, 27 Jun 2020 00:00:00 UTC. Please switch to the new name before then.

To ensure that policy performs as intended, edit all instances of the renamed attribute and re-apply policy by the specified date. You can use the [View Occurrences](#) or [search](#) functionality in the VPM to locate other instances of the attribute.

To edit an existing attribute:

1. On the **Add Application Attributes** dialog, select the attribute to edit.
2. Click **Edit**. The VPM opens the **Edit Application Attribute** dialog.
3. Edit the attribute as required. See the previous table for details.

To delete an existing attribute:

1. On the **Add Application Attributes** dialog, select the attribute to delete.
2. Click **Delete**. The attribute is deleted.

## Application Group

This object allows you to apply policy actions to a group of similar applications. For example, deny all applications within the File Transfer group. To create policy for file transfers through a specific application, use the "Application Name" below object.

To block all users from accessing specific web applications, see "Application Name" below. To block access to all social networking sites, see "Request URL Category" on page 77 .

Modifications to the database are automatically provided in updates via the subscription feed.

If policy includes an application group name that has been removed, a deprecation message appears at compile time and you must update policy to reflect the changes. Database updates also include new application groups.

To control web application groups:

1. (Optional) Filter the list of application groups. In the **Filter list of application groups by** section, enter a search string in the **Name** field. The dialog shows a filtered list of groups that match the search criteria you entered, and the list header reads **Application Groups (filtered)**.

To show the complete list, clear the **Name** field. The list header reads Application Groups.

2. Select the check box for each group you want to select. The **Application Groups Selected** section displays the selected groups.

To remove groups from the list, clear the check box for each group you want to remove.

3. Verify the selected groups in the **Application Groups Selected** section.

## Application Name

Specify an action for one or more web applications.

Because a web application pulls in content from multiple sources on the web and is a collection of URLs that might belong to several different categories, this object gives you the flexibility to regulate access to all content associated with the application. For example, the application Facebook that belongs to the Social Networking category includes URLs that belong to Email and Games categories.

This object allows you to define the behavior/rule when the URL in a user request matches the specified Web application. To create policy for a specific URL, use the Request URL object.

**Note:** Modifications to the database are automatically provided in updates via the subscription feed.

To control web applications:



1. (Optional) Filter the list of applications. In the **Filter list of applications by** section, do at least one of the following:
  - Show only the applications available for a given application group. Select a group from the **Application Group** menu.
  - Show only the web applications that support a specific operation. Select an operation from the **Supported Operation** menu.
  - Search for an application by name. Enter a search string in the **Name** field.

The **Applications (filtered)** list shows the applications that match your filter and/or search criteria. To show the complete list again, clear the filters and search field. The list header reads Applications.

2. Select the check box for each application you want to control. The **Applications Selected** section displays your selections.

To remove applications from the list, clear the check box for each application you want to remove.

3. Verify the selections in the **Applications Selected** section.

## Application Operation

Control whether users can perform the specified web application operation(s). For example, block users from uploading attachments.

When you block an operation, URLs that support or perform that operation are blocked; the web application itself is not blocked. For example, when you block users from uploading attachments, users in your network are unable to upload attachments to Facebook, but they can still access Facebook, post comments, and upload videos.

To block all users from accessing specific web applications, see "Application Name" on the previous page. To block access to all social networking sites, see "Request URL Category" on page 77 .

To control web application operations:

1. (Optional) Filter the list of operations. In the **Filter list of operations by** section, do at least one of the following:
  - Show only the operations available for a given web application. Select an application from the **Supporting Application** menu.
  - Search for an operation by name. Enter a search string in the **Name** field.

The Operations (filtered) list shows the operations that match your filter and/or search criteria. To show the complete list again, clear the filter and search field. The list header reads **Operations**.

2. Select the check box for each operation you want to control. The **Operations Selected** section displays your selections.

To remove operations from the list, clear the check box for each operation you want to remove.

3. Verify the selections in the **Operations Selected** section.

## Category

This object functions the same as "Request URL Category" on page 77, but is unique to the DNS Access Layer.

## Destination Host/Port

Specifies the hostname or port of a destination server. The policy defined in this rule applies to this host on this port only. Enter the host name and port number, and select matching criteria. This object is automatically prefixed with **Destination**, such as **Destination: company.com:80**.

## Destination IP Address/Subnet

Specifies the client IPv4 or IPv6 address, an IPv4 address with one or more wildcards, or a range of IP addresses in a network; an optional subnet mask (for IPv4) or prefix length (for IPv6).

- For information on using an IP address range, refer to article:

<https://knowledge.broadcom.com/external/article/16627>

- For information on using wildcards, refer to article:

<https://knowledge.broadcom.com/external/article/165925>

The policy defined in this rule only applies to this address only or addresses within this subnet. This object is automatically prefixed with **Destination**, such as **Destination: 1.2.0.0/255.255.0.0**.

## DNS CNAME

Specifies the rule applies to DNS CNAME responses matching a given hostname. Enter the host name and select matching criteria. This object is automatically prefixed with **DNS CNAME**, such as **DNS CNAME: host.com**.

## DNS Response Code

Specifies the rule applies to DNS responses containing a specific DNS Response code. Select one or more codes from the list.

## DNS Response IP Address/Subnet

Specifies the client IPv4 or IPv6 address, an IPv4 address with one or more wildcards, or a range of IP addresses in a network; an optional subnet mask (for IPv4) or prefix length (for IPv6).

- For information on using an IP address range, refer to article:

<https://knowledge.broadcom.com/external/article/16627>

- For information on using wildcards, refer to article:

<https://knowledge.broadcom.com/external/article/165925>

The policy defined in this rule only applies to DNS responses containing this address or addresses within this subnet. This object is automatically named using the prefix DNS; for example, DNS: 1.2.3.4/255.255.0.0.

## File Extensions

Creates a list of file extensions. The rule is triggered for content with an extension matching any on the list. You can create multiple lists that contain various extensions to use in different rules.

Select pre-defined extensions:

1. In the search field, enter a search string. The dialog displays a filtered list.
2. Select the extensions you want to add.

If the File Extension object does not include the file extension type that you require, you can create a new extension:

1. Click **Add Extension**.
2. In the dialog that appears, enter the extension and description.
3. Click **Set**.

To edit an existing extension:

1. Click the pencil icon beside the extension you want to edit.
2. On the dialog that appears, edit the extension or description.
3. Click **Set**.

To delete an existing extension:

1. Click the recycle bin icon beside the extension you want to edit.
2. On the confirmation message that appears, click **OK**.

## Flash Application Name

Identifies the name of the Flash application exchanged during the connect stage:

- **Simple Match**: Enter the name of a valid Flash application in the **Flash Application** name field.
- **Regular Expression Match**: Enter a valid regular expression string in the **RegEx** field.

## Flash Stream Name

Identifies the name of the stream that is being requested:

- **Simple Match**: Enter the name of a valid Flash stream in the **Flash Stream** name field.
- **Regular Expression Match**: Enter a valid regular expression string in the **RegEx** field.

## HTTP MIME Types

Creates a list of HTTP MIME content types. The rule is triggered for content matching any on the list. You can create multiple lists that contain various MIME types to use in different rules. For example, create a list called MicrosoftApps, and select MIME types application/vnd.ms-excel, application/vnd.ms-powerpoint, application/vnd.ms-project, and application/vnd.works.

**Note:** If you require a MIME type not contained in this list, use a "Request URL" below object that uses the **At End** matching criteria.

## Respmod Header

Allows you to create a condition that inspects ICAP RESPMOD response headers and perform a regular expression match:

1. From the **Header Name** menu, specify the name of the header to inspect.

Before you add a header name, the menu is empty. Any header names you add are saved in the list so you can select them in the future.

2. In the **Regex** field, enter the pattern to match.

## RDNS Response Host

Specifies a reverse DNS response hostname resolved in the reverse lookup of a client IP address. Enter the host name and select matching criteria. This object is automatically named using the prefix RDNS, such as RDNS: host.com. If you select a matching qualifier, that attribute is appended to the object in parentheses, such as RDNS: host.com (RegEx).

## Request URL

Applies to a URL in a user request (that is, a request sent by the client to the ProxySG appliance). Use this object when you want to create policy for a website that has a URL construct you are reasonably certain of. Most websites today have multiple sources that populate the content of the website and it is a challenge to block content using a specific URL.

To create a rule for all URLs that belong to a specific application, use the "Application Name" on page 72 object. To define rules to permit or allow specific actions for Web applications, see "Application Operation" on page 73.

Alternatively, use the "Request URL Category" on the facing page object to create policy for all URLs belonging to a specific web filtering category.

To check for a match against a requested URL, select an option and enter the required information in the fields:

- **Simple Match**—Matches a partial URL. If a host name is specified, all hosts in that domain or subdomain match; if a path is specified, all paths with that path prefix match; if a scheme or port number is specified, only URLs with that scheme or port match. This object is automatically named using the prefix URL, such as URL: host.com.

- **Regular Expression Match**—Specifies a regular expression. This object is automatically named using the prefix URL, such as URL: host.com (RegEx).
- **Advanced Match**—Specifies a scheme (protocol), host, port range, and/or path. Unlike the other options on this dialog, selecting Advanced Match allows you to enter a name at the top of the dialog to name the object. With host and path, you can select from the drop-down list to match exactly as entered or parts thereof: Exact Match, Contains, At Beginning, At End, or RegEx. If you select a matching qualifier, that attribute is appended to the object in parentheses, such as host.com (Contains).

## Request URL Category

Allows you to allow or restrict access to an entire category of URLs. Based on the content filtering vendor that you have enabled, the relevant categories display in this object.

When you use this object, you can enforce access to all URLs that belong to the specified category. Each user request is checked against the content filter database for a category match, and evaluated for further action based upon the policy.

- **Blue Coat**—Displays the Symantec categories described as follows:

<https://sitereview.bluecoat.com>

- **Local database categories**—Displays all categories defined in custom local content filtering databases if the databases are enabled. The name of the default local database is Local.

Up to seven custom local databases are supported. Custom database names appear in the list under their user-defined names.

- **Policy**—Displays all current predefined and user created URL categories. This includes all category-related configurations created in the VPM, as well as in the Local and Central policy files (after being installed). Select and deselect categories as required.

You can also create new categories from this dialog, which is similar to the dialog accessed through the VPM Menu Bar as described in Creating Categories.

- **YouTube**—Displays YouTube categories if this provider is enabled. The categories are static. For more information, see “Filtering Web Content” in the SGOS Administration Guide.

**Note:** This feature is provided on an "as-is" basis. Symantec has no control of, and is not responsible for, information and content provided (or not) by YouTube. You are obligated to comply with all terms of use regarding the foregoing, including quotas that may be imposed by YouTube. Symantec shall not be liable for any discontinuance, availability or functionality of the features described herein.

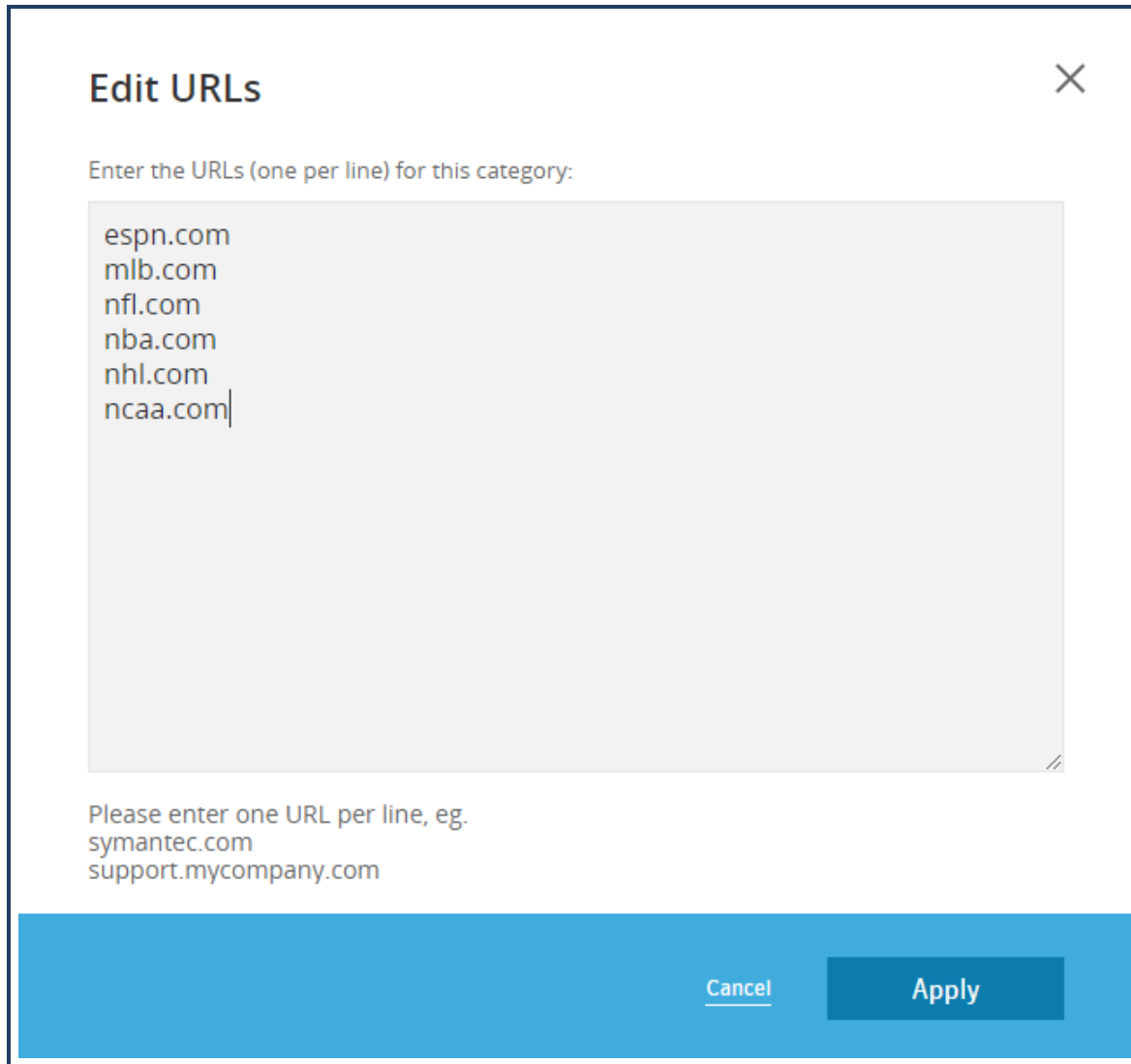
- **System**—Displays hard-coded statuses. Select and deselect categories as required.

Create a policy category:

## Symantec: A Division of Broadcom

1. Select **Configuration > Categories**.
2. In the Edit Categories dialog, click **Add Category**.
3. In the New Category dialog, enter a descriptive name and click **OK**.
4. Select the category name under Policy and click **Edit URLs**.
5. In the Edit URLs dialog, enter URLs, one per line, for the category.

Show image)



**Edit URLs**

Enter the URLs (one per line) for this category:

espn.com  
mlb.com  
nfl.com  
nba.com  
nhl.com  
ncaa.com

Please enter one URL per line, eg.  
symantec.com  
support.mycompany.com

Cancel **Apply**

6. Click **Apply** to save the category URL definition. The category is now available to use in policy objects that use URL categories.

## Category Hierarchy Behavior

Once categories have been created, they can be selected and deselected as required. If you create sub-categories (a parent and child category hierarchy), the category selection behavior is the following:

- Selecting a parent category automatically selects all child categories if no child categories are already selected.
- Deselecting a parent category automatically deselects all child categories if all child categories are already selected.
- If one or more of the child categories are already selected or deselected, selecting or deselecting the parent category does not affect child categories—the status of selected or deselected remains the same.

This behavior applies to as many levels as you create.

## Resolved Country

The geographical location of the IP address of the specific host from which the appliance retrieves content for the response.

For detailed information on this policy gesture and usage examples, refer to the `supplier.country=` condition in the *Content Policy Language Reference*.

Specify the following as needed:

- Under **Locations**, select one or more license statuses.
- In the list of countries, select the countries you want to add. Optionally, type a string in the **Filter** field to select from a smaller list.

The Selected Locations list displays the license statuses and countries you selected.

## Response Code

Specifies that the rule applies to content responses containing a specific HTTP code. Select a code from the drop-down list.

## Response Data

Specifies the rule applies to content responses containing specific regular expressions:

1. In the **RegEx to match** field, enter the regular expression string to match.
2. In the **Number of bytes to examine** field, enter how many object bytes are scanned for the match.

## Response Header

Specifies the rule applies to content responses containing a specific header. Symantec supplies a list of standard headers, but you can also enter a custom header.

To specify a response header:

## Symantec: A Division of Broadcom

1. From the **Show** drop-down list select the viewing field from All to Standard or Custom, as desired. Standard displays only the default standard headers. Custom displays any admin-defined headers that exist.
2. From the **Header Name** drop-down list, select a standard or custom header.
3. In the **Header Regex** field, enter the header string this rule applies to.

## Server Certificate

Allows testing of server certificate attributes to be used by the proxy-to-server HTTPS connections. Select one of the options:

- **Hostname:** This is the hostname you want to match in the server certificate. After you enter the hostname, select from the dropdown list one of the following: Exact Match, Contains, At Beginning, At End, Domain, or Regex.
- **Subject:** This is the fully qualified subject name in the server certificate. After you enter the subject, select from the dropdown list one of the following: Exact Match, Contains, At Beginning, At End, Domain, or Regex.

## Server Certificate Category

Functions the same as the "Request URL Category" on page 77 object, but the piece of information used for matching and categorizing is the hostname in the server certificate.

## Server Connection DSCP

Tests the inbound differentiated service code point (DCSP) value of primary server-to-proxy connections. By testing DCSP bits (in the IP header), additional policy dictates how to handle traffic associated with the type of service. Specify DSCP values to test against inbound server connections:

- Select IP Precedence values (denoted by CS) and Assured Forwarding Classes (Denoted by AF) as required).
- (Optional) Rather than select Precedence and AFC values, enter a DSCP value range. The valid range is 0 to 63. Symantec does not recommend this option. Most applications fit into one of the defined values.

For conceptual information about configuring the ProxySG to manipulate traffic based on type of service, see "Managing QoS and Differentiated Services" on page 200.

## Server Negotiated Cipher

Tests the cipher suites used in a proxy-to-server connection, select one or more cipher suites valid for this rule.

**Note:** Refer to the list of supported cipher suites:

<https://knowledge.broadcom.com/external/article/170130>



## Server Negotiated Cipher Strength

Specifies the cipher strength between a proxy-to-server HTTPS connection, select one or more of the strength options valid for this rule Export, High, Medium, or Low.

Low, Medium, and High strength ciphers are not exportable.

## Server Negotiated SSL Version

Specifies the SSL version between a proxy-to-server HTTPS connection.

To specify a server-negotiated SSL version, select one or more of the strength options valid for this rule: TLSv1.3, TLSv1.2, TLSv1.1, TLSv1, SSLv3.

## Server URL

This object is functions the same as the "Request URL" on page 76 object, but applies to a URL sent from the ProxySG appliance to a server. If the appliance is performing URL rewrites, the URL sent from the client might change, which requires another URL matching check.

## Server URL Category

Matches the content categories of the URL that the ProxySG appliance sends for a user request. If a URL has been rewritten, the condition matches the categories of the rewritten URL instead of the requested URL.

## Threat Risk Level

The Threat Risk Levels service assigns threat risk levels to URLs according to specific criteria. See the following table for an overview of the risk levels and how they are represented on in the Threat Risk Details report in the Management Console (**Statistics > Threat Risk Details**).

**Tip:** This object is available in more than one policy layer. Depending on the layer, the object may be called **DNS Request Threat Risk Level**, **Request URL Threat Risk Level**, **Server Certificate Hostname Threat Risk Level**, or **Server URL Threat Risk Level**.

### Threat Risk Levels

Level	Report Color	Description
Low (Levels 1-2)	Green	The URL has an established history of normal behavior and has no future predictors of threats; however, this level should be evaluated by other layers of defense (such as Content Analysis and Malware Analysis).

Level	Report Color	Description
Medium-Low (Levels 3-4)	Green	The URL has an established history of normal behavior, but is less established than URLs in the Low group. This level should be evaluated by other layers of defense (such as Content Analysis and Malware Analysis).
Medium (Levels 5-6)	Yellow	The URL is unproven; there is not an established history of normal behavior. This level should be evaluated by other layers of defense (such as Content Analysis and Malware Analysis) and considered for more restrictive policy.
Medium-High (Levels 7-9)	Orange	The URL is suspicious; there is an elevated risk.  Symantec recommends blocking at this level.
High (Level 10)	Red	The URL is confirmed to be malicious.  Symantec recommends blocking at this level.  The service returns a system-defined value in the rare instance when a threat risk level does not apply.

Specify the risk level:

- Select **Risk levels between \_\_\_ and \_\_\_** to specify the risk level.

For both values, select a level from 1 to 10. Select the same number in both fields to specify one level; select different values to specify a range. Refer to Table 3-6, Threat Risk Levels for descriptions.

- Specify a system-defined value. Refer to "System-Defined Threat Risk Levels" below for descriptions.

(Optional) Select **Use Effective Threat Risk Level (if configured)** if you want to override the assigned threat risk level. For information on the effective threat risk level, see "Set Effective Threat Risk Level" on page 118. If no effective threat risk level is set, the assigned one is used.

### System-Defined Threat Risk Levels

CPL		
Use for <code>url.threat_risk.level=</code>	VPM	Description
	Use in Threat Risk Level Objects	
none	<b>Threat Risk Level not available</b>	The URL does not have a threat risk level assigned to it and the request is not forwarded to WebPulse (or it has been forwarded and there is still no data), or the Threat Risk Levels service is disabled.

CPL		
	VPM	
Use for <code>url.threat_risk.level=</code>	Use in Threat Risk Level Objects	Description
pending	<b>Threat Risk Level data pending background WebPulse analysis</b>	No risk level is assigned to the URL on the appliance, but the appliance performed a WebPulse request in the background. Subsequent requests for the URL could match a result from the WebPulse cache.
unavailable	<b>Threat Risk Level database or service not accessible</b>	A non-licensing problem exists with the BCWF database or with accessing the WebPulse service.
unlicensed	<b>Threat Risk Level feature not licensed</b>	The Threat Risk Levels license is not valid.

## WebEx Site

Specifies the WebEx site to allow or deny connections to.

# Destination Column/Policy Layer Matrix

**Destination** column objects are available in the following policy layers:

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Application Attributes						X	X		X			
Application Group						X	X		X		X	
Application Name						X	X		X		X	
Application Operation							X		X		X	
Category				X								
Combined Destination Object				X				X	X	X	X	X
Destination Host/Port						X	X	X	X	X	X	X
Destination IP Address/Subnet						X	X	X	X	X	X	X
DNS Response CNAME				X								
DNS Response Code				X								
DNS Response Contains No Data				X								

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
DNS Response IP Address/Subnet				X								
File Extensions									X	X		X
HTTP MIME Types									X	X		
ICAP Respmode Response Header									X			
RDNS Response Host				X								
Request URL						X	X	X	X	X		X
Request URL Category						X	X	X	X	X	X	
Resolved Country				X		X	X		X	X		X
Response Code									X			
Response Data									X			
Response Header									X			
Server Certificate						X	X			X	X	
Server Certificate Category						X	X					

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Server Connection DSCP				X					X	X	X	
Server Negotiated Cipher							X					
Server Negotiated Cipher Strength							X					
Server Negotiated SSL Version							X					
Server URL						X	X					
Server URL Category												X
Threat Risk				X		X			X	X	X	
WebEx Site									X			

# Service Column Objects

A service object specifies a service type, such as a protocol, that is evaluated by the policy. Not all policy layers contain the same Service objects; see the "Service Column/Policy Layer Matrix" on page 90 for details.

**Caution:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define a service object name.

## Static Objects

Static VPM objects are listed by default on the **Set *object type* Object** dialog; you do not have to click **Add a new object** to display them. To add a static object, select it in the list and click **Set**. There is no further need to configure the object after it is added to a policy rule.

The following static objects are available:

- **Client Certificate Requested:** Checks whether or not the OCS requests for client certificate authentication. The ProxySG appliance returns an exception page is sent to the browser when SSL proxy intercept is enabled and a client certificate is requested by the OCS; or you can configure the appliance to tunnel SSL over TCP when a protocol error occurs.
- **Request Forwarded:** Specifies that the request was forwarded. Set the object to Negate to specify that the request was not forwarded.
- **Using HTTP Transparent Authentication:** The rule applies if the service is using HTTP transparent authentication.
- **Virus Detected:** The rule applies if ICAP scanning detects a virus.

## Combined Service Object

An object that invokes multiple services. See "Combined Objects " on page 142.

## Client Protocol

Specify the client protocol types and subsets.

From the first drop-down list, select a type: CIFS, Endpoint Mapper, FTP, HTTP, HTTPS, Instant Messaging, MS-TURN, P2P, Shell, SIP, SOCKS, SSL, Streaming, TCP Tunneling, or WebSocket.

The second drop-down list allows you to select a protocol subset (the options available depend on the selected protocol):

- All—Applies to all communication using the specified client protocol.
- Pure—Applies if no other protocol is tunneled over the specified client protocol.

- **Over**—Applies if the client protocol communicates through the specified transport method.

## Health Check

This condition tests whether the current transaction is a health check transaction. Optionally, the condition tests whether the transaction is that of a specific health check.

1. Select one of the following:
  - **Not a Health Check**: Transaction is not identified as a health check.
  - **Any Health Check**: A health check service of any type was matched.
  - **Any of the selected health checks below**: A health check of the selected types was matched.

Select one or more options in the list of health checks.

## Health Status

This condition tests whether the target of the specified health check is health or sick.

## ICAP REQMOD/RESPMOD Error Code

Defines an object that recognizes one or more ICAP error codes returned during a malware scan. The rule applies if the scan returns the specified errors.

Select one of the options:

- **No errors**: An ICAP scan was performed without scanning errors.
- **Any errors**: An ICAP error code was returned during a scan.
- **Selected errors**: An ICAP error code of a specific type or types. In the Available Errors field, select one or more ICAP error codes (press and hold the Control key to select more than one type or the Shift key to select a block of types).

## Protocol Methods

Specifies the protocol methods that trigger a rule.

1. From the **Protocol** drop-down list, select one of the options: FTP, HTTP, HTTPS, SOCKS.
2. Select one or more methods.

## Service Group

Specify any default or custom proxy service group that exists on the appliance (created from the Management Console; select **Configuration > Services > Proxy Services**).



**Note:** The **Web Access** layer only displays and accepts proxy service groups.

## Service Name

Specify any default or custom proxy service that exists on the appliance (created from the Management Console; select **Configuration > Services > Proxy Services**).

- The Web Access Layer only displays and accepts proxy services.
- The Admin Access Layer only displays and accepts console services.

## SSL Proxy Mode

Specifies the deployment mode of the SSL proxy:

- HTTPS Forward Proxy requests
- HTTPS Reverse Proxy requests
- Unintercepted SSL requests

This object allows you to apply policy to a subset of SSL traffic going through the appliance. For example, this object can be used to enforce strong cipher suites for HTTPS reverse proxy requests while allowing all cipher suites for HTTPS forward proxy requests.

## Streaming Content Type

Specifies streaming protocols. Select **All Streaming Content** to select all protocols, or specify one or more streaming protocols.

# Service Column/Policy Layer Matrix

Servicecolumn objects are available in the following policy layers:

Object	Admin Authentic ation	Admin Access	Admin Logi n Banner	DNS Acce ss	SOCKS Authentic ation	SSL Interc ept	SSL Acce ss	Web Authentic ation	Web Acce ss	Web Cont ent	Web Requ est	Forwar ding
Client Certificate Requested						X						
Client Protocol							X		X	X	X	X
Combined Service Object							X		X	X	X	X
Health Check							X					X
Health Status						X				X	X	X
ICAP REQMOD/RES PMOD Error Code									X			
Protocol Methods									X	X		
Request Forwarded							X					
Service Group										X	X	
Service Name		X	X						X	X	X	
SSL Proxy Mode							X					
Streaming Content Type									X			
Using HTTP Transparent Authentication									X	X		
Virus Detected									X			

# Time Column Objects

A time object specifies a block of time or time trigger that determines client access regarding other parameters in the rule (such as Web sites and content types). Not all policy layers contain the same Time objects; see the "Time Column/Policy Layer Matrix" on the next page for details.

**Caution:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define a service object name.

## Combined Time Object

An object that combines multiple time restrictions. See "Combined Objects" on page 142.

## Time

Specifies time restrictions:

- Time zone: Specify **Local** or **UTC**. Local time sets the rule to follow the appliance's internal clock. UTC sets the rule to use the Universal Coordinated Time (also known as Greenwich Mean Time or GMT).
- Time of the day: Specify **All** or select a time range in 24-hour notation. The range can be contained within one 24-hour calendar day, or overlap days. For example, configuring the time to range from 22:00 to 06:00 sets a limit from 10 at night to 6 the following morning.
- Days of the week: Specify **All** or select specific days.
- Days of the month: Specify **All** or enter specific dates. To select a single date, enter the same number in both fields. For example, selecting 22 and 22 specifies the rule to apply only the 22nd day of every month.
- Time of year: specify **All** or set a different restriction that spans one or more months. Select the month and day ranges. This calendar restriction applies every year unless the restriction is modified. Overlapping months is allowed, similar to the behavior of Days of the week.
- Time range: Specify **All** or specify a one-time only restriction. Select the year, month, and day range. This calendar restriction applies only during the time specified and does not repeat.

# Time Column/Policy Layer Matrix

Timecolumn objects are available in the following policy layers:

Object	Admin Authentica tion	Admi n Acce ss	Admin Login Ban ner	DNS Acce ss	SOCKS Authentica tion	SSL Interc ept	SSL Acce ss	Web Authentica tion	Web Acce ss	Web Cont ent	Web Requ est	Forward ing
Combi ned Time Object				X					X	X	X	
Time				X					X	X	X	

# Action Column Objects

An action object determines which action to take if other parameters, such as source, destination, service, and time requirements validate the rule. Not all policy layers contain the same Action objects; see the "Action Column/Policy Layer Matrix" on page 126 for details.

**Note:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define object names.

## Static Objects

Static VPM objects are listed by default on the **Set *object type* Object** dialog; you do not have to click **Add a new object** to display them. To add a static object, select it in the list and click **Set**. There is no further need to configure the object after it is added to a policy rule.

The following static objects are available:

- **Accept/Do Not Accept HTTP/2 Client-Side Connections:** Whether or not the server accepts HTTP/2 requests from the client.
- **Allow:** The specified user request is allowed. Selecting this overrides other related configurations.
- **Allow Access to Server:** The outgoing request to the OCS is allowed. Selecting this overrides other related deny policy configurations.
- **Allow Content From Origin Server:** Allows request to access content from an OCS if the content is not cached.
- **Allow DNS From Upstream Server:** Allows the ProxySG appliance to send requests for data not currently cached to DNS servers.
- **Allow Read-Only Access:** Grants full access to view data on the appliance.
- **Allow Read/Write Access:** Grants full access to view and manipulate data on the appliance.
- **Always Verify:** Cached content is always verified for freshness for the sources, destinations, or service specified in the rule. For example, the CEO and Executive Staff always require content to be the most recent, but everyone else can be served from the cache.
- **Allow Access to Server:** The outgoing request to the OCS is allowed. Selecting this overrides other related deny policy configurations.
- **Allow Content From Origin Server:** Allows request to access content from an OCS if the content is not cached.
- **Allow DNS From Upstream Server:** Allows the ProxySG appliance to send requests for data not currently cached to DNS servers.
- **Allow Read-Only Access:** Grants full access to view data on the appliance.
- **Allow Read-Write Access:** Grants full access to view and manipulate data on the appliance.
- **Enable/Disable ICAP Mirroring for response modification:** ICAP Mirroring allows you to serve content for known, difficult-to-handle data types (such as stock tickers or media streams without end) directly to users, without needing to wait for a portion of (or the complete) stream to be downloaded.

ICAP Mirroring can be used with any source or destination in policy to match an HTTP request. A Web Content layer rule to specify the ICAP service is also required to send response data to the ICAP server.

If the ICAP server scans the data and identifies an issue (virus, malware detected, or a DLP rule is triggered) while the user is still receiving the data, their connection will be reset by the ProxySG appliance and an entry detailing this action is added to the HTTP access log. If the user has downloaded the content in its entirety before the ICAP server responds with a "virus found" or "DLP violation" message, the detection will be logged without affecting the user.
- **Enable/Disable DNS Imputing:** If DNS imputing is enabled, the ProxySG appliance appends the suffixes in the DNS imputing list to host names looked up when the original name is not found.
- **Enable/Disable Pipelining:** Enables or disables the ProxySG pipelining feature, which, when enabled, examines Web pages for embedded objects and requests them from the origin server in anticipation of a client request.
- **Exempt From Access Security:** If set, the current rule is exempt from Access Security policy.
- **Force Deny:** Forces a request to be denied, regardless if rules in subsequent layers would have allowed the request.
- **Force Deny (Content Filter):** Forces a request to be denied, regardless if rules in subsequent layers would have allowed the request. In the access logs, the Content Filter moniker allows you to identify policy denies based on content filtering versus other reasons.
- **Force/Do Not Force IWA for Server Auth:** When configured for explicit proxy, Internet Explorer (IE) does

- **Always Verify:** Cached content is always verified for freshness for the sources, destinations, or service specified in the rule. For example, the CEO and Executive Staff always require content to be the most recent, but everyone else can be served from the cache.
- **Block/Do Not Block PopUp Ads:** Blocks or allows pop up windows. Symantec recommends creating separate Web Access Layers that only contain pop up blocking actions. Furthermore, many Web applications require pop up windows. As it is unlikely that your Intranet contains pages that pop up unwanted advertising windows, Symantec recommends disabling pop up blocking for your Intranet. For example:

Web Access Layer rule 1: Specify the Intranet IP address and subnet mask in the Destination column and select Do Not Block Popup Ads in the Action column.

Web Access Layer rule 2: Select Block Popup Ads in the Action column.

As you continue to modify policy, you can add more policy layers to block or allow specific IP addresses, but the policy layer as defined in the Web Access Layer rule 2 above must always be positioned last. Blocking pop up ads is the default if a previous policy rule does not trigger.

- **Bypass Cache:** Prevents the cache from being queried when serving a proxy request, and prevents the response from the origin server from being cached.
- **Bypass DNS Cache:** Prevents the request from querying the DNS cache list of resolved lookup names or addresses.
- **Check/Do Not Check Authorization:** Controls whether or not the ProxySG appliance forces a request to be sent to an upstream server every time to check authorization, even if the content is already cached. The check action is not usually required for upstream origin content servers performing authentication, as the appliance automatically tracks whether content required authentication in each case. However, it can

not support an IWA challenge from an origin server. If Force IWA for Server Auth is applied, the ProxySG appliance converts the 401-type server authentication challenge to a 407-type proxy authentication challenge, which IE supports. The appliance also converts the resulting Proxy-Authentication headers in client requests to standard server authorization headers, which allows an origin server IWA authentication challenge to pass through when IE is explicitly proxied through the appliance.

- **Integrate/Do Not Integrate New Hosts:** Used in server accelerator deployments. When enabled, the corresponding host that is accessed is added to the list of hosts for which the ProxySG appliance performs health checks. If that host name resolves to multiple IP addresses that correspond to different servers, the appliance fetches content from the available servers and ignores the servers that fail the health check.
- **Log Out/Do Not Log Out Other Users With Same IP:** If more than one user is logged in at the IP address of the current transaction, this property logs out all users from the current IP address except the user of the current transaction.
- **Log Out/Do Not Log Out User:** If more than one user is logged in at the IP address of the current transaction, this property logs out all users from the current IP address except the user of the current transaction.
- **Log Out/Do Not Log Out User's Other Sessions:** If a user is logged in at more than one IP address, this property logs out the user from all IP address except the IP address of the current transaction.
- **Mark/Do Not Mark As Advertisement:** Specifies content to be identified as an advertisement. The ProxySG appliance still fetches content from the cache (if present); however, just after serving to the client, the content is re-fetched from the ad server so that hit counters are updated.
- **Preserve Untrusted Issuer:** If an OCS presents a certificate to the ProxySG appliance that is not signed by a trusted Certificate Authority (CA), the appliance acts as a CA and presents the browser with an untrusted certificate. A warning message is displayed

be required when an upstream proxy is performing proxy authentication because of the way some proxies cache credential information, causing them not to reliably challenge every request. When requests are directed to an upstream proxy which operates in this manner, enabling Check Authorization ensures that all such requests are properly authorized by the upstream proxy before the content is served from the local cache.

- **Connect Using ADN When Possible/Do Not Connect Using ADN:** Connect Using ADN When Possible instructs the ProxySG appliance to use the byte caching tunnels (used in Application Delivery Network (ADN) deployments). Do Not Connect Using ADN prevents the use of tunnel connections.
- **Deny:** Selecting this overrides other related configurations and denies the specified user requests. For the configurable Deny object, see "Deny" on page 101.
- **Deny (Content Filter):** Selecting this overrides other related configurations and denies the specified user requests; use this object when you want the logged exception to indicate a Content Filter verdict was the reason for denial.
- **Disable/Do Not Disable Fast-Caching in Windows Media Client:** When disabled, the ProxySG appliance does not utilize fast-caching with a Windows Media Client.
- **Disable SSL Interception:** Selecting this object disables HTTPS interception.
- **Do Not Authenticate:** Selecting this overrides other configurations and the specified users are not authenticated when requesting content. In the SOCKS layer, the object is Do Not SOCKS Authenticate.
- **Do Not Authenticate (Forward Credentials):** Selecting this action forwards credentials upstream instead of authenticating on the appliance.
- **Do Not Bypass Cache:** The ProxySG appliance always checks if the destination is cached before going to the origin server; also, the content is cached if

to the user, and they can decide to ignore the warning and visit the website or cancel the request.

- **Require/Do Not Require Client Certificate:** For the SSL Proxy, specifies whether a client (typically a browser) certificate is required or not.

In forward proxy deployments, this is used to either request consent certificates or to support certificate realm authentication.

In reverse proxy deployments, client certificates are requested for certificate realm authentication.

See "Set Client Certificate Validation" on page 115.

- **Send Direct:** Overrides forwarding host, SOCKS gateway, or ICP configurations and instructs the ProxySG appliance to request the content directly from the origin server.
- **Serve Content Only From Cache:** Requests to access content that is not cached are denied. If the content is cached, the content is served.
- **Serve DNS Only From Cache:** Instructs the ProxySG appliance to only serve a DNS request from content that is already cached.
- **Support/Do Not Support Persistent Client Requests:** Allowing persistent connections to the ProxySG appliance from clients reduces load improves the all-around performance of the network. This object specifies whether or not to allow persistent server connections.
- **Support/Do Not Support Persistent Server Requests:** If the back-end authentication authority (such as LDAP, RADIUS, or the BCAA service) receives large numbers of requests, you can configure the ProxySG appliance to use persistent connections to the server. This dramatically reduces load on the back-end authentication authority and improves the all-around performance of the network. This object specifies whether or not to allow persistent server connections.
- **Trust/Do Not Trust Destination IP:** The Trust Destination IP object instructs the ProxySG appliance



cacheable.

- **Do Not Bypass DNS Cache:** The ProxySG appliance always queries the DNS cache list of resolved lookup names or addresses.
- **Do Not Cache:** Specifies that objects are never cached.
- **Do Not Duplicate Proxy Credentials Upstream:** Adding this object disables credential forwarding for a particular transaction.
- **Do not Preserve Untrusted Issuer:** If an OCS presents a certificate to the ProxySG appliance that is not signed by a trusted Certificate Authority (CA), the appliance either sends an error message to the browser, or ignores the error and processes the request, based on the configuration of the Server Certificate Validation object.
- **Do Not Use Kerberos Constrained Delegation:** Adding this object disables Kerberos Constrained Delegation for a particular transmission.
- **to trust the IP address sent by the client, forgoing a DNS lookup.** This is designed for transparent and ADN deployments. Conversely, the Do Not Trust Destination IP instructs the appliance to always perform a DNS lookup.
- **Use Default Caching:** Overrides the Do Not Cache and Set Force Cache Reasons actions and instructs the ProxySG appliance to use its default determination of whether or not to cache the content.
- **Use Default Setting for Preserve Untrusted Issuer:** The Preserve untrusted certificate issuer configuration setting in the ProxySG Management Console is used to determine whether or not untrusted certificate issuer should be preserved for a connection. This is the default behavior.
- **Use Default Verification:** Overrides the Always Verify action and instructs the ProxySG appliance to use its default freshness verification.

## Combined Action Object

An object that invokes multiple actions. See "Combined Objects " on page 142.

## Add Attack Detection Failure Weight

Allows you to change the default value of a single failed request event for a given response code on the ProxySG appliance. Each failed request can have a value of 0 - 500, depending on the nature of the failed request. This value specifies the amount that the client's failure counter increases per failure event.

## Add Default Group

A default group can be assigned to any realm. You can assign users to these groups, which are valid when authorization succeeds, fails, or not attempted. Default groups support guest users, which are users who are not authenticated against a realm, but are given a guest name and allowed access to specific information. For example, you create a default group that all guest users are assigned to, which makes it easier to track and log.

Default Groups are configured as described in "Group" on page 57.

## ADN Server Optimization

Specifies whether byte caching is employed on either branch or core, or both sides of an Application Delivery Network connection (specified IP addresses in the rule). Byte caching reduces WAN latency.

- **Optimize traffic in both directions:** Apply Byte Caching to incoming and outgoing traffic.
- **Optimize only inbound traffic:** Apply Byte Caching to incoming traffic.
- **Optimize only outbound traffic:** Apply Byte Caching to outgoing traffic
- **Do not optimize traffic:** Do not allow Byte Caching on specified connections.

## Authenticate

Creates an authentication object to verify users. Users will be prompted to provide a valid user name and password.

**Note:** Called **SOCKS Authenticate** and **Admin Authenticate** in the respective layers.

In the SOCKS Authenticate and Admin Authenticate layers, select an existing authentication realm from the **Realm** drop-down list.

In the Web Authentication layer, also specify a mode from the **Mode** drop-down list. The mode determines the way the appliance interacts with the client for authentication specifying the challenge type and the accepted surrogate credential:

- **Auto**—The default; the mode is automatically selected, based on the request. Selects among proxy, origin-IP, and origin-IP-redirect, depending on the type of connection (explicit or transparent) and the transparent authentication cookie settings.
- **Form Cookie**—For forms-based authentication: cookies are used as surrogate credentials. The cookies are set on the OCS domain only, and the user is presented with the form for each new domain. This mode is most useful in reverse proxy scenarios where there are a limited number of domains.
- **Form Cookie Redirect**—The user is redirected to the authentication virtual URL before the form is presented. The authentication cookie is set on both the virtual URL and the OCS domain. The user is only challenged when the credential cache entry expires.
- **Form IP**—The user's IP address is used as a surrogate credential. The form is presented whenever the user's credential cache entry expires.
- **Form IP Redirect**—This is similar to Form IP except that the user is redirected to the authentication virtual URL before the form is presented.
- **Proxy**—For explicit forward proxies: the appliance uses an explicit proxy challenge. No surrogate credentials are used. This is the typical mode for an authenticating explicit proxy.
- **Proxy IP**—The appliance uses an explicit proxy challenge and the client's IP address as a surrogate credential.

- **Origin**—The appliance acts like an OCS and issues OCS challenges. The authenticated connection serves as the surrogate credential.
- **Origin Cookie**—For transparent proxies: for clients that understand cookies but do not understand redirects; the appliance acts like an origin server and issues origin server challenges. The surrogate credential is used.
- **Origin Cookie Redirect**—For transparent forward proxies: the client is redirected to a virtual URL to be authenticated, and cookies are used as the surrogate credential. The appliance does not support origin-redirects with the CONNECT method.
- **Origin IP**—The appliance acts like an OCS and issues OCS challenges. The client IP address is used as a surrogate credential.
- **Origin IP Redirect**—Significantly reduces security; only useful for when clients have unique IP addresses and do not understand cookies (or you cannot set a cookie). Provides partial control of transparently intercepted HTTPS requests. The client is redirected to a virtual URL to be authenticated, and the client IP address is used as a surrogate credential. The appliance does not support origin-redirects with the CONNECT method.
- **SG2**—The mode is selected automatically, based on the request using the SGOS 2.x-defined rules.

If you selected a form mode in the Web Authentication layer, specify the form to use for forms-based authentication:

- **Authentication Form**—Selects the form used to challenge the user.
- **New Pin Form**—(Used with RSA SecurID authentication) Selects the form to prompt user to enter a new PIN.
- **Query Form**—(Used with RSA SecurID authentication) Selects the form to display to the user when a yes/no questions needs to be answered.

**Note:** In most deployments, the default form settings should be adequate; however, if you have customized authentication forms configured (in the Management Console, under **Configuration > Authentication > Forms**), you can select them from the drop-down lists.

## Authenticate Guest

Allows a user to be authenticated as a guest user. One scenario is to allow access to a user who might otherwise be considered unauthenticated. Another is where no authentication is required, but you want to track access. For more information, see the “Controlling Access to the Internet and Intranet” chapter in the *SGOS Administration Guide*.

1. In the **Guest Username** field, enter the name the guest is given. This name appears in the access logs.
2. In the **Guest Realm** area, select one of the following options:
  - Use realm:
  - Use realm from previous authenticate request:

3. In the **Guest Surrogate Refresh Time** area, select one of the following options:
  - Use realm's surrogate refresh time:
  - User surrogate refresh time:
4. From the **Mode** drop-down list, choose the authentication method the guest will see when challenged. The default mode is none. (For an explanation of the various kinds of modes, see "Authenticate" on page 98.)

## Authentication Charset

The VPM allows you enter non-ASCII in many objects, such user and group names and text for the **Notify User** object. This object allows you specify the character set to use in conjunction with localized policy. From the drop-down list, select a character set.

## Client and Server Certificate Exceptions

Built-in exceptions can be used to notify the user that the verification of the server or client's certificate failed. For a list and description of exceptions, see "Defining Exceptions" on page 183.

## Control Request/Response Header

Allows you to control and modify request or response headers by:

- Inserting a header with a specific value.
- Rewriting the value of a specific header.
- Suppressing a specific header.

To create a Control Request Header or Control Response Header object:

1. From the **Show** drop-list, select one of the following:
  - **All**—Shows all headers.
  - **Standard**—Shows default standard headers.
  - **Custom**—Shows any admin-defined headers.
2. (If applicable) From the **Header Name** list, select a standard (pre-defined) header or a custom header.
3. Select an action:
  - **Suppress**—The header is not visible.
  - **Set value**—Replace the header with a string or value.
  - **Append to value**—Add a string or value to the existing header.

## Deny

Force a request to be denied, and specify if the deny should occur whether not rules rules in subsequent layers would have allowed the request. You can also re-allow authentication and insert substitution strings. For the static **Deny** object, see the [Static Objects](#) list at the top of this page.

## Disable SSL Detection

Specify whether SSL is detected over HTTP, SOCKS, and/or TCP.

- If you configured SSL detection for one or two proxies, select **Traffic Tunneled Over** and at least one of the proxies listed.
- If you configured all proxies to not detect SSL, select **All Tunneled Traffic**.

## Duplicate Proxy Credentials Upstream

Sends BASIC credentials to an upstream server or proxy. User credentials (from ProxySG authentication) or custom credentials derived from a substitution must be specified.

1. Select the authentication method from the **Authentication Type** drop-down list:
  - **Origin**—If you are authenticating to an upstream OCS.
  - **Proxy**— If you are authenticating to a proxy server.
2. Select the credentials required for a particular OCS:
  - Select **Send user credentials** to send user credentials to the OCS.
  - Select **Send custom credentials** to forward a fixed username and password to the OCS.

**Note:** For all transactions that match this object, credentials are sent even if the receiving server does not require them.

## Dynamic Categorization

Dynamic categorization extends the process of categorizing a URL. Traditional content filtering involves searching of massive URL pattern databases, which are published by vendors and downloaded to the ProxySG appliance at specified intervals. As new content constantly reaches the Web, the limitation is that it cannot be filtered until its existence is discovered, added, and uploaded. Dynamic categorization enhances content filtering by scanning a new Web page, attempting to determine its contents, and categorizing accordingly in real time.

When an un-categorized page is first encountered, the appliance calls an external service with a categorization request. Once the content is scanned, a category is assigned (a majority of the time). For related information, refer to the *SGOS Administration Guide*.

Select a mode:

- **Perform immediately**—(Default selection) Objects not categorized by the database are dynamically categorized on first access. If this entails consulting the WebPulse service, the proxy request is blocked until WebPulse responds.
- **Perform in background**—Objects not categorized by the database are dynamically categorized as time permits. Proxy requests are not blocked while WebPulse is consulted. Objects not found in the database appear as category pending, indicating that WebPulse categorization was requested, but the object was served before the response was available.
- **Do not perform**—The loaded database is consulted for category information. URLs not in the database show up as category none.
- **Use dynamic categorizing setting from configuration**—Default to the ProxySG configuration (**Threat Protection > WebPulse**).

## Enable Encrypted Tap

Allows you to tap intercepted SSL traffic to an otherwise unused port. The data is presented in a format that can be understood by common network traffic analysis tools like Wireshark, common network intrusion detection systems such as Snort.

You can configure encrypted tap for client connections, server connections, or both.

**Note:** SSL interception must be enabled to use this object.

Configure client encrypted tap options:

1. Select **Enable client encrypted tap**.
2. From the **Interface** drop-down, select the unused interface to use for the tap.

To disable tap, select **Disable client encrypted tap**. Select **Does not apply** if this does not apply to client connections (no CPL is generated).

Configure server encrypted tap options:

1. Select **Enable server encrypted tap**.
2. From the **Interface** drop-down, select the unused interface to use for the tap.

To disable tap, select **Disable server encrypted tap**. Select **Does not apply** if this does not apply to server connections (no CPL is generated).

## Enable SSL Interception

1. Select content to be SSL intercepted:
  - **Enable HTTPS interception** - Allow SSL content to be examined.
  - **Enable HTTPS interception on exception** - Intercept SSL traffic if there is an exception, such as a certificate error or policy denial.
  - **Enable STunnel Interception** - Establish a policy where configured STunnel services (such as POP3S and SMTPS) are terminated and accelerated.
  - **Enable SSL interception with automatic protocol detection** - In addition to STunnel interception as described above, discovered HTTPS is handed off to the HTTPS proxy. Otherwise, SSL traffic continues in STunnel mode.
2. **Issuer Keyring** - Accept the default keyring or select this option and from the drop-down list select a previously generated keyring. This is the keyring used for signing emulated certificates.
3. **Hostname** - The hostname you enter here is the hostname in the emulated certificate.
4. **Splash Text** - The limit is 200 characters. The splash text is added to the emulated certificate as a certificate extension. The splash text is added to the emulated certificate as a certificate extension. For example:

Visit [http://example.com/https\\_policy.html](http://example.com/https_policy.html)

To add substitution variables to the splash text, click **Edit** and select from the list.

5. **Splash URL** - The splash text is added to the emulated certificate as a certificate extension.

The SSL splash can be caused by such occurrences as when a browser receives a server certificate signed by an unknown CA, or a host mismatch.

## Force Authenticate

Forces the user to authenticate even though the request is going to be denied for reasons that do not depend on authentication. This action is useful to identify a user before the denial so that the username is logged along with the denial. Refer to the *SGOS Administration Guide* for a description of the fields in this object.

**Note:** In the SOCKS Authentication policy layer, the object is **Force SOCKS Authenticate**. In the Admin Authentication layer, the object is **Force Admin Authenticate**.

## Kerberos Constrained Delegation

Allows you to select the IWA realm used to handle KCD for a particular transmission. An IWA realm is necessary to enable KCD on the ProxySG appliance.

1. Select the authentication method from the **Authentication Type** drop-down list:
  - **Origin**—If you are authenticating to an upstream OCS.
  - **Proxy**— If you are authenticating to a proxy server.
2. In the **IWA Realm** field, enter a valid IWA realm to use for Kerberos authentication.
3. (Optional) Enter the **Service Principal Name** to use for the OCS. The default SPN for the service is set to http/hostname. If a non-standard port is used for a service, use http/hostname:port

## Manage Bandwidth

Allows you to manage bandwidth for all protocols or specific protocols, on both inbound and outbound traffic.

1. Select to limit bandwidth on the client side or the server side:
  - **Client side**—Traffic flowing between a client and the ProxySG appliance.
  - **Server side**—Traffic flowing between a server and the appliance.
2. Select to limit bandwidth for inbound or outbound traffic:
  - **Inbound**—Network packets flowing into the appliance. Inbound traffic mainly consists of packets originating at the origin content server (OCS) and sent to the appliance to load a Web object and packets originating at the client and sent to the appliance for Web requests.
  - **Outbound**—Network packets flowing out of the appliance. Outbound traffic mainly consists of packets sent to the client in response to a Web request and packets sent to an OCS or other service (such as a virus scanner) to request a service.
3. Select a **Bandwidth Class** from the drop-down list.

## Modify Access Logging

Defines access logging behavior.

- **Disable all access logging**—No activity is logged for the requests matched by the rule.
- **Reset to default logging**—Resets to logging the request to the default log specified by the ProxySG configuration, if one exists.
- **Enable logging to**—Enables logging of requests matched by this rule to the specified log.
- **Disable logging to**—Disables logging of requests matched by this rule to the specified log.

## Notify User

This action displays a notification page in the user's web browser. A user must read the notification and click an **Accept** button before being allowed to access the content. You can customize the following:



- The page title, a notification message, and the **Accept** button.
- The conditions that cause a notification to be displayed again. By default, the notification is displayed each time a user begins a new web browsing session (reboots, logs out, or closes all web browser windows). You can configure re-notification to occur for each new visited host or web site, or after a time interval.

**Note:** The **Accept** button click action is logged if HTTP access logging is enabled. A URL is logged that contains the string `accepted-NotifyName`, where *NotifyName* is the name of the **Notify User** object.

This feature is designed to provide the following functionality:

- **Web-use compliance:** A compliance page is a customized notification page displayed on a user's Web browser when attempting to access the Internet. This page ensures employees read and understand the company's Acceptable Use Policy before Internet use is granted. Typically, a compliance notification is displayed each time a browser is opened, but you can configure a time condition to display the page at specific intervals or times of the day, week, or month.
- **Coach users:** A coaching page displays when a user visits a Web site that is blocked by content filtering policy. This page explains why the site is blocked, the consequences of unauthorized access, and a link to the site if business purposes warrants access. A coaching page is configured to display each time a user visits a new Web page that is barred by content filtering policy; however, you can also configure this page to appear at different time intervals.

**Caution:** This feature is not designed to enforce security controls. For best security, use policy actions that are designed for controlling access, such as Deny.

Example of the Notify User object

Notify User ?

Body:\*

<body>  
<!-- REPLACE THE FOLLOWING WITH YOUR MESSAGE -->  
Click on Accept after reading this message.  
  
<!-- The following is the Accept button, which you can customize. -->  
<p><a href="\$(exception.details)" onclick="Accept();">Accept</a>  
</body>

Notify mode:\*

☒ Notify once for all hosts

☐ Notify once for related domains

☐ Notify on every host

Virtual notify URL

http://notify.bluecoat.com

Notify users again:\*

☒ At next browser session

☐ After

Cancel

Apply

To configure HTML notification:

1. In the **Title** field, specify the title of the page (text only; no HTML is allowed).
2. In the **Body** field, enter HTML for the message that the browser should display to the user. The HTML body must contain an Accept button or link, which you can customize.

Default Accept link HTML:

```
<body><a href="$(exception.details)" onclick="Accept();">Accept</a></body>
```

Default button image HTML with example link to image on web server:

```
<body><a href="$(exception.details)" onclick="Accept();">  
 </a> </body>
```

If you use a WYSIWYG editor to write HTML, you can paste it into the VPM; be sure to copy the HTML from the <body> tag to the </body> tag.

3. Under **Notify mode**, select an option that determines notification when visiting a new Web site:

- **Notify once for all hosts**—The notification page is displayed only once; this is used for configuring compliance pages. This option uses a Virtual Notify URL. If you must change the URL from the default value, please read the limitation section following this procedure.

**Note:** This option might cause users to experience some noticeable Web browsing slowness.

- **Notify only once for related domains**—The notify page reappears each time the user visits a new Web site; this is used for configuring coaching pages.

**Note:** This option interferes with some Web advertising banners. In some cases, the notification page appears inside the banner. In other cases, banner ads are disabled by JavaScript errors. To fix these problems, do not serve notification pages for URLs that belong to the Web Advertising, Advertising, or Web Ads category. The actual name of this category varies with the content filtering vendor, and some vendors do not have an equivalent.

- **Notify on every host**—The notify page reappears each time the user visits a new Web host. Symantec recommends that only highly experienced administrators employ this option. In addition to breaking banner ads, as described above in the previous option, this option, on some Internet Web sites, might cause Javascript errors that impair the functionality of the site.

4. Under **Notify users again**, select an option that specifies when the notification expires and re-notification is required:

- **At next browser session**— The notification page does not reappear until the next browser session. When a user reboots, logs out, or closes all Web browser windows, this ends the browser session.
- **After (time interval)**—Notification reoccurs after the defined elapsed time (minutes or hours); this is useful for coaching.
- **After (specific time)**—Notification reoccurs at a specific time of day. You can specify an interval of days; this is useful for compliance.

**Note:** The time is referenced from the local workstation. If a compliance page is configured, verify the workstations and ProxySG clocks are synchronized.

## Interactivities and Workarounds

If you must change the default Virtual Notify URL, consider the following:

## Symantec: A Division of Broadcom

- The Virtual Notify URL consists of an HTTP domain name or IP address (http://); a port number is optional.
- Do not use a host name that is explicitly defined as a trusted site on Internet Explorer 6 for Windows XP, Service Pack 2. Furthermore, only use domain names that contain dots. If you use domain names that do not contain dots, the HTTP redirects generated by the notification action causes Internet Explorer to display false warning messages each time the user is redirected from an untrusted site to a trusted site, or the other way around.
- For transparent proxy deployments, the domain name must be DNS-resolvable to an IP address that is in the range of destination IP addresses that are routed to the ProxySG appliance.

### Policy Interactions

This action generates CPL that might interfere with other policy or cause undesired behavior. Consider the following guidelines:

- Do not create VPM policy that modifies the Cookie request header or the Set-Cookie and P3P response headers.
- Notification pages are saved in browser history.
- If multiple appliance in a chain of appliances are configured with different notification pages, each page must have a different object name.

## Override Access Log Field

Allows you to manipulate access log entries. For any specific log value, you can suppress the value, encode the value in Base64, or rewrite the value:

1. From the **Log Name** drop-down list, select a log (it must already be configured on the ProxySG appliance).
2. From the **Field Name** drop-down list, select an access log field.
3. Select one of the following:
  - **Log original value**—Records unmodified value in the access log.
  - **Suppress value**—Prevents value from appearing in the access log.
  - **Base64 encode value**—Records an encoded version of the value in the access log.
  - **Rewrite value**—In the field, enter a string that replaces the value.
    - (Optional) Click **Edit** to add substitution variables. The substitution variables instruct the ProxySG appliance to append specific information to the tracking object. The variables are categorized alphabetically by prefix (when available).
      - a. From the **Category** drop-down list, select a category to narrow the view to a subset of variables.
      - b. Under **Display Options**, filter variables by ELFF or CPL. By default, all variables are listed.
      - c. Select variables and click **Insert**.

**Note:** Some variables do not have prefixes, which allows you to substitute the value with information defined by other field types.

## Perform Request Analysis

This action specifies the request analysis service or service group that will be used to scan HTTP request data. These services are configured in the Management Console, under **Configuration > Content Analysis > ICAP**).

1. Select **Use the following external request analysis services** to specify ICAP services to handle requests.
2. Select the request analysis service(s) from the Available list. Selected services appear in the Selected - Ordered List.
3. If external request analysis services are used, specify the **Connection Security** that will be used when the proxy sends traffic to the ICAP server.
4. To configure error handling, select one of the following options under **If the request analysis service is not available**:
  - To deny all requests if a communication error occurs, select **Deny the client request**.
  - To allow requests to go through without request analysis scanning, select **Continue without further request processing**. Be advised that this presents a content integrity risk.

**Note:** When the request analysis service is restored, these objects are scanned and served from the cache if they are requested again.

Select **Do not perform request analysis** to bypass ICAP processing for requests.

## Perform Response Analysis

This action specifies the response analysis service or service group that will be used to scan HTTP response data. These services are configured in the Management Console, under **Configuration > Content Analysis > ICAP**).

1. Select **Use the following external response analysis services** to specify ICAP services to handle responses. (These services should be configured in the Management Console, under **Configuration > Content Analysis > ICAP**).
2. Select the response analysis service(s) from the Available list. Selected services appear in the Selected - Ordered List.
3. If external response analysis services are used, specify the **Connection Security** that will be used when the proxy sends traffic to the ICAP server.
4. To configure error handling, select one of the following options under **If the response analysis service is not available**:

## Symantec: A Division of Broadcom

- To deny all responses if a communication error occurs, select **Deny the client response**.
- To allow responses to go through without request analysis scanning, select **Continue without further response processing**. Be advised that this presents a content integrity risk.

Select **Do not perform response analysis** to bypass ICAP processing for responses.

## Permit Authentication Error

After an authentication failure occurs, the authentication error is checked against the list of errors that policy specifies as permitted:

- If the error is not on the list, the transaction terminates.
- If the error is on the list, the transaction proceeds; however, the user is unauthenticated. Because the transaction is not considered authenticated, the `authenticated=yes` condition evaluates to false and the user has no username, group information, or surrogate credentials. Policy that uses the user, group, domain, or attribute conditions does not match.

To permit all types of authentication errors, select **Any errors**.

To specify some types of errors, select **Selected errors**. In the Show: menu, you can filter errors by name, group name, or common error types.

## Permit Authorization Error

After an authorization failure occurs, the authorization error is checked against the list of errors that policy specifies as permitted.

- If the error is not on the list, the transaction is terminated.
- If the error is on the list, the transaction is allowed to proceed and the user is marked as not having authorization data.
- If a user is successfully authenticated but does not have authorization data, the `authenticated=yes` condition evaluates to true and the user has valid authentication credentials.
- The `user.authorization_error=any` condition evaluates to true if user authorization failed and the user object contains username and domain information, but not group or attribute information. As a result, policy using user or domain actions still match, but policy using group or attribute conditions do not.

To permit all types of authorization errors, select **Any errors**.

To specify some types of errors, select **Selected errors**. In the Show: menu, you can filter errors by name, group name, or common error types.

## Reflect IP

Specifies which IP address is used when making connections to upstream hosts. Select one of the following:

- **Do not reflect IP**—Disables the ability to reflect IP addresses; the ProxySG appliance uses the IP address of the interface that the request is sent from.
- **Incoming client IP(IP spoofing)**—Reflects the client IP address.
- **Incoming proxy IP**—Reflects the IP address of where the request arrived.
- **Proxy IP**—Reflects a specific IP address of the appliance; enter the IPv4/IPv6 address in the field.
- **Use global configuration**—Specifies whether to use reflect IP for all services system wide. The default is enabled.

**Note:** To turn on reflect IP addresses for all but a few services, enable this option first, and then write policy to disable reflect IP for the exceptions.

## Request HTTP/2 On Server-Side

Specifies whether the proxy requests HTTP/2 on the server-side connection. Select one of the following:

- **Yes** - Request HTTP/2 on the server-side connection.
- **No** - Do not request HTTP/2 on the server-side connection.
- **Preserve Client-Side Setting** - Request HTTP/2 on the server-side connection only if HTTP/2 is requested on the client-side connection.

## Return Exception

Allows you to select exception types and associate a custom message, if desired. Policy provides built-in exceptions and accepts custom exceptions. To create custom exceptions, see "Defining Exceptions" on page 183.

To select a built-in exception, select one from the drop-down menu.

1. Specify the exception type:
  - Select **Built-in exception** and choose one from the drop-down menu.
  - (If custom exceptions are already created on the appliance) Select **User-defined exception** and choose one from the drop-down menu.
2. (Optional) Select **Force exception even if later policy would allow request** to supersede other policy that applies to this request.
3. (Optional) In the **Details** field, enter a message that is displayed along with the summary and exception ID on the exception page displayed to the user when the exception is returned. Click **Edit** to add ELFF and CPL strings to the exception.

## Return ICAP Feedback

Specifies to display a patience page to the client or employ data trickling if ICAP scanning exceeds the given time duration.

Select either interactive traffic (Web browser based requests) or non-interactive traffic (non-Web browser based clients, such as flash players or automatic updates). Then, configure ICAP feedback settings for the selected traffic:

- **Do not provide feedback during ICAP scanning:** Users do not receive feedback for longer ICAP scans.
- **Provide feedback after:** Specifies how far into the scan to wait before providing feedback (patience page or data trickling) to the client:
  - Enter the number of seconds. The range for the patience page method is 5 to 65535. The range for the trickling methods is 0 to 65535.
  - Specify a feedback method:
    - **Return patience page:** (For interactive traffic only) The ProxySG appliance displays a (customizable) page in users' browsers, informing them that a content scan is in progress.
    - **Trickle object data from start:** The more secure method because most of the object data does not reach the client, pending the result of the content scan.
    - **Trickle object data at end:** The client receives most of the object data, pending the result of the content scan. This method provides the better user experience because they perceive the connection as being almost complete, but it is less secure.

Enter a time value (in seconds) that the appliance waits for content to be serviced from the origin content server before displaying the page that instructs users an ICAP scan is in progress.

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

Patience page management and limitations are described in "Configuring ICAP Feedback" in the *SGOS Administration Guide*.

## Return Redirect

Aborts the current transaction and forces a client request to redirect to a specified URL. For example, used to redirect clients to a changed URL; or redirecting a request to a generic page stating the Internet access policy. Applies only to HTTP transactions.

**Note:** Internet Explorer ignores redirect responses from FTP over HTTP requests. To prevent issues, do not use redirect when `url.scheme=ftp`. If the URL that you are redirecting the browser to also triggers a redirect response due to policy, this could put the browser into an infinite loop.

This object supports the following redirect codes:



- **301** (Moved Permanently)—The ProxySG appliance redirects this and all future requests to the specified URL. Clients with link editing capabilities should automatically re-link references to one or more of the new references returned by the server. Unless indicated, this response is cacheable. For example, an internal resource Web page moved to a new server and all requests must go to that location.
- **302** (Found)—This is the default. The requested resource temporarily resides in a different location. For example, you are replacing a server and clients must go to an alternate location during the downtime. Clients continue to use the original URI for future requests. This response is only cacheable if indicated by a Cache-Control or Expires header field.
- **307** (Temporary Redirect)—Similar to 302; the request connects with using the specified URL, but future requests can still be made from the original URL.

In the **URL** field, enter the redirect destination URL.

## Rewrite Host

Rewrites host component of a URL in HTML, XHTML, JavaScript, Windows Media Player, Flash, and Real Media content. Use this to identify host details in request or response data and replace it with different a host address.

To specify a rewrite:

1. In the **Name** field, enter a name or leave as is to accept to the default.
2. Set the **Scheme** drop-down to either All, Windows Media, Flash Media, or Real Media protocols, depending on the content to be rewritten.

If left at **All**, content is parsed based on the format of that content. For HTML and XHTML content, the HTML parser will examine the content for hosts matching the defined pattern.

If the content is JavaScript, the JavaScript parser analyzes the content. The JavaScript parser includes the following content types:

```
text/javascript
text/x-javascript
text/x-json
application/javascript
application/x-javascript
application/json
```

**Note:** Due to the variable nature of XML and the tags and attributes contained therein, if the content identifies itself as XML, the ProxySG appliance cannot perform the Rewrite Host action.

3. In the **Pattern** field, enter the string to be rewritten.
4. In the **Replacement** field, enter the name the pattern is rewritten to.

## Select Forwarding

Specifies which forwarding host or group, if any, to use; defines behavior if communication between the forwarding and the ProxySG appliance is down.

- To instruct the rule to connect directly without redirecting to a forwarding host or group, select **Do not use Forwarding List**.
- To instruct the rule to redirect to a forwarding host, select **Use Forwarding List** and select a configured forwarding host in the Available field. Under **If no forwarding is available**, select **Deny the request (fail closed)** or **Connect directly (fail open)** to specify whether or not requests bypass the forwarding host.

## Send DNS/RDNS Response Code

Specifies to send out the default response code or a selectable error response code:

- Select **Send Default DNS Response**; optionally, enter a TTL (time to live) value.
- Select **Send Error Response Code** and select a code from the drop-down list.

## Send DNS Response

Specifies which IP address to return for a specified host:

1. In the **Host** field, enter a host name that is returned.
2. To respond with the IP address of the proxy that is forwarding the request, select **Respond with proxy IP**.
3. To respond with a different IP address or addresses:
  - a. Select **Respond with listed IPs**.
  - b. Click **Add**. The Add New IP Address dialog appears.
  - c. Enter an IP address and click **OK**.
  - d. Repeat the previous steps to add more addresses.
4. (Optional) In the **TTL** field, enter a time-to-live value to specify how long the response is cached.

## Send Reverse DNS Response

Specifies which **Host** to return for a reverse DNS response. Optionally, define a time-to-live (**TTL**) value.

## Set ADN Connection DSCP

Specifies DSCP settings for Application Delivery Network (ADN) tunnel connections, which allows you more granular control to regulate WAN traffic. For example, you might not want the DSCP values for packets sent from the OCS and downstream tunnel packets to have the same value.

To specify an ADN connection DSCP value, select one of the following options:

- **Preserve the incoming DSCP value:** This is the default behavior if no other policy is specified. The ADN proxies (branch and concentrators) preserve the inbound packet DSCP values:
  - The client inbound packet and upstream tunnel packet DSCP values are the same.
  - The server inbound packet to the concentrator and downstream tunnel packet DSCP values are the same.
- **DSCP name:** Select one of the standard DSCP values. The behavior is as follows:
  - The DSCP value of the upstream tunnel packets is the selected value until it is reset by an intermediary device.
  - The DSCP value of a downstream packet is the selected value until it is reset by an intermediary device, even if the intermediary device modifies DSCP values of upstream tunnel packets.
- **DSCP value (0-63):** Specify a value if your network uses a numerical DSCP value system,.

**Note:** For more information about DSCP values, see "Managing QoS and Differentiated Services" on page 200.

## Set Apparent Data Type Action

Controls how the Apparent Data Type of content found in an HTTP POST request is handled. Intended for use in reverse proxy deployments, this action matches policy against both single and multi-part files. The allow/deny transaction selection defines how policy reacts to the data types that are selected in the list.

## Set Authorization Refresh Time

Realms that support authorization and authentication separately use the authorization refresh time value to manage the load on the authorization server. They determine authorization data (group membership, attribute values) separately from authentication, allowing the time the authorization data is trusted to be increased or decreased.

For realms that must authenticate the user to determine authorization data, the authorization data is updated only when the user credentials are verified with the authentication server.

## Set Client Certificate Validation

If a client certificate is requested (see **Require/Do Not Require Client Certificate** in the [Static Objects](#) list at the top of this page.), this object specifies whether the requested client certificate is validated using Online Certificate Status Protocol (OCSP) revocation or the local Certificate Revocation List (CRL).

Enable client certificate validation and select the validation method:

- **Use OCSP revocation check if available otherwise use local:** If OCSP is configured, this validation method uses OCSP to check the revocation status of the client certificate. If OCSP is not configured, this method uses on-box

Certificate Revocation List (CRL) to perform the revocation check. This is the default.

- **Use only OCSP revocation check:** Uses only OCSP to check the revocation check of the client certificate.
- **Use only local certificate revocation check:** Uses the CRL configured on the ProxySG appliance to perform the revocation check for a client certificate.
- **Do not check certificate revocation:** Does not check the revocation status of the client certificate; however it still carries out the other certificate validation checks.

Otherwise, disable client certificate validation.

## Set Client Certificate Validation CCL

Specify a client certificate to use for intercepted SSL connections. Otherwise, the appliance uses the default client certificate validation CCL.

**Note:** Create the CCL you want to use for interception before starting this process.

After policy is installed, the specified CCL is used when an intercepted SSL session matches the configured URL.

## Set Client Connection DSCP

Sets the outgoing differentiated service code point (DSCP) value or action for primary client connections (from the server) matching the DSCP value(s) specified in the **Source** of the policy rule:

- **Echo the inbound packet's DSCP value:** Use the same outbound (point of reference, the ProxySG appliance) packet DSCP value as the inbound value.
- **Preserve the incoming DSCP value:** Track the inbound (from the client) DSCP bits on the primary server connection and use that same value when sending packets to outbound to the server. This is valuable for protocols that have multiple client/server connections. For example, FTP control and data connections. The values remain independent for each connection.
- **DSCP name:** Instead of the incoming DSCP, use the DSCP value selected from the drop-down list.
- **DSCP value (0-63):** Instead of the incoming DSCP value, use this non-categorized DSCP value.

For conceptual information about configuring the ProxySG appliance to manipulate traffic based on type of service, see "Managing QoS and Differentiated Services" on page 200.

## Set Client HTTP Compression

Specifies the behavior when the client wants the content in a compression form different from that in the cache:

1. Set the behavior when a client requests compressed content, but only uncompressed content is available:
  - **Compress content before serving it**—The default. Objects are compressed.
  - **Serve uncompressed content**—No compression is applied.
2. Set the behavior when a client requests uncompressed content, but only compressed content is available.
  - **Decompress content before serving it**—The default. Objects are decompressed.
  - **Retrieve uncompressed content from server**—Uncompressed content is requested and retrieved.

For recommended compression configurations, refer to the *SGOS Administration Guide*.

## Set Client Keyring

Select a keyring or keylist that can provide client certificates when requested:

- **Do not send a client certificate**: No keyring or keylist is selected.
- **Send the client certificate in a keyring**: Select a keyring from the **Keyring** list.
- **Select the client certificate to send from a keylist**: Select a keylist from the **Keylist** list. In the **Selector** field, type a substitution variable.
- **Emulate the original client certificate**: Select a keyring from the **Issuer Keyring** list.

All substitution variables are supported; however recommended substitution variables for the **Selector** include `$(user)`, `$(group)`, and `$(server.address)`. For information on substitution variables, refer to "CPL Substitutions" in the *Content Policy Language Reference*.

**Note:** The **Selector** value must match the set of extractor values that are displayed when you run the view command for a keylist. For example, if the Subject.CN in the certificate is set to represent a user name, use the substitution variable `$(user)`, and select the Extractor value `$(Subject.CN)`. If the Extractor value was set to `$(Subject.O)`, no match would be found and a certificate would not be sent. If you are using the `$(group)` selector, you must also create a list of the groups to be included in the `$(group)` substitution variable. See "Creating the Group Log Order List" on page 148.

## Set Content Security Scanning

This action specifies the Content Security scanning level for a Web response, and is applicable only if you have added the Content Security policy layer. This option allows you to create exemptions to the scanning behavior specified in the Content Security layer. For example, you can select a different protection level from the one specified in the Content Security layer, or exempt the rule entirely from Content Security (responses will not be scanned).

The following options are available:

- Use protection level set by Content Policy Layer
- Use Recommended protection level
- Use Strong protection level
- Use Maximum protection level
- Exempt From Content Security

## Set Credential Refresh Time

The credential refresh time value determines how long a cached username and password is trusted. After that time has expired, new transactions that require credential authentication result in a request to the authentication server. A password different than the cached password also results in a request to the authentication server.

This value can be only valid for realms that cache the username and password on the proxy and realms that use Basic username and password credentials: LDAP, RADIUS, XML, IWA (with Basic credentials), SiteMinder, and COREid.

## Set Effective Client IP

Specify one or more request header substitutions to use to look up the effective client IP address. If the appliance is able to extract the effective client IP address, it is used whenever it is specified in policy.

If you select or enter multiple substitutions, policy evaluates them in order of preference and uses the first substitution that evaluates to a valid IP address.

To specify one or more substitutions, select **Use the first valid substitution below as the effective IP address**. Then, select available substitutions or add a new one using the + button. The following request header substitutions are available by default:

- `$(request.header.X-Forwarded-For)` sets the address in the X-Forwarded-For header field as the client IP address.
- `$(request.x_header.X-Client-IP)` sets the address in the X-Client-IP header field as the client IP address.
- `$(request.header.Client-IP)` sets the address in the Client-IP header field as the client IP address.

To use the original client address, select **Use the original client address as the effective client IP address**.

## Set Effective Threat Risk Level

You can specify a threat risk level based on a policy condition to override the threat risk level that WebPulse returns for a request. This object is available in the DNS Access, SSL Intercept, Web Access, Web Authentication, Web Content, and Forwarding layers.

To set the effective threat risk level, enter a value to assign a specific level. See "Threat Risk Levels" on page 81 for a description of the level. You can override the risk level with a 0 in addition to the values described in the table.

## Set Force Cache Reasons

Specifies one or more reasons to force the caching of objects that may not otherwise be cached. For example, you can force objects to be cached when the response header contains set-cookie, no-store, and/or private.

## Set FTP Connection

For an outgoing request over FTP, specifies whether the FTP connection should be made immediately or deferred, if possible. The benefit of deferring connections is that requests for previously cached content can be served without contacting the origin server, which reduces the FTP load on that server.

## Set Geolocation Restriction

Tests for IP addresses in specified geographical locations. During a connection attempt to a domain, the DNS server returns one or more IP addresses associated with the domain. The appliance tests each IP address against policy and skips any that are not allowed.

For detailed information on this policy gesture and usage examples, refer to the `supplier.allowed_countries()` property in the *Content Policy Language Reference*.

Select one of the following:

- **Create a new policy for all locations** - Set the restriction to:
  - **Allow all locations** - Allow connections to IP addresses in all countries that are not specified in geolocation policy. This is the default setting.
  - **Deny all locations** - Deny connections to IP addresses in all countries that are not specified in geolocation policy.
- **Create a new policy for a list of allowed location(s)** - Create policy for one or more selected locations.
- **Modify the current policy for a list of selected location(s)** - Modify the existing policy for one or more selected locations.

## Set HTTP Compression Level

Allows you to set the level of compression to low, medium, or high. When configuring, consider that a higher compression level consumes more CPU resource.

You can control the compression level based on any transaction condition (such as the client IP address, the hostname, request/response headers, and the like).

**Note:** If you enable HTTP Compression using the VPM but do not specify a HTTP Compression Level, by default the level is Low.

Specify an HTTP compression level:

- **Low**—Equivalent to compression level 1.
- **Medium**—Equivalent to compression level 6.
- **High**—Equivalent to compression level 9.

## Set HTTP Request Max Body Size

Specifies a limit (in bytes) for the size of body content for HTTP requests. When the limit is exceeded, the request is denied.

## Set HTTP/2 Client Max Concurrent Streams

Specify the maximum number of concurrent HTTP/2 streams that the client may initiate on the current client connection.

## Set IP Address For Authentication

Some Application Delivery Network (ADN) configurations in proxy chain deployments mask the source IP address of the request. Policy to set the IP address for authentication is required so that Windows Single Sign On (SSO), Novell SSO, and policy substitution realms can authenticate users.

1. Click **Edit** to add ELFF and CPL strings.
2. From the **IP Address** drop-down list, select a substitution string. For example, `$(request.header.Client-IP)` sets the address for authentication to the address received from the HTTP Client-IP header.

Refer to the *SGOS Administration Guide* for more information about this type of authentication.

## Set Server Certificate Validation

Disabled by default; enable the feature by selecting **Enable server certificate validation**.

When the feature is enabled, you can mimic the overrides supported by browsers by ignoring one or more failure types:

- **Ignore hostname mismatch**: Ignores the comparison of hostname in URL and certificate (intercepted connections only).
- **Ignore expiration**: Ignores the verification of certificate dates. (Not Before and Not After date fields.)
- **Ignore untrusted issuer**: Ignores the verification of issuer signature.

When the feature is enabled, select the server certificate validation method:

- **Use OCSP revocation check if available otherwise use local**: If OCSP is configured, this validation method uses OCSP to check the revocation status of the server certificate. If OCSP is not configured, this method uses on-box Certificate Revocation List (CRL) to check the certificate revocation status. This is the default.
- **Use only OCSP revocation check**: Uses only OCSP to check the revocation status of the server certificate.
- **Use only local certificate revocation check**: Uses the CRL configured on the appliance to perform the revocation check for a server certificate.



- **Do not check certificate revocation:** Does not check the revocation status of the server certificate; however it still carries out the other certificate validation checks.

## Set Server Certificate Validation CCL

Allows you to configure the CA Certificate List (CCL) to use for a specific IP address or hostname. When this object is not used, the default server certificate validation CCL is applied.

**Note:** Create the CCL you want to use for interception before starting this process.

Select the CCL to use when the policy applies. When an intercepted SSL session matches the configured URL, the validate CCL policy rule is applied to those sessions.

## Set Server Connection DSCP

Identical to "Set Client Connection DSCP " on page 116, but applies to using the DSCP values or bits from client connections to server connections.

## Set Server HTTP Compression

Enables or disables HTTP compression:

- **Disable HTTP compression**—Objects are not compressed.
- **Use client HTTP compression options**—Default to the type of content requested by the client.
- **Always request HTTP compression**—Force clients to always request compressed content.

For recommended compression configurations, refer to the *SGOS Administration Guide*.

## Set Server URL DNS Lookup

Sets the IP connection type preference for resolving server URL host names. For example, if you have a known list of servers that are on IPv6 networks, you can avoid timeouts and unnecessary queries by creating policy to look up these host names on IPv6 DNS servers only. Select one of the following:

- **Look up only IPv4 addresses**—Uses configured IPv4 DNS servers for all DNS lookups on the specified server.
- **Look up only IPv6 addresses**—Uses configured IPv6 DNS servers for all DNS lookups on the specified server.
- **Prefer IPv4 over IPv6 addresses**—First uses configured IPv4 DNS servers; if that query fails, uses configured IPv6 DNS servers.
- **Prefer IPv6 over IPv4 addresses**—First uses configured IPv6 DNS servers; if that query fails, uses configured IPv4 DNS servers.

## Set SOCKS Acceleration

(Deprecated) Specifies whether or not accelerate SOCKS requests:

- **Automatically:** Accelerates SOCKS requests automatically, based on the destination port receiving the connection.
- **Do not accelerate:** Never accelerate SOCKS requests matched by this rule.
- **Accelerate via:** Accelerate SOCKS requests using the specified transport method.

## Set SOCKS Compression

(Deprecated) Specifies which SOCKS gateway, if any, to use; defines behavior if communication between the SOCKS gateway and the ProxySG appliance is down.

- To instruct the rule to connect directly without routing through a SOCKS service, select **Do not use SOCKS gateway**.
- To instruct the rule to connect through a SOCKS gateway, select **Use SOCKS Gateway** and select an installed SOCKS service from the drop-down list.

In the **If no SOCKS gateway is available** field, select **Deny the request or Connect directly**, which allows requests to bypass the SOCKS service.

## Set Streaming Max Bitrate

Specifies the maximum bitrate, in kilobits per second, of requested streaming media. If a request exceeds this rule, the request is denied.

## Set Streaming Transport

Specifies which streaming transport method the rule uses.

- **Auto**—Connects using the transport method used by the client.
- **HTTP**—Streaming over HTTP.
- **TCP**—Streaming over TCP.

## Set Surrogate Refresh Time

Specifies how long surrogate credentials are trusted in a particular realm.

## Set TTL

Specifies the time-to-live (TTL) an object is stored in the ProxySG appliance. In the **TTL** field, enter the amount of time in seconds.

## SSL Interception

Allows the ProxySG appliance to act as a forward proxy for HTTPS traffic. Provides performance gains and security (authentication, content filtering, anti-virus scanning) for HTTPS traffic before it is delivered to clients. This object allows HTTPS content to be intercepted and examined.

## Strip Active Content

Strips HTTP tags from pages with the specified active content types. For each item selected for removal, you can also create a custom message that is displayed to the user.

**Note:** Pages served over an HTTPS tunneled connection are encrypted, so the content cannot be modified. See "Stripping or Replacing Active Content" on page 179 for detailed information about the different types of active content.

By default, all active content types (applet, embed, object, and script) are selected to be stripped. The default replacement text is "Active content removed".

### Exempting the Appliance

Stripping active content might interfere with Web applications deployed on your intranet. For example, if you create a policy rule that removes Java applets, and the destination defined in the rule contains an IP address of a ProxySG appliance functioning as a proxy, the policy rule disables the Management Console because the console comprises Java applets.

To prevent this, for each appliance functioning as a forward proxy, create a rule that exempts the IP address of the appliance from the stripping action.

1. Add a **Destination IP Address & Subnet** object and specify the appliance IP address.
2. Select the object and select **Negate** from the drop-down list.
3. In the Action column, add a **Strip Active Content** object that strips applets.

## Suppress Headers

Specifies one or more standard headers that are suppressed (not transmitted) on the outbound request, the outbound response, or both:

1. Select **Request**, **Response**, or **Both**. The valid headers vary for requests and responses. Both displays a small subset of headers valid for requests and responses.
2. Select one or more header types from the list.

## Time Quota

Restrict the amount of time (quota amount) that users can spend on the Internet or Internet resource during a specific period of time (quota period). You can optionally display an exception page to users if they reach a specific percentage of the quota.

If more than one time quota matches a given transaction, only the last matched applies.

**Tip:** Before you can create quota policy, you must enable the quota library in the CLI. Issue the following command: `#(config)policy quota`

1. Specify the quota period and amount:
  - a. **Quota period:** Define the length of time against which to track the quota. At the end of the quota period, time tracking restarts. The quota period you select determines the units of measurement available for the quota amount. For example, to create a daily quota, select **Daily**. Selections for hours and minutes are available for the quota amount.
  - b. **Quota amount:** Specify the maximum for the quota. For example, to specify a 90-minute quota, select 1 for **Hour** and 30 for **Minutes**.
2. (Optional) To display an exception page to users when they reach a certain percentage of the quota, select **Display warning message**. Select a value from the menu to indicate the percentage.

For example, specifying a 75% threshold for the 90-minute daily quota means that users receive an exception page when they reach 67 minutes within the 24-hour quota period.

**Note:** The threshold is checked only at the beginning of a transaction; thus, if a user reaches the threshold during a transaction, access is still permitted and the user does not receive an exception page.

## Volume Quota

Restrict users' Internet or Internet resource usage (volume quota) during a specific period of time (quota period). You can optionally display an exception page to users if they reach a specific percentage of the quota.

If more than one volume quota matches a given transaction, only the last matched applies.

**Tip:** Before you can create quota policy, you must enable the quota library in the CLI. Issue the following command: `#(config)policy quota`

1. Specify the quota period and amount:
  - a. **Quota period:** Define the length of time against which to track the quota. At the end of the quota period, usage tracking restarts. For example, to create a weekly quota, select **Weekly**.
  - b. **Quota amount:** Specify the maximum for the quota.
2. (Optional) To display an exception page to users when they reach a certain percentage of the quota, select **Display warning message**. Select a value from the menu to indicate the percentage.

For example, specifying a 75% threshold for the 2500 MB weekly quota means that users receive an exception page when they reach 1750 MB within the week.

**Note:** The threshold is checked only at the beginning of a transaction; thus, if a user reaches the threshold during a transaction, access is still permitted and the user does not receive an exception page.

The Web Isolation settings are set to the cloud-based service defaults, but you can use the `#(config isolation)` CLI commands to configure a custom isolation service; refer to the *Command Line Interface Reference* and [KB 201609](#) for details.

# Action Column/Policy Layer Matrix

**Action** column objects are available in the following policy layers:

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Accept HTTP/2 Client-Side Connections									X			
Add Default Group								X				
ADN Server Optimization												X
Allow							X		X			
Allow Access to Server											X	
Allow Content From Origin Server												X
Allow DNS From Upstream Server				X								
Allow Read-Only Access		X										
Allow Read-Write Access		X										
Always Verify									X	X	X	
Authenticate	X		X		X			X				
Authenticate Guest								X				
Authentication Charset								X				

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Block/Do Not Block PopUp Ads									X			
Bypass Cache									X		X	
Bypass DNS Cache				X								
Check/Do Not Check Authorization									X	X	X	
Client and Server Certificate Exceptions												
Combined Action Object		X	X	X		X	X	X	X		X	X
Connect Using ADN When Possible/Do Not Connect Using ADN												X
Control Request/Response Header									X		X (Request Header only)	
Deny	X	X					X	X	X		X	
Deny (Content Filter)							X		X		X	
Disable/Do Not Disable Fast-Caching in Windows Media Client									X		X	

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Disable SSL Detection									X		X	
Disable SSL Interception						X						
Do Not Authenticate	X				X			X				
Do Not Authenticate (Forward Credentials)								X				
Do Not Bypass Cache									X		X	
Do Not Bypass DNS Cache				X								
Do Not Cache										X		
Do Not Duplicate Proxy Credentials Upstream								X				
Do not Preserve Untrusted Issuer						X						
Do Not Use Kerberos Constrained Delegation								X				
Duplicate Proxy Credentials Upstream								X				
Dynamic Categorization										X		



Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Enable/Disable DNS Imputing				X								
Enable/Disable ICAP Mirroring for response modification									X			
Enable/Disable Pipelining										X		
Enable Encrypted Tap							X					
Enable SSL Interception						X						
Exempt from Default Security									X			
Force Authenticate	X		X		X			X				
Force Deny		X					X		X			
Force Deny (Content Filter)							X		X			
Force/Do Not Force IWA for Server Auth									X		X	
Integrate/Do Not Integrate New Hosts												X
Kerberos Constrained Delegation								X				

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Log out/Do Not Log out Other Users With Same IP		X							X			
Log out/ Do Not Log out User		X							X			
Log out/ Do Not Log out User's Other Sessions		X							X			
Manage Bandwidth				X					X	X	X	X
Mark/Do Not Mark As Advertisement										X		
Modify Access Logging									X	X	X	
Notify User									X			
Override Access Log Field									X	X	X	
Perform Request Analysis									X	X	X	
Perform Response Analysis										X		
Permit Authentication Error								X				
Permit Authorization Error								X				

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Preserve Untrusted Issuer						X						
Reflect IP				X					X		X	X
Require/Do Not Require Client Certificate							X					
Return Exception							X		X			
Return ICAP Feedback									X			
Return Redirect								X			X	
Rewrite Host									X		X	
Select Forwarding												X
Send Direct												X
Send DNS/RDNS Response Code				X								
Send DNS Response				X								
Send Reverse DNS Response				X								
Serve Content Only From Cache												X
Serve DNS Only From Cache				X								

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Set ADN Connection DSCP												X
Set Apparent Data Type Action									X		X	
Set Attack Detection Failure Weight									X			
Set Authorization Refresh Time		X							X			
Set Client Certificate Validation							X		X			
Set Client Certificate Validation CCL							X					X
Set Client Connection DSCP				X					X		X	
Set Client HTTP Compression									X	X		
Set Client Keyring							X					
Set Credential Refresh Time		X							X			
Set Effective Client IP									X			
Set Effective Threat Risk Level				X		X			X		X	X

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Set Force Cache Reasons										X		
Set FTP Connection									X		X	
Set Geolocation Restriction							X		X	X		X
Set HTTP Compression Level									X	X		
Set HTTP Request Max Body Size									X		X	
Set IP Address For Authentication								X				
Set Malware Scanning										X		
Set Server Certificate Validation							X		X			
Set Server Certificate Validation CCL						X						X
Set Server Connection DSCP				X					X	X	X	X
Set Server HTTP Compression									X	X	X	
Set Server URL DNS Lookup									X		X	X

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Set SOCKS Acceleration									X		X	
Set SOCKS Gateway Compression												X
Set Streaming Max Bitrate									X		X	
Set Streaming Transport												X
Set Surrogate Refresh Time		X							X			
Set TTL										X		
Strip Active Content									X			
Support/Do Not Support Persistent Client Requests									X		X	
Support/Do Not Support Persistent Server Requests									X	X		
Suppress Headers									X		X	
Time Quota									X			
Trust/Do Not Trust Destination IP									X		X	
Use Default Caching												

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request	Forwarding
Use Default Setting for Preserve Untrusted Issuer						X				X		
Use Default Verification									X	X	X	
Volume Quota									X			

# Banner Objects

An admin login banner object specifies the content of the notice and consent banner displayed before the user may access the Management Console; see the "Time Column/Policy Layer Matrix" on page 92 for details.

For details on configuring the banner, refer to the *Notice and Consent Banner WebGuide*:

<https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/web-and-network-security/proxysg/7-1/notice-and-consent-banner-config.html>

**Caution:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define a banner object name.

## Banner Attribute

To specify the banner text and/or image, do one or both of the following:

- Click **Browse** to select an image. Supported file types are .jpg, .gif, and .png.
- Enter text in the **Banner Text** field. There is a 2000 character limit.



# Banner Column/Policy Layer Matrix

**Banner** column objects are available in the following policy layers:

Object	Admin Authentication	Admin Access	Admin Login Banner	DNS Access	SOCKS Authentication	SSL Intercept	SSL Access	Web Authentication	Web Access	Web Content	Web Request Layer	Forwarding
Banner			X									

# Track Object

A track object defines the parameters for tracking and tracing traffic. Not all policy layers contain the same Track objects; see the "Track Column/Policy Layer Matrix" on page 141 for details.

**Caution:** Because of character limitations required by the generated CPL, only alphanumeric, underscore, dash, ampersand, period, or forward slash characters can be used to define a track object name.

## Combined Track Object

An object that combines multiple tracking options. See "Combined Objects " on page 142.

## E-mail

Configure email notifications.

1. Select the recipients for the email:
  - **Default** - Send email to the global recipient list. This is the default selection.
  - **Custom** - Send email to one or more existing recipient lists. If there are no existing email lists, click **Add Email List**.
    - a. Enter a list name.
    - b. For each recipient in the list, specify a valid email address and click **+**.
    - c. Click **OK** to save the list.
    - d. Repeat the previous steps to add more email lists.
2. Select the email lists for the object.
3. Enter an email **Subject** and **Message**.

## Event Log

Configure details for event log entries.

1. In the **Details** field, enter text that you want to appear with the event log entry.
2. (Optional) Add substitution variables. The substitution variables instruct the ProxySG appliance to append specific information to the tracking object. The variables are categorized alphabetically by prefix (when available).

- a. From the **Category** drop-down list, select a category to narrow the view to a subset of variables.
- b. Under **Display Options**, filter variables by ELFF or CPL. By default, all variables are listed.
- c. Select variables and click **Insert**.

## Policy ID

Set a policy ID for a rule. The ID will be visible in all policy traces and access logs associated with requests matching the rule. This is very useful for identifying how frequently certain rules are used, and can aid in improving policy.

To view the ID in access logs, include the `x-bluecoat-reference-id` field in the access log format.

## SNMP

Configure SNMP messages.

1. In the **Message Text** field, enter the SNMP message.
2. (Optional) Add substitution variables. The substitution variables instruct the ProxySG appliance to append specific information to the tracking object. The variables are categorized alphabetically by prefix (when available).
  - a. From the **Category** drop-down list, select a category to narrow the view to a subset of variables.
  - b. Under **Display Options**, filter variables by ELFF or CPL. By default, all variables are listed.
  - c. Select variables and click **Insert**.

## Trace

Specifies rule and Web traffic tracing.

Select **Trace Level** and select one of the following trace options:

- **Trace Disabled:** (Default) Tracing is fully disabled.
- **Trace Enabled:** Tracing is fully enabled.

Traces are logged to a default location on the appliance (`default.html`), but you can enter a custom location for any trace produced by the current transaction. To specify a location, select **Trace File** and enter a path in the field.

If a trace destination is configured in multiple layers, the actual trace destination value displayed is the one specified in the last layer that had a rule evaluated (which has a destination property configured).

Consider the following example of generated CPL:

```
<Proxy>
url.domain=aol.com trace.request(yes) trace.destination("aol_tracing.html")
url.domain=msn.com trace.request(yes) trace.destination("msn_tracing.html")
```

## Symantec: A Division of Broadcom

<Proxy>

```
client.address=10.10.10.1 trace.request(yes)
```

The resulting actions are:

- Requests to the aol.com domain are logged to aol\_tracing.html.
- Requests to the msn.com domain are logged to msn\_tracing.html.
- Requests from the client with the IP of 10.10.10.1 are logged to the default location of default.html.

**Note:** After using a trace to troubleshoot, remove the trace to reduce log space.

The **Trace File** option can be used in conjunction or separately from the **Trace Level** option.

Access the default path of the trace file through one of the following URLs:

- If the Management Console secure mode is enabled (the default on a new or upgraded system):

[https://IP\\_address:8082/Policy/Trace/default\\_trace.html](https://IP_address:8082/Policy/Trace/default_trace.html)

- If the Management Console is deployed in non-secure mode:

[http://IP\\_address:8081/Policy/Trace/default\\_trace.html](http://IP_address:8081/Policy/Trace/default_trace.html)

# Track Column/Policy Layer Matrix

Track column objects are available in the following policy layers:

Object	Admin Authenticat ion	Admi n Acce ss	Admi n Login Bann er	DNS Acce ss	SOCKS Authenticat ion	SSL Interce pt	SSL Acce ss	Web Authenticat ion	Web Acce ss	Web Conte nt	Web Requ est	Forwardi ng
Combin ed Track Object		X		X	X	X	X	X	X	X	X	X
Email	X	X			X	X	X	X	X	X	X	X
Event Log		X		X		X	X		X	X	X	
Policy ID	X	X			X	X	X	X	X	X	X	X
SNMP		X		X		X	X	X	X	X	X	
Trace	X	X		X	X	X	X	X	X	X	X	X

# Combined Objects

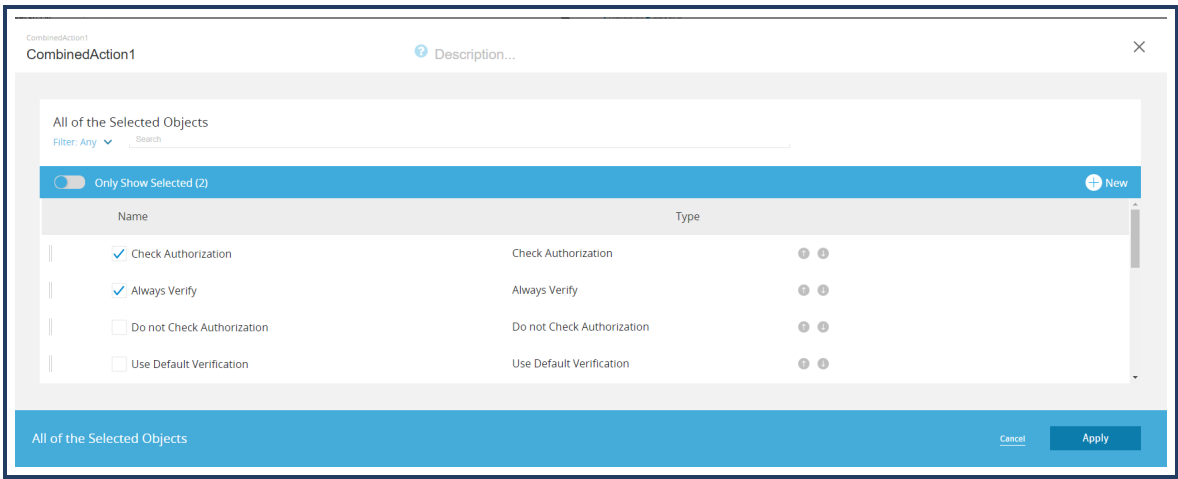
You can combine most object types to select multiple objects, thus creating more complex tools. There are two uses for combined conditions: lists and multiple object types. The **Negate** option exempts the objects in the list.

## Example: Force Authorization

Create a rule that forces authorization and sends the request to an ICAP service for content scanning.

1. In the Set Action Object dialog, click **Add a new object** and select **Combined Action Object**.
2. (Recommended) Specify a name and a description that explains the purpose of the combined object.
3. Select the **Check Authorization** and **Always Verify** objects.
4. Click **Apply**. The combined object appears as a separate, selectable object.
5. Select the new combined object and click **Set**. The object is now part of the rule.

Based on the other parameters specified in the rule, all requests are forced to an upstream server for authorization and the Web responses are subject to content scanning through the ICAP service.

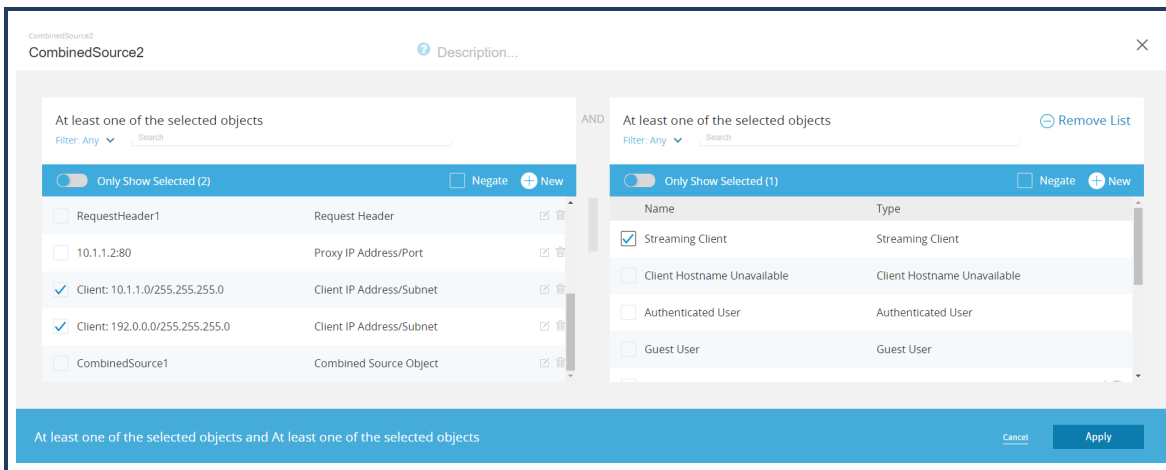


## Example: Match Against Client IP Address and Streaming Client

Create a rule that matches against one of the specified client IP addresses and one of the streaming client user agents.

1. In the Set Source Object dialog, click **Add a new object** and select **Combined Source Object**.
2. (Recommended) Specify a name and a description that explains the purpose of the combined object.
3. Select the existing **Client IP Address/Subnet** objects.
4. Select the **Streaming Client** object.

5. Click **Apply**. The combined object appears as a separate, selectable object.
6. Select the new combined object and click **Set**. The object is now part of the rule.



**Note:** The VPM displays various warning messages if you attempt to add objects that creates an invalid combined object; however, it is possible to add a combined object to another combined object, even if doing so presents duplication of simple object definitions without receiving validation warnings. For example, the contents of a child combined object might have already been included either within the parent combined object directly, or indirectly within other child combined objects. This is allowed because of the complexity that some combined objects and policies can achieve.

## View and Manage All Objects

This section describes how to use the All Objects dialog to view and manage every VPM object.

You can view a list of all objects—both static and user-defined—that currently exist across all layers and columns. To view all configured VPM objects, select **Operations > View All Objects**. The dialog shows the list in alphabetical order. To reduce the number of results, use the search field or filter by name or type. Selecting **Show only unused objects** displays all static and user-defined objects that are not currently used in any policy layer.

The All Objects dialog also allows you to create objects. Once an object is created, it appears in the list. When creating or editing policy layers, the objects are available to add to rules.

To create an object, click **Add a new object** and select the object type from the list. Define the object as required. See "VPM Object Reference" on page 52 for details.

**Note:** When creating Combined Objects, not all objects that appear in the left column are valid for more than one policy layer type. For example, the **User** object is only valid in the **Web Access Layer > Source** column. If you attempt to add an object that is not valid, a dialog appears with that information.

**Caution:** You cannot delete an object that is currently part of an installed policy or combined object. On the drop-down menu within the rule, select **View Occurrences**. The VPM displays a dialog that shows the other layers and rules that include the object.



# Creating Categories

This feature allows you create the content filter URL categories that can be used in the Category object. The Destination column in the DNS Access, Web Access, Web Authentication, and Web Content policy layers contain the Category object. Similarly, categories created in the **Category** object (see "Request URL Category" on page 77) appear in this dialog and can be edited.

Create a category:

1. In the VPM, select **Configuration > Categories**.

The Edit Categories dialog displays categories that exist currently on the appliance:

- **Policy:** Categories defined in the VPM.
- **Blue Coat:** Blue Coat (WebFilter or Intelligence Services) categories, if the provider is enabled and the license is valid.
- **System:** System-defined statuses:
  - none: The request is uncategorized by all enabled content filter providers. If even one content filter provider returns a category for the requested site, policy rules containing a \*.category=none condition will not match.
  - pending: The categorization request has not been processed or is not complete.
  - unavailable: A content filter provider is selected in configuration, but an error occurs in determining the category. Other categories can still be assigned directly by policy. This categorization might be a result of a missing database.
  - unlicensed: A content filter provider license is expired. When this status is true, the unavailable status is also true.

2. Click **Add Category**.
3. In the Add Category dialog appears, enter URLs appropriate for the content filter category you are creating; click **Apply**. The category appears in the **Policy** list.
4. Click **Apply** in the Edit Categories dialog.

**Note:** If other administrators have access to the ProxySG appliance through other workstations and are creating categories either through VPM or with inline commands, consider that newly-created or edited categories are not synchronized until the policy is installed. When the policy is installed with VPM, the categories are refreshed. If too many categories are created at the same time and confusion occurs, select the **Operations > Revert to Existing Policy** option to restore the policy to the previous state and reconfigure categories.

## Refreshing Policy

Between occurrences when either VPM is closed and reopened, or policy is installed, the VPM does not recognize changes to VPM-managed policy that were made on the ProxySG appliance through another method. For example:

- Another administrator opens a separate VPM to make changes.
- Another administrator edits the local or central policy file through the serial console.
- Another administrator makes edits the local or central policy file.
- A new content filter database is downloaded automatically and the new update contains category changes.
- A new content filter database is downloaded manually by an administrator.

## Creating Subject Directory Attribute Objects

The subject field of an SSL certificate can contain attributes and the ProxySG appliance can match policy against these attributes.

To manage subject directory attributes:

1. In the VPM, select **Configuration > Subject Directory Attributes**. The Edit Subject Directory Attributes dialog appears.
2. Click **Add Attribute**.
3. In the Add Attribute dialog that appears, enter a string value to match (such as 2.16.840.1.101.2.1.5.61) in the **OID** field.
4. Click **Apply**.
5. Click **Apply** in the Edit Subject Directory Attributes dialog.

## Restricting DNS Lookups

This section discusses DNS lookup restrictions and describes how to create a list.

### About DNS Lookup Restriction

The DNS lookup restriction list is a list of domain names that apply globally, regardless of policy layer definitions. Once a domain name is added to the list, DNS lookup requests do not occur for that domain name while policy is evaluated. For more detailed information about using DNS lookups, refer to the *Content Policy Language Reference*.

### Creating the DNS Lookup Restriction List

The list is created from the Configuration menu. This prevents the ProxySG appliance from performing DNS lookups of addresses in the list while evaluating policy.

To create the DNS lookup restriction list:

1. Select **Configuration > DNS Lookup Restrictions**. The Set DNS lookup restrictions dialog appears.
2. Specify DNS lookup restrictions (by default, no domain names are restricted):
  - To restrict every domain name, select **All**.
  - To add specific domain names, select **Listed** and add domain names to the Host Patterns field.
3. Specify DNS lookup exceptions (by default, no domain names are excepted):
  - To except every domain name, select **All**.
  - To add specific domain names, select **Listed** and add domain names to the Host Patterns field.
4. Click **Apply** to save changes.

## Restricting Reverse DNS Lookups

This section discusses reverse DNS lookup restrictions and describes how to create a list.

### About Reverse DNS Lookup Restriction

The Reverse DNS lookup restriction list is a list of subnets that apply globally, regardless of policy layer definitions. Once a subnet is added to the list, the ProxySG appliance does not perform a reverse lookup of addresses on that subnet during policy evaluation. For more detailed information about using reverse DNS lookups, refer to Content Policy Language Reference.

### Creating the Reverse DNS Lookup Restriction List

The list is created from the Configuration menu. This prevents the ProxySG appliance from performing reverse DNS lookups of addresses in the list while evaluating policy.

To create the reverse DNS lookup restriction list:

1. Select **Configuration > Reverse DNS Lookup Restrictions**. The Set Reverse DNS lookup restrictions dialog appears.
2. Specify reverse DNS lookup restrictions (by default, no domain names are restricted):
  - To restrict every domain name, select **All**.
  - To add specific domain names, select **Listed** and add domain names to the Subnets field.
3. Specify reverse DNS lookup exceptions (by default, no domain names are excepted):
  - To except every domain name, select **All**.
  - To add specific domain names, select **Listed** and add domain names to the Subnets field.
4. Click **Apply** to save changes.

## Setting the Group Log Order

This section discusses the group log order and describes how to create a list.

### About the Group Log Order

The Group Log Order object allows you to establish the order group data appears in the access logs. For more detailed information about using group log ordering, refer to the *Content Policy Language Reference*.

### Creating the Group Log Order List

To create the group log order list:

1. Select **Configuration > Group Log Order**; the Set Group Log Order dialog appears.
2. Click **Add Group**.
3. In the Group dialog, select an existing authentication realm.
4. Click **Apply**. Repeat as required to add more groups.
5. Select groups on the Add Group dialog to make them available for ordering, and then click **Apply**.
6. On the Set Group Log Order dialog, drag groups to order them on the list.
7. Click **Apply** to save changes.

# Managing Policy Layers, Rules, and Files

Refer to the following sections to learn about managing policy layers, rules, and files.

- "How Policy Layers, Rules, and Files Interact" on the next page
- "Managing Policy" on page 156
- "Installing VPM-Created Policy Files" on page 157
- Troubleshooting Policy Problems

# How Policy Layers, Rules, and Files Interact

The following critical points discuss the behaviors and priorities of policy rules, layers, and files:

- Rules in different policy layers of the same type work together, and the order of policy layers is important.
- The order of policy layers of different types is important.
- The order of rules in a policy layer is important.
- Policy created in VPM is saved in a file on the appliance; the state of the VPM user interface is also stored as an XML file on the appliance.

**Note:** These files are stored only if the policy is installed without any errors.

- How the appliance evaluates those rules in relation to policy layers that exist in the central and local policy files is important. For more information, see "Managing Policy Files" on page 6.

## How VPM Layers Relate to CPL Layers

VPM generates CPL in various layers, but the concept of layers presented in VPM is slightly different. VPM provides policy layers for special purposes. For example, Web Authentication and Web Authorization, which both generate CPL <proxy> layers. This minimizes timing conflicts by restricting the choices of conditions and properties to those compatible timing requirements. The following table summarizes the purpose of VPM layers and the underlying CPL.

### VPM-Generated CPL Layers

VPM Layer	Policy Purpose	CPL Layer
Access Security Policy	Pre-configured policy that allows you to block or monitor transactions based on Symantec's URL Threat Risk Levels and URL categories.  For details on the Access Policy, refer to the <i>SGOS Administration Guide</i> and the <i>ProxySG Security Best Practices</i> document.	<Proxy>
Admin Access	Determines who can access the appliance to perform administration tasks.	<Admin>
Admin Authentication	Determines how administrators accessing ProxySG appliance must authenticate.	<Admin>
Admin Login Banner	Configure a notice and consent banner for the Management Console.	<Admin>

VPM Layer	Policy Purpose	CPL Layer
Content Security Policy	Pre-configured policy that allows you to scan traffic based on Symantec's current content scanning recommendations and set failover and security options for the ICAP service.  For details on the Access Policy, refer to the <i>SGOS Administration Guide</i> and the <i>ProxySG Security Best Practices</i> document.	<Proxy>, <Cache>
DNS Access	Determines how the appliance processes DNS requests.	<DNS>
Forwarding	Determine forwarding hosts and methods.	<Forward>
SOCKS Authentication	Determines the method of authentication for accessing the proxy through SOCKS.	<Proxy>
SSL Intercept	Determines whether to tunnel or intercept HTTPS traffic.	<SSL-Intercept>
SSL Access	Determines the allow/deny actions for HTTPS traffic.	<SSL>
Web Access	Determines what clients can and cannot access on the Web and specifies any restrictions that apply.	<Proxy>
Web Authentication	Determines whether user clients that access the proxy or the Web must authenticate.	<Proxy>
Web Content	Determines caching behavior, such as verification and Content Analysis redirection.	<Cache>
Web Request	Determine if a request is denied before reaching the OCS.	<Proxy>

**Note:** VPM currently does not support the <Exception> layer.

See "Composing CPL Directly in the VPM" on page 173.

## Ordering Rules in a Policy Layer

The appliance evaluates the rules in the order in which they are listed in a policy layer. When it finds a rule that applies to the situation, it skips the remaining rules in the policy layer and goes on to the next policy layer.

Consider the following simple example. Assume that a company has a policy that prohibits everyone from accessing the Web. This is a policy that is easy to create with a Web Access Layer rule.

There are, however, likely to be exceptions to such a broad policy. For example, you require the manager of the purchasing department to be able to access the Web sites of suppliers. Members of the sales department need to access their customer websites. Creating Web Access Layer rules for both these situations is also simple. But if you put all these rules in a single policy layer, then the rule prohibiting access to everyone must be ordered last, or the other two rules are not applied.

**Tip:** Always go from the specific to the general.

## Using Policy Layers of the Same Type

Because the appliance skips the remaining rules in a policy layer as soon as it finds one that meets the condition, multiple policy layers and a combination of rules might be required to accomplish a task.

Consider the following example. A company does not want to prohibit its employees from accessing the Web, but it does not want them to abuse the privilege. To this end, the company wants employees who access the Web to authenticate when they do so; that is, enter a username and password. So the company creates a Web Authentication Layer with a rule that states:

If anyone from anywhere in the company sends a request to a URL on the Web, authenticate the client before granting access.

The company also allows members of the group Sales to access various sports Web sites only during non-work hours. Given the Web Authentication Layer rule above, these people must authenticate when they do this. But the company feels that it is not important for people going to these sites after hours to authenticate. So the company creates the following Web Access Layer rule:

- Grant Sales personnel access to sports websites from 5:00 PM to midnight.

But there are additional issues. Some members of the sales department spend a lot of time watching game highlights on video clips, and this takes up a lot of bandwidth. At the same time, a lot of customers access the company website in the evening (during non-work hours), so internal bandwidth should remain manageable. The company, therefore, limits the bandwidth available to the people in the Sales department with a Web Access Layer rule that is identical to the one above in all respects except for the action:

- Grant Sales personnel access to sports websites from 5:00 PM to midnight, but limit the maximum streaming bitrate to 300 kilobits per second.

For both these rules to work, they need to be in separate policy layers. If they were in the same policy layer, the rule listed second would never be applied.

## Ordering Policy Layers

The order of policy layers is also important. The appliance evaluates policy layers in the order in which they are listed in VPM. When the appliance is going through policy layers, it does not execute a given rule as soon as it finds that it meets the specific situation. Rather, it compiles a list of all the rules that meet the condition; when it has gone through all the policy layers, it evaluates the list, resolves any apparent conflicts, and then executes the required actions. If there is a conflict between rules in different policy layers, the matching rule in the policy layer evaluated last takes precedence.

In the above example, there are two Web Access Layers: one contains a rule stating that Sales personnel can access certain Web sites without authenticating, and the other states that when they do access these websites, limit the available bandwidth. The order of these policy layers is irrelevant. The order is irrelevant because there is no conflict between the rules in the layers.



The following is an example in which the order of policy layers does matter. Assume all URL requests from members of the purchasing department are directed to a single proxy server. To discourage employees from surfing the Web excessively during business hours, a company creates a Web Authentication Layer rule that states:

Whenever a client request comes in to the proxy server, prompt the client to authenticate.

Members of the purchasing department, however, need to access specific websites for business reasons, and the company does not want to require authentication every time they do this. So they create a Web Access Layer rule that states:

If any member of the purchasing department sends a request to a specific URL contained in a combined-object list, allow access.


The policy layer with the first rule needs to come first in evaluation order; it is then overridden by the second rule in a subsequent policy layer.







**Tip:** Always go from the general to the specific; that is, establish a general rule in an early policy layer, then write exception rules in later policy layers.

## About the Layer Guard Rule

The VPM layer guard feature allows you to set a condition by which the whole layer is evaluated or not. This saves system resources, especially if you have layers with large numbers of rules. When added, the layer guard is a single rule table that appears above the selected layer. The layer guard rule contains all of the columns available in the layer except for the Action and Track columns. These columns are not required because the rule itself does not invoke an action other than allowing or not allowing policy evaluation for the entire layer. All of the objects valid in the available columns are selectable and configurable in the layer guard rule, just as they are in the layer.

You cannot add a layer guard rule until you have created other policy layer rules.

To add a layer guard, go to  in a layer (supported in the CPL layer and the Default Security Policy layer) and click **Add Layer Guard**. Layer guards are denoted with a lock icon:

  Web Access Layer (1)		Web Access		Guard + 1 Rule			
LAYER NAME		TYPE		CONFIGURATION			
Source	Destination	Service	Time	Action	Track	Enforcement	
  Any	Any	Any	Any	-	-	-	
1   Authenticated User	Any	Any	Any	Deny	None	Appliance	

**Note:** If you create and install a **Notify User** object, the following layer guard is automatically added to the Web Access, Web Content, and SSL Access policy layers in the CPL:  
"condition=!\_\_is\_notify\_internal". This is required for compatibility and does not require any user interaction or tasks.

## Disabling or Deleting a Layer Guard Rule

By default, a layer guard rule is enabled when you add it. You can disable it (which retains the rule) or delete the rule from the VPM. See "Configuring layers" on page 20 for details on disabling and deleting rules.

# Installing Policies

As you add policy layers and rules, your work is saved in a file on the appliance; however, policies only take effect after you install the policies and the generated XML has been validated. The appliance then compiles the policies into CPL format and saves the resulting policies in the `vpm.cpl` file. This overwrites any policies previously created using VPM. The appliance saves VPM-generated policies in a single file and loads it all at once. You do not need to load policies separately, as is the case with the local or central policy files.

To install policies, click **Apply Policy**. The VPM validates the generated XML for any issues. If the validation passes, the CPL is generated and the policies are loaded.

If the XML fails the validation, you can compare the current policy to installed policy. See [Troubleshooting Policy Problems](#) for details. Alternatively, close the Generated CPL pane and continue to edit the policy.

Furthermore, the failed XML file is written to your hard disk; view this file, called `vpm_err.xml`, to troubleshoot the failed XML. The default location for this file is in the bluecoat folder on the hard drive.

**Note:** The Category, Notify User, DNS Lookup Restrictions, Reverse DNS Lookup Restrictions, and Group Log Order configuration objects generate CPL even if they are not included in rules. These objects and features allow you to edit categories and lists that might or might not be used in current policies.

# Managing Policy

This section describes how to manage VPM policy.

## Searching Policy

To search policy, type a string in the field beside **Search All**. You can limit the search to layer names or rule names and objects.

The layer name is included in the unfiltered search and the layer search. The CPL layer contents are not searched.

**Note:** The search field is also available after you apply policy, whether or not policy installation was successful; however, if policy installation fails, it might be useful to search for gestures or settings for troubleshooting.

## Refreshing Policy

Between occurrences when either VPM is closed and reopened or Install Policies is invoked, VPM does not recognize changes to VPM-managed policy that were made on the appliance through another method. For example:

- Another administrator opens a separate VPM to make changes.
- Another administrator edits the local or central policy file through the serial console.
- Another administrator makes edits the local or central policy file.
- A new content filter database is downloaded automatically and the new update contains category changes.
- A new content filter database is downloaded manually by an administrator.

## Reverting to a Previous Policy

If after creating new policies or editing an existing policy you decide to abandon the process and continue with the existing policy installed on the appliance, you can revert to that version. All current changes are deleted (VPM provides a verification prompt).

To revert to an existing installed policy, select **File > Revert to Existing Policy**.

## Changing Policies

You can change, edit, delete, add to, and otherwise manage policies created in VPM at any time by returning to VPM and working with policy layers and rules just as you did when creating them.

## Managing Policy Layers and Rules

To manage policy layers and rules, see "VPM Overview" on page 19

# Installing VPM-Created Policy Files

The appliance automatically creates the following files when saving VPM-created policies:

- config\_policy\_source.xml
- config\_policy\_source.txt

You can install VPM policies that were created on another appliance. This requires the following steps:

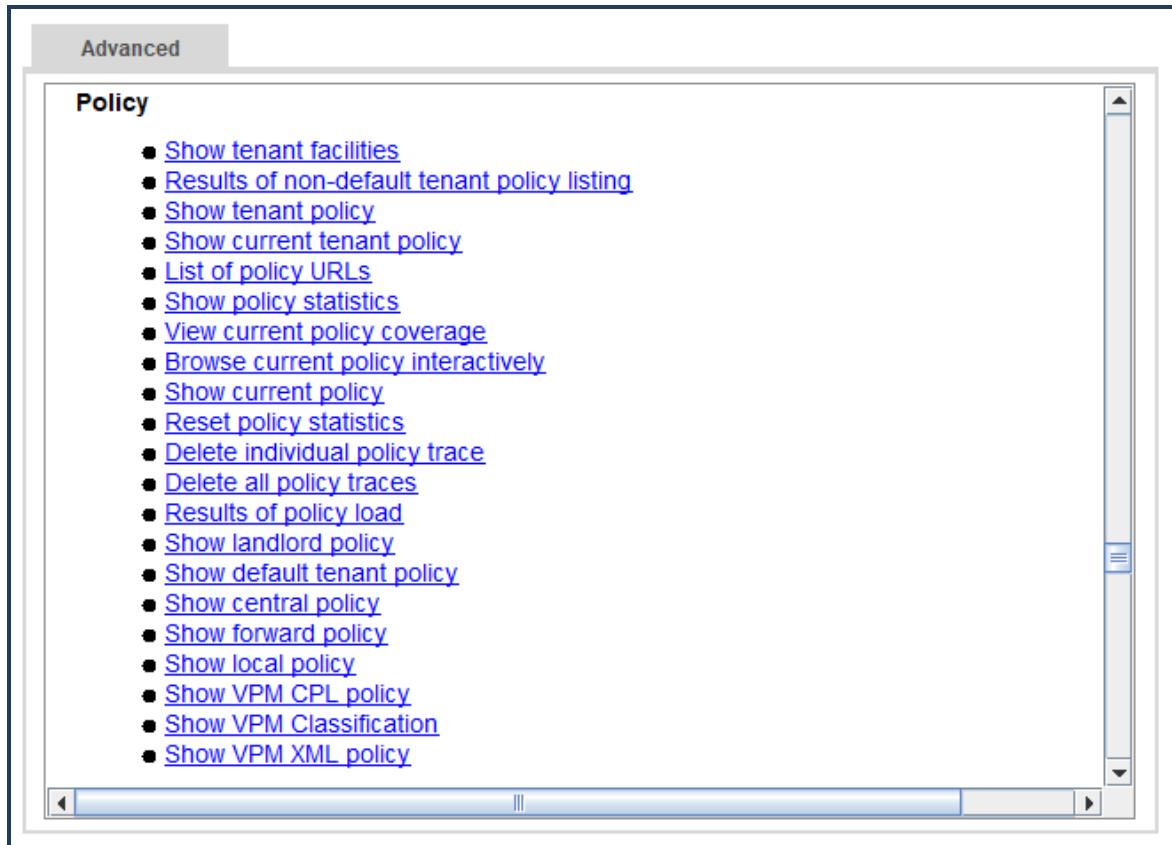
1. Copy the two VPM files, to be shared, to a Web server from the appliance on which they reside. See "Copying VPM Files To a Web Server" below.
2. Use the Management Console or CLI to load VPM files on another appliance. See "Loading VPM Files to an Appliance" on the next page.

## Copying VPM Files To a Web Server

To copy VPM files from a ProxySG appliance to a web server:

1. Select **Statistics > Advanced**.
2. Scroll down and click **Policy**.

The page displays the policy files links.



3. Right-click the **Show VPM CPL policy** link.
4. In the Save As dialog, enter the full path to a directory on the Web server before the file name and click **OK**.

The Save As dialog offers the appropriate default file name (config\_policy\_source.xml or config\_policy\_source.txt). You can change the names, including the extension. This can be helpful if an enterprise is using various sets of shared VPM files. You could rename files to indicate the appliance on which they were created, for example, or for a department that has a set of VPM-specific policies, used perhaps in multiple locations (sales\_vpm.cpl and sales\_vpm.xml)

5. Repeat the previous step for the second VPM file.

## Loading VPM Files to an Appliance

To load VPM files to an appliance:

1. Select **Configuration > Policy > Policy Files > Visual Policy Files**.
2. In the Install Visual Policy field:
  - a. Select **Remote URL** from the Install VPM-CPL from drop-down list.
  - b. Click **Install**. The Install VPM-CPL dialog appears.
  - c. In the Installation URL field, enter the URL to the VPM CPL file copied to the Web server (this is the file with the default .txt extension) and click Install.
  - d. Repeat Steps a through c to enter the URL to the second VPM XML file copied to the Web server (this is the file with the default .xml extension) and click **Install**.
3. Click **Apply**.

If VPM files already exist on the appliance, the URLs to those files display in the two file fields. In addition:

- To replace the VPM files, delete the URLs and type new ones. Installing new files overwrites any that are already present.
- To review VPM-generated policies before installing them, enter the URL to the CPL file on the Web server and click **View**.
- To review the CPL or XML files of the policies currently on the appliance at any time, click **VPM-CPL** and **VPM-XML** in the View Visual Policy Files box at the bottom of the dialog.

If you receive a "Conditions Removed From Policy" message, the policy included unsupported conditions. See "Determining unsupported conditions" on page 21 for information.

**Caution:** Never edit either of the VPM files directly. Change the files only by working with the policies in VPM and saving changes there.

# Tutorials

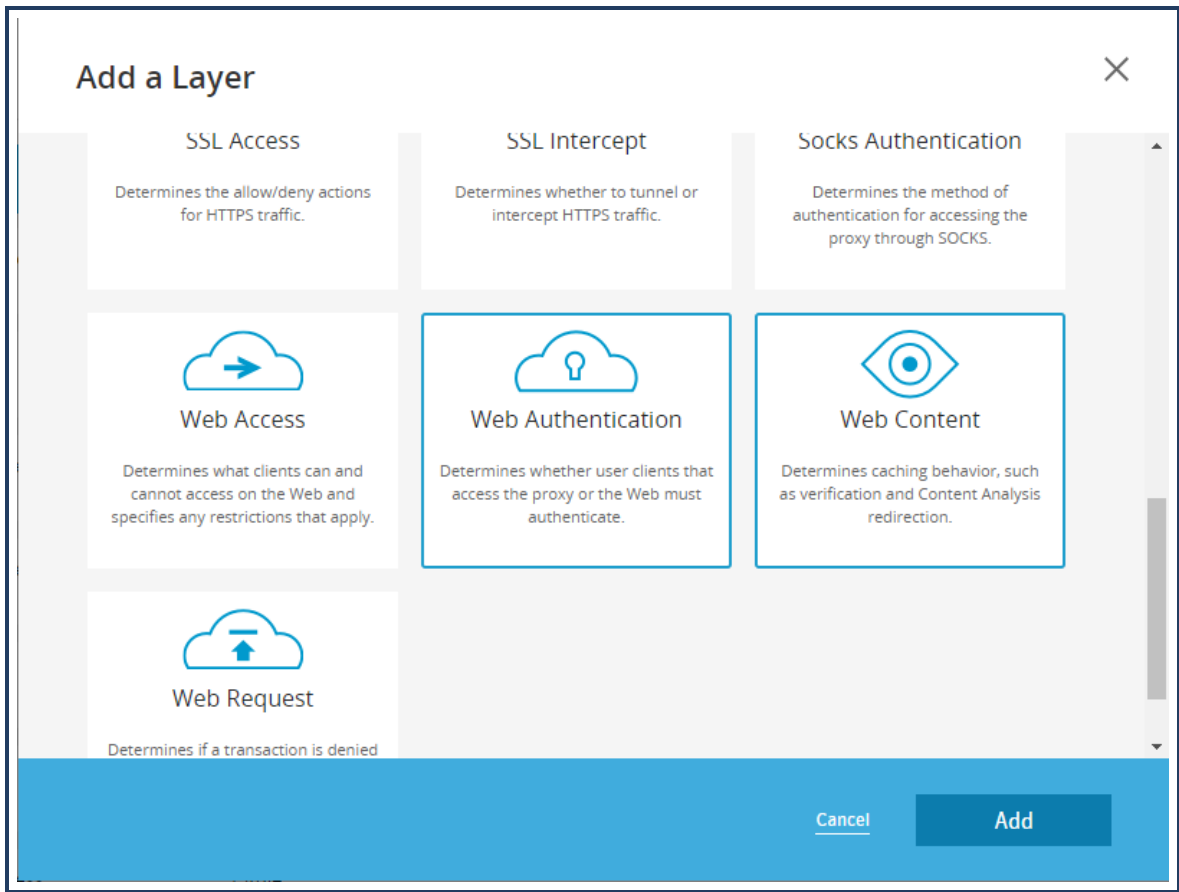
Refer to the following tutorials to create policies and rules for Web authentication and controlling user access.

- "Example: Create an Authentication Rule" below
- "Example: Exempt Specific Users from Authentication" on page 162
- "Example: Restrict Access to Specific Websites" on page 165
- "Example: Allow Specific Users to Access Specific Websites" on page 168

## Example: Create an Authentication Rule

Use Web Authentication policies to specify whether the individual making a request is prompted to authenticate by entering a username and password. This rule applies to all users going through the proxy.

1. Add a **Web Authentication** policy layer. See "Layers" on page 23.



2. Set an **Admin Authenticate** action object. See "Authenticate" on page 98 for more information.



In this example, specify an LDAP realm and Proxy IP as the authentication mode.

**Authenticate** ?

Name \*

Authenticate1

Realm\*

LDAP\_1 (LDAP)

Mode\*

Proxy IP

Authentication Form

New PIN Form

Query Form

Cancel Apply

3. Set a **Trace** object. See "Trace " on page 139 for more information.

In this example, enable tracing to log all authentication activity.

Trace?

×

Name \*

Trace1

☒ Set Trace Level

☐ Set Trace File

Trace Level\*

☒ Enabled

☐ Disabled

Cancel

Apply

The following example shows the completed rule:

<div><div></div><div><div></div></div></div>		<div><div>Web Authentication La...</div><div>LAYER NAME</div></div>	<div><div>Web Authentication</div><div>TYPE</div></div>	<div><div>1 Rule</div><div>CONFIGURATION</div></div>		
		Source	Destination	Action	Track	Enforcement
1	<div><div></div><div><div></div></div></div>	Any	Any	Authenticate1	Trace1	Appliance

## Example: Exempt Specific Users from Authentication

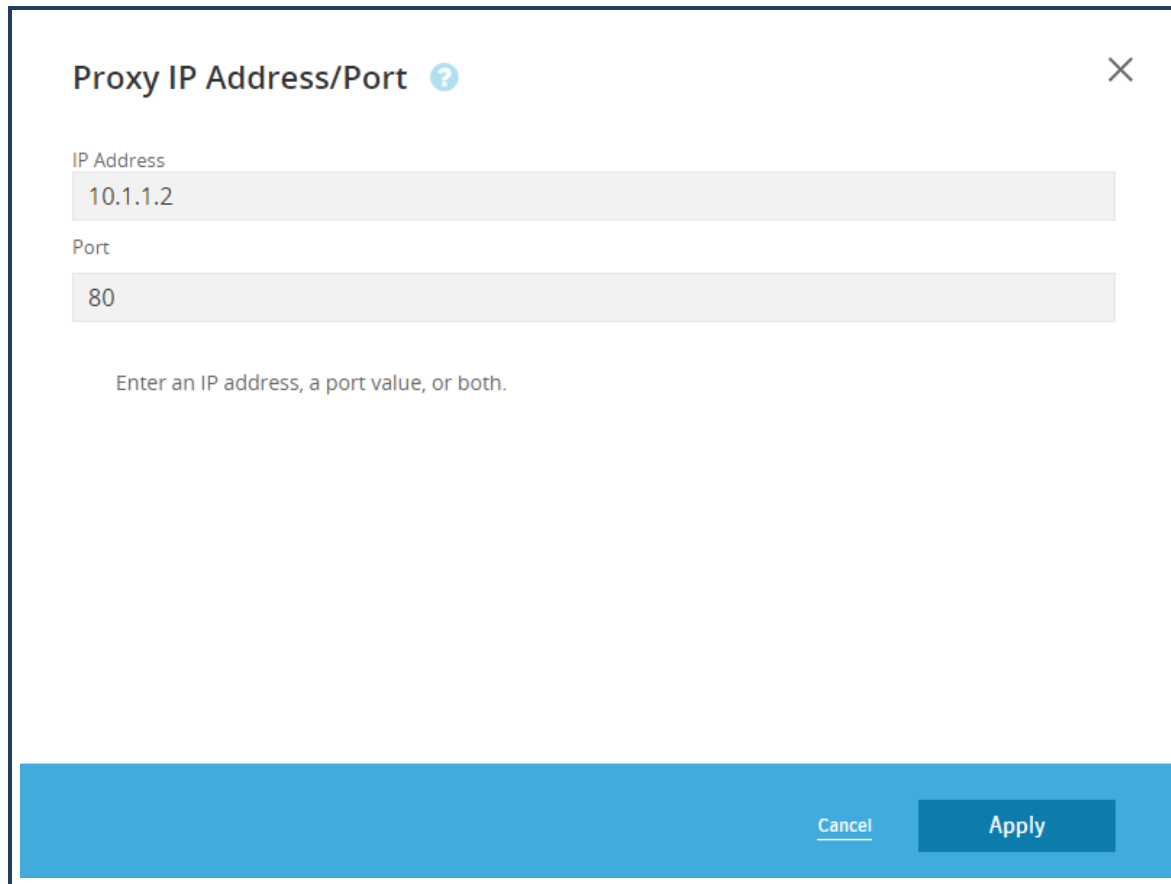
Certain individuals and groups are exempt from the restriction in the previous example.

In this example, a company uses a PAC file to configure most employee browsers to connect to a specific IP address on the appliance. The company wants these users to authenticate when their browsers send a request to the proxy. By default, the unmodified rule applies to everyone in Sales whose browsers connect to a specific IP address.

Individuals in the purchasing department are required to access the Web often so they can order online from supplier Web sites, and the company does not want them to authenticate. The company uses a PAC file to configure these employees' browsers to connect to a specific IP address on the appliance (10.1.1.2).

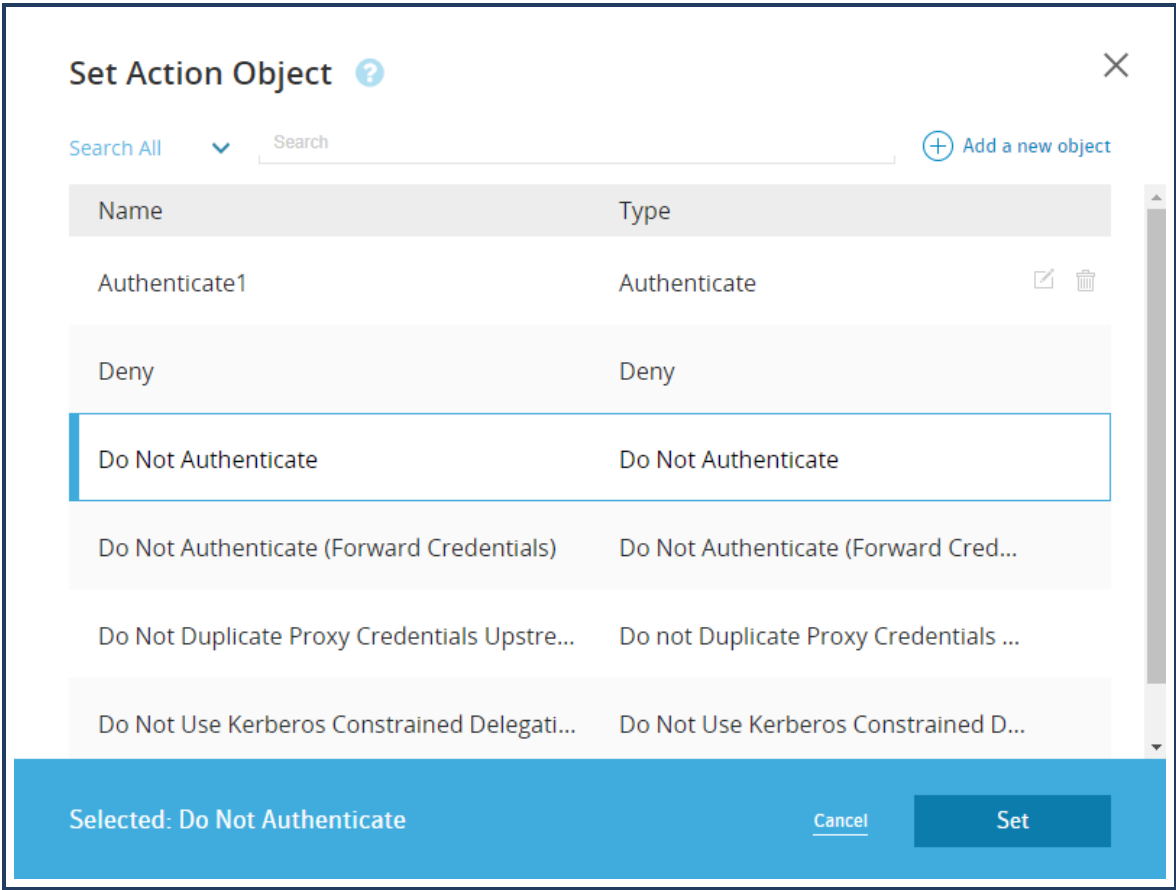
1. Click **Add Rule** to add a new rule to the **Web Authentication** policy layer created in the previous example. See "Policy Rules " on page 25.
2. Set a **Proxy IP Address/Port** source object. See "Proxy IP Address/Port" on page 60 for more information.

In this example, specify the IP address on the appliance to which the PAC file sends the purchasing department browsers.



The screenshot shows a configuration dialog box titled "Proxy IP Address/Port" with a question mark icon and a close button (X) in the top right corner. Inside the dialog, there are two input fields: "IP Address" containing the text "10.1.1.2" and "Port" containing the text "80". Below these fields is a hint text that reads "Enter an IP address, a port value, or both." At the bottom right of the dialog, there are two buttons: "Cancel" and "Apply".

3. Set a **Do Not Authenticate** action object.



The following example shows the completed rules:

		Web Authentication La...	Web Authentication	2 Rules		
		LAYER NAME	TYPE	CONFIGURATION		
		Source	Destination	Action	Track	Enforcement
1	<input checked="" type="checkbox"/>	Any	Any	Authenticate1	Trace1	Appliance
2	<input checked="" type="checkbox"/>	10.1.1.2:80	Any	Do Not Authentica...	None	Appliance

However, the second rule cannot be evaluated because the first rule affects everyone who goes through the proxy. If you try to install policy now, you receive the message "Warning: Unreachable statement (previous policy rule always matches) condition". The rules must be reversed for policy to be evaluated as intended.

4. Drag the second rule up to reorder the rules. See "VPM Overview" on page 19.

<div> <div></div> <div></div> <div></div> </div>		<div> <div></div> <div></div> <div></div> </div>	Web Authentication La...	Web Authentication	2 Rules	
			LAYER NAME	TYPE	CONFIGURATION	
			Source	Destination	Action	Track
1			10.1.1.2:80	Any	Do Not Authentica...	None
2			Any	Any	Authenticate1	Trace1
						Enforcement
						Appliance
						Appliance

- Click **Apply Policy** to install policy.

## Creating a Web Access Policy

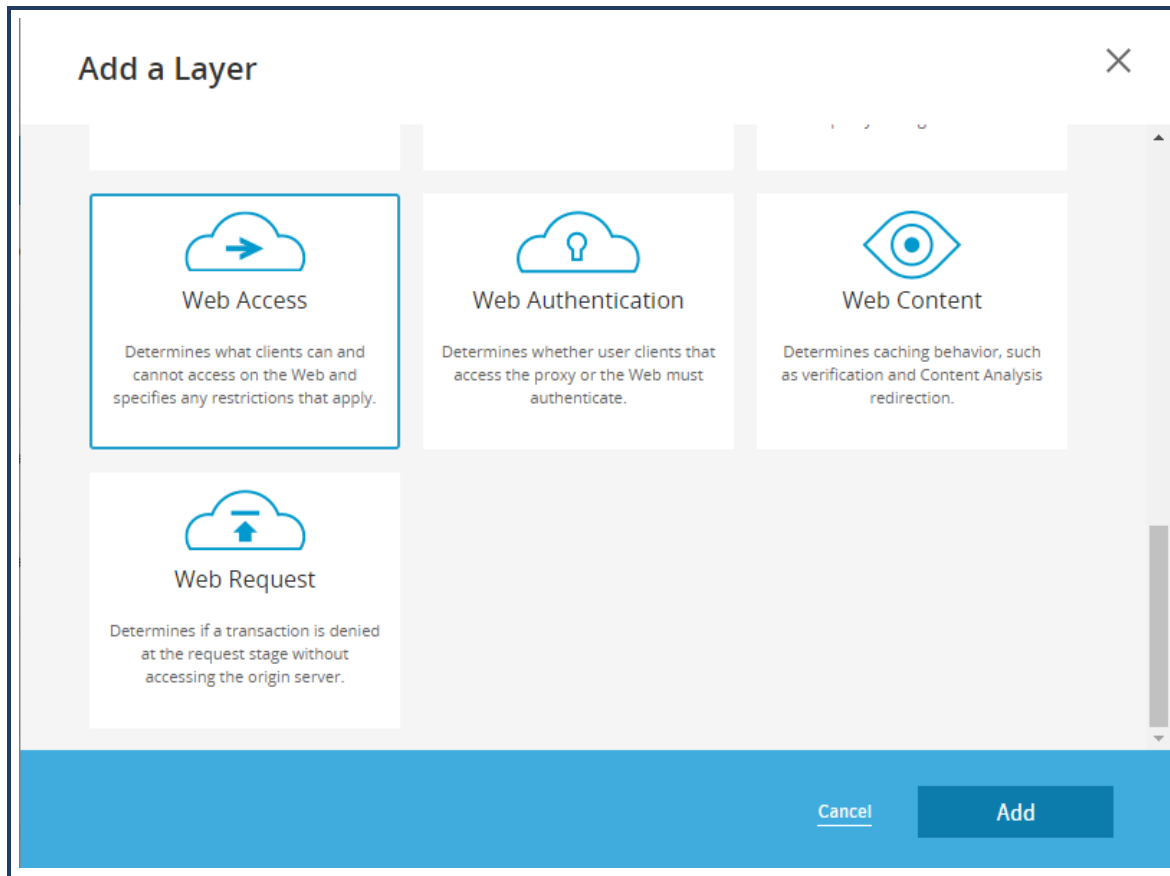
This tutorial demonstrates how to create policies and rules for Web access using a combined object. See "Combined Objects " on page 142 for more information.

Use ProxySG policies to define end-user access to Web resources. For more information about Web access policies, refer to "Configuring Access Logging" in the *SGOS Administration Guide*. This section provides examples.

## Example: Restrict Access to Specific Websites

This example demonstrates a simple rule that denies everyone access to specific job searching Web sites. This rule requires you to configure only one rule option; it uses the defaults for all other options.

1. Add a **Web Access** policy layer. See "Layers" on page 23.



2. Set a **Combined Destination** object that combines multiple **Request URL** objects. See "Request URL" on page 76 for more information.
3. In the Combined Destination object dialog, click **New** and select **Request URL** from the list of objects.  
Select **Simple Match** for matching type and enter the URL to match against.

## Request URL ?

×

Matching Type\*

☒ Simple Match  
☐ Regular Expression Match  
☐ Advanced Match

URL

hotjobs.com

If the host specified is a domain name, all hosts in that domain (or any subdomain) will match. If a path is specified, all paths with that prefix will match. If a scheme or port number is specified, only URLs with that scheme or port will match.

Cancel
Apply

4. Repeat the previous step for additional URLs. Then, select each **Request URL** object you want to combine.

CombinedDestination1

CombinedDestination1 ? Description...

At least one of the selected objects

Filter: Any ▼

☒ Only Show Selected (3) ☐ Negate + New

Name	Type	
<input type="checkbox"/> Destination: 1.1.1.3	Destination IP Address & Subnet	<span>✎</span> <span>✕</span>
<input type="checkbox"/> RequestURLCategory1	Request URL Category	<span>✎</span> <span>✕</span>
<input type="checkbox"/> FileExtension1	File Extensions	<span>✎</span> <span>✕</span>
<input checked="" type="checkbox"/> Request URL: monster.com	Request URL	<span>✎</span> <span>✕</span>
<input checked="" type="checkbox"/> Request URL: hotjobs.com	Request URL	<span>✎</span> <span>✕</span>
<input checked="" type="checkbox"/> Request URL: linkedin.com	Request URL	<span>✎</span> <span>✕</span>

5. Click **Apply** in the Combined Destination object dialog.

6. Click **Set** to add the combined object to the rule. As the default action is deny, the rule is complete. No one can access these Web sites.

		Web Access Layer (2)	Web Access	1 Rule			
		LAYER NAME	TYPE	CONFIGURATION			
		Source	Destination	Service	Time	Action	Enforcement
1	<input checked="" type="checkbox"/>	Any	CombinedDestina...	Any	Any	Deny	Appliance

7. Click **Apply Policy** to install policy.

## Example: Allow Specific Users to Access Specific Websites

The after-hours IT shift consists of part-time college interns who are on call to handle small problems, but are not involved in major projects. Therefore, you allow them to browse certain sports and entertainment Web sites when all is quiet; access is allowed from two workstations and you still want to track their browsing activity.

Before installing the following policy, make sure that the sports and entertainment categories are already defined. See "Destination Column Objects " on page 69 for details.

1. Add a **Web Access** policy layer. See " Layers" on page 23.
2. Set a **Combined Source** object that combines multiple **Client IP Address/Subnet** objects. See "Client IP Address/Subnet" on page 55 for more information.
3. In the Combined Source object dialog, click **New** and select **Client IP/Subnet** from the list of objects.
4. Enter the IP address and gateway to match against.



Client IP Address/Subnet ?

IP Address

10.1.1.0

Prefix Length or Subnet Mask

255.255.255.0

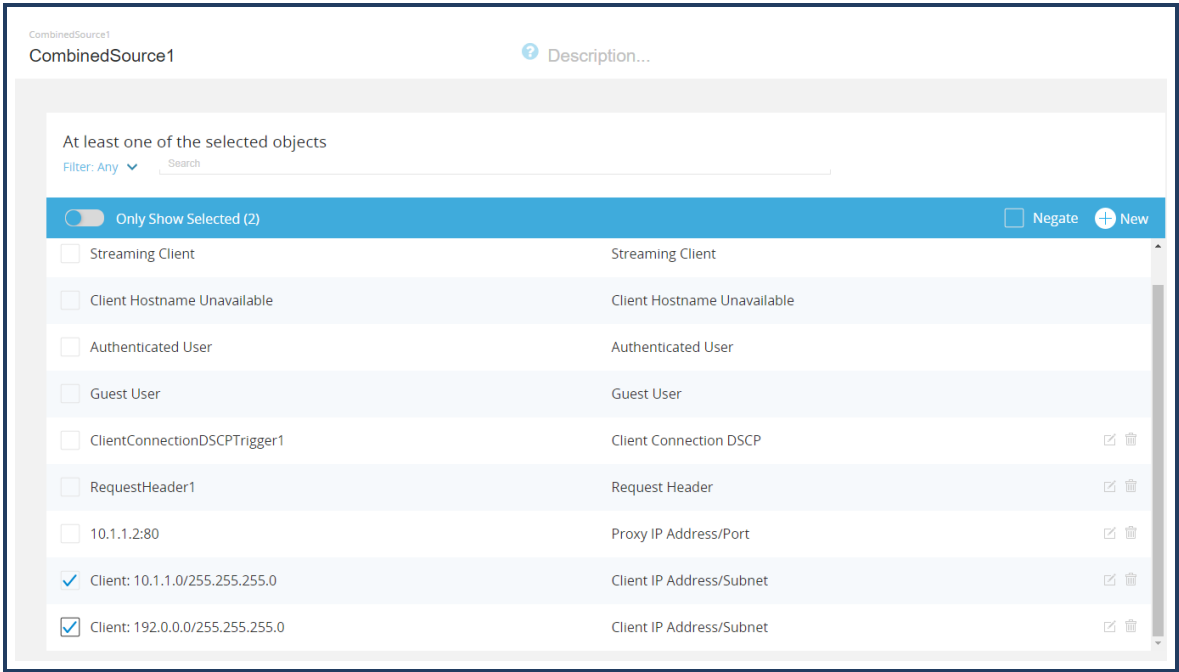
☐ Look up effective client IP (if configured)

Cancel

Apply

5. Repeat the previous step for additional IP addresses. Then, select each **Client IP Address/Subnet** object you want to combine.

Symantec: A Division of Broadcom



- 6. Click **Apply** in the Combined Source object dialog.
- 7. Click **Set** to add the combined object to the rule.
- 8. Set a **Request URL Category** destination object that includes the previously-defined entertainment and sports categories. See "Request URL Category" on page 77 for more information.

**Request URL Category** ?

Name \*

RequestURLCategory2

☒ Policy

- ☒ Allowable Entertainment
- ☒ Allowable Sports

☐ System

Allowable Entertainment

Allowable Sports

[Cancel](#) **Apply**

- Click **Set** to add the combined object to the rule.
- Set a **Time** object that allows specified users to access the sports and entertainment Web sites after business hours.

In the Time dialog:

- Select Time of the day and enter a start and end time.
- Select Days of the week and select Monday, Tuesday, Wednesday, Thursday, and Friday.

Time ?

Local

UTC

Time of the day\*

All

Selected

Between: 18 : 00 and 05 : 59

Days of the week\*

All

Selected

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☐ Saturday

☐ Sunday

Days of the month\*

All

Selected

Time of year\*

All

Selected

Cancel

Apply

11. Click **Set** to add the combined object to the rule.
12. In the Action column, specify **Allowed**. The following example shows the completed rule:

Web Access Layer (2)		Web Access		1 Rule			
LAYER NAME		TYPE		CONFIGURATION			
Source		Destination		Service	Time	Action	Enforcement
1	<div><div></div><div>CombinedSource1</div></div>	RequestURLCateg...		Any	Time1	Allow	Appliance

13. Click **Apply Policy** to install policy.

# Composing CPL Directly in the VPM

You can compose CPL directly into the VPM using the CPL Layer. The CPL Layer can be manipulated like any other policy layer, with some exceptions (described in "Policy Rules " on page 25). When the CPL Layer is installed with other policy layers, it is subject to the policy evaluation order.

**Note:** The VPM does not validate CPL. If any errors exist, policy installation fails. Refer to the **Problems** pane in the VPM for messages such as "Error: Unknown tag" and correct the CPL manually.

For details on CPL, refer to the *Content Policy Language Reference*.

# Advanced Policy Tasks

This section provides conceptual and procedural information about the ProxySG appliance's advanced policy features. While many appliance features have a policy component, some features have no configuration component outside policy. Configuring advanced policy is accomplished by defining rules in the Visual Policy Manager (VPM) or by composing Content Policy Language (CPL). While some examples are provided in this chapter, references to the relevant chapter component are included in each section.

Excluding exceptions, you must use policy to implement these capabilities. (For exceptions, you can create a list outside of policy to install on the system.)

# Blocking Pop-Up Windows

This section describes the Symantec solution for blocking unwanted pop up windows.

## About Pop Up Blocking

The ProxySG appliance allows you to block pop up windows, which are usually in the form of unsolicited advertisements. Pop up windows are blocked by inserting Javascript code into each HTML Web page. Every time the Web page tries to open a new window, the code attempts to determine if the window is a result of user click. The window is allowed to open if the appliance determines a user clicked a button or link; otherwise, the window does not open.

## Interactivity Notes

Because of the dynamic nature of the Web, blocking pop up windows is not a perfect solution. Consider the following caveats before configuring this feature:

- Windows that contain desired or useful information cannot be distinguished from undesired content, such as advertisements.
- If the Web browser caches a page that spawns pop up windows before the blocking policy was installed, pop up ads continue to be served from that page regardless of current policy.
- Animated ads contained within Web pages are not blocked. Commonly seen in scrolling or drop-down form, these are not true pop up windows but are contained within the page. Users who see these ads might believe that pop up window blocking is not implemented.
- Pop up windows that are delivered through HTTPS are not blocked.
- Although the ProxySG request headers instruct a Web server not to use compression, it is possible (though not likely) for a Web server to be configured to send compressed responses anyway. The pop up blocking feature does not work on compressed HTML pages.

## Recommendations

- To compensate for limiting factors, administrators and users can override pop up blocking:
- Administrators—Use the to create policy rules that exempt pop up blocking for specific Web sites and IP address ranges. For example, Symantec recommends disabling pop up blocking for your Intranet, which commonly resides on a IP address range. The following example shows a rule for disabling pop up blocking on the corporate site.

Web Access Layer (1)		Web Access		2 Rules			
LAYER NAME		TYPE		CONFIGURATION			
	Source	Destination	Service	Time	Action	Track	Enforcement
1	Any	Request URL: torp...	Any	Any	Block Popup Ads	None	Appliance

## Symantec: A Division of Broadcom

- Users—When a pop-up window is blocked, a message is displayed in the status bar:

blocked popup window -- use CTRL Refresh to see all popups.

While pressing the Control key, click the Web browser Refresh button; the page is reloaded with pop up blocking disabled for that action.

- Create a separate Web Access policy layer for pop up blocking actions. This alleviates interference with Web applications deployed on your Intranet that require pop up windows.
- To prevent a cached Web page from spawning pop up windows, clear the browser cache, then reload the page without holding down the CTRL key.

See "Action Column Objects" on page 93 for information about how to create blocking actions in a policy layers.



# Exempting Non-Contiguous IP Addresses

The ProxySG policy language includes several triggers that test a value of the current transaction against an IP address. All such triggers allow either an individual IP or a subnet, however non-contiguous IP ranges can present a problem. Replicating a rule multiple times to match each IP/subnet is not as efficient as grouping this information into a single object that is valid for all appropriate trigger conditions.

## CPL Example

```
; define list of IPs in subnet
define subnet internal_ranges
    10.0.0.0/16
    192.168.1.0/24

end

; allow requests from defined IPs
<proxy>
    client.address=internal_ranges ALLOW
```

## VPM Example

1. Add a **Web Access Layer**. See "Layers" on page 23.
2. Add a policy rule to the layer. See "Policy Rules " on page 25.
3. Create a **Client IP Address/Subnet** object for each IP address/subnet. See "Client IP Address/Subnet" on page 55.
4. Add a **Combined Source** object called Internal\_IP\_Ranges that includes the objects you created in the previous step. See "Combined Objects " on page 142.

Symantec: A Division of Broadcom

CombinedSource1

Internal\_IP\_Ranges

Description...

At least one of the selected objects

Filter: Any Search

Only Show Selected (2)

Negate New

<input type="checkbox"/>	IMUser1	IM User Object	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	RequestHeader1	Request Header	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Client: testtest	Client Hostname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	10.1.1.2:80	Proxy IP Address/Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Client: test	Client Hostname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Client: test (Contains)	Client Hostname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Client: 10.0.0.0/16	Client IP Address/Subnet	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Client: 192.68.1.0/24	Client IP Address/Subnet	<input checked="" type="checkbox"/>	<input type="checkbox"/>

AND

Add a second list

At least one of the selected objects

Cancel

Apply

5. Set the action to **Allow**. See "Action Column Objects" on page 93.

# Stripping or Replacing Active Content

Scripts activated within Web pages can pose a security concern. The ProxySG policy can be configured to supplement standard virus scanning of Web content by detecting and removing the HTML tags that launch active content such as Java applets or scripts. In addition, the removed content can be replaced with predefined material, a process referred to as active content transformation.

When the appliance is configured to perform active content transformation, Web pages requested by a client are scanned before they are served and any specified tags and the content they define are either removed or replaced. Because the transformed content is not cached, the transformation process is based on a variety of conditions, including time of day, client identity, or URL.

**Note:** Pages served over an HTTPS tunneled connection are encrypted, so the content cannot be modified.

The following tags and related content can be removed or replaced:

- `<APPLET>`—Java applets.
- `<EMBED>`—Embedded multimedia objects displayed using older browser plug-ins.
- `<OBJECT>`—Embedded multimedia objects displayed using Internet Explorer Active-X controls and other multimedia elements.
- `<SCRIPT>`—Embedded JavaScript and VBScript programs, whether these are represented as HTML `<SCRIPT>` elements, JavaScript entities, JavaScript URLs, or event handler attributes. The `<NOSCRIPT>` tag is not affected by this feature.

You can strip active content through the VPM (see "Strip Active Content" on page 123) or by composing CPL (refer to the *Content Policy Language Reference*).

## About Active Content Types

The following sections provide more detail about the types of active content that can be removed or replaced.

### Script Tags

Scripts are generally put between the start and end tags `<SCRIPT>` and `</SCRIPT>`. The type of script used is defined by the `LANGUAGE` attribute, such as `<SCRIPT LANGUAGE="JavaScript 1.0">`. When the `LANGUAGE` attribute is undefined, the browser assumes JavaScript.

When transform `active_content` is configured to remove scripts, the basic operation is to remove all content between and including `<SCRIPT>` and `</SCRIPT>`, regardless of the language type, and substitute any defined replacement text. A notable exception occurs when a script is defined in the header portion of the HTML document (defined by the `<HEAD>` tag). In this case, the script is simply removed. This is because images, objects, and text are not allowed in the header of an HTML

document. If the end script tag `</SCRIPT>` is missing from the document (the end of the document is defined as either up to the `</BODY>` or `</HTML>` tag, or the last character of the document), then all content from the start `<SCRIPT>` tag to the end of the document is removed.

## JavaScript Entities

JavaScript entities have the following format: `&{javascript code}`.

They are found anywhere in the value part of an attribute (that is, `<IMG SRC="&{images.logo};">`). You can define more than one entity in the value portion of the attribute. When transform `active_content` is configured to remove scripts, all JavaScript entities attribute/value pairs are removed. No replacement text is put in its place.

## JavaScript Strings

JavaScript strings have the following format: `javascript: javascript code`

They are found anywhere in the value part of an attribute, though usually only one of them can be defined in an attribute. Most modern browsers support JavaScript strings. When transform `active_content` is configured to remove scripts, all JavaScript string attribute/value pairs are removed. No replacement text is put in its place.

## JavaScript Events

JavaScript events are attributes that start with the keyword `on`. For example, `<A HREF="index.html onMouseOver="javascript code">`. The HTML 4.01 specification defines 21 different JavaScript events:

`onBlur`, `onChange`, `onClick`, `onDblClick`, `onDragDrop`, `onFocus`, `onKeyDown`, `onKeyPress`, `onKeyUp`, `onLoad`, `onMouseDown`, `onMouseMove`, `onMouseOut`, `onMouseOver`, `onMouseUp`, `onMove`, `onReset`, `OnResize`, `onSelect`, `onSubmit`, `onUnload`

Browsers can have defined variations on these events as well as many others. To catch all JavaScript events, the active content transformer identifies any attribute beginning with the keyword `on`, not including `on` itself. For example, the attribute `onDonner` in the tag `<A HREF="index.html" onDONNER="DONNER">` is removed even though `onDonner` does not exist as a valid JavaScript event in the browser. In this case, the transformed file would show `<A HREF="index.html">`.

## Embed Tags

HTML `<EMBED>` tags are not required to have an `</EMBED>` end tag. Many web browsers do, however, support the `<EMBED>` `</EMBED>` tag pair. The text between the tags is supposed to be rendered by the browsers when there is no support for the embed tag, or if the MIME-type of the embed object is not supported. Thus, when transform `active_content` is configured to transform embed tags, only the `<EMBED>` tag is removed and replaced with any replacement text. Any occurrence of the end tag `</EMBED>` is simply removed, leaving the text between the beginning and end tags intact.

## Object Tags

Objects tags have an `<OBJECT>` `</OBJECT>` tag pair, and the attributes `CODETYPE` and `TYPE` specify the type of object. The text between the tags is supposed to be rendered by the browsers when the object tag is not supported, so when transform `active_content` is configured to transform object tags, only the `<OBJECT>` and `</OBJECT>` tags are removed and replaced with

any replacement text. The text between the tags remains. The CODETYPE or TYPE attributes do not affect the transformation. Also, if the end `</OBJECT>` tag is missing, the transformation will not be affected.

# Modifying Headers

The request headers are sent when users access Web objects that contain a lot of information. This can raise a concern that such details compromise the privacy or security of the enterprise or user.

When a user clicks on a link, the Web browser sets the request's Referer header to the URL of the Web page that contained the link. (This header is not set if the URL was entered or selected from a favorites or bookmarks list.) If an internal Web page provides links to external Web sites, users clicking those links sends the URL of the internal pages, and are logged in the Web logs of those external sites. This is not usually an issue; however, if the external Web site is a competitor Web site or another site with interest in the internal details of your enterprise, this might be a concern.

For example, how you structure your intranet might suggest something about your company's current or future direction. Certain project names or codewords might show up in directory or file names. Exposing the structure of the intranet makes it easier for hackers to attack the network.

The broad solution of deleting Referer headers from all requests presents a problem because some Web sites do not serve images or other linked objects unless the Referer header is set to a referring page on that same Web site. The solution implemented by Symantec is to strip the Referer header only when the target Web page resides on the Internet and the referring page is on an internal host. For details on suppressing headers, see "Suppress Headers" on page 123.

# Defining Exceptions

Exceptions are sent in response to certain ProxySG client requests, such as denial by policy, failure to handle the request, and authentication failure. Exceptions are returned to users based on policy rules defined by the ProxySG administrator. For example, if a client sends a request for content that is not allowed, an exception HTML page (for HTTP connections) or an exceptions string (for non-HTTP connections) is returned, informing the client that access is denied.

Two types of exceptions are used: "Built-in Exceptions" below and "User-Defined Exceptions" on page 188.

## Built-in Exceptions

Built-in exceptions are a set of pre-defined exceptions included on the ProxySG appliance. Built-in exceptions send information back to the user under operational contexts that are known to occur, such as `policy_denied` or `invalid_request`.

Built-in exceptions are always available and can also have their contents customized; however, they cannot be deleted, and you cannot create new built-in exceptions.

The table below lists the built-in exceptions and the context under which they are issued.

Exception Type	HTTP Response Code	Issued When...
authentication_failed	401	The transaction cannot be authenticated, usually because the credentials were incorrect. <code>authentication_failed</code> is a synonym for <code>deny.unauthorized</code> .
bad_credentials	400	The username or password were sent using an invalid/ unrecognized format. This can have two causes: <ul style="list-style-type: none"> <li>• The username or password contains non-ASCII characters, and the appliance is not configured to use the same authentication character encoding as is being used by the web browser.</li> <li>• The username or password is too long. (The limits for the username and password are 64 bytes each, after being translated to UTF-8.)</li> </ul>
client_failure_limit_exceeded	503	Too many requests from your IP address ( <code>\$(client.address)</code> ) have failed.
configuration_error	403	A configuration error on the appliance was detected, and the requested operation could not be handled because of the configuration error. This exception is a likely indicator that the administrator of the ProxySG must intervene to resolve the problem.
connect_method_denied	403	A user attempted an <code>CONNECT</code> method to a nonstandard port when explicitly proxied. Symantec does not allow <code>CONNECT</code> methods to non-standard ports by default because it is considered a security risk to do so.
content_encoding_error	502	A Web site presented a content encoding header of one type but encoded the data differently

Exception Type	HTTP Response Code	Issued When...
content_filter_denied	403	A particular request is not permitted because of its content categorization.
content_filter_unavailable	403	An external content-filtering service could not be contacted, and the appliance is failing closed in such a situation.
dns_server_failure	503	The request could not be processed because the appliance was unable to communicate with the DNS server in order to resolve the destination address of the request.
dns_unresolved_hostname	404	The request could not be processed because the appliance was unable to resolve the hostname in the request with DNS.
dynamic_bypass_reload	200	The dynamic_bypass policy action is matched.
gateway_error	504	There was a network error while attempting to communicate with the upstream gateway.
icap_communication_error	504	A network error occurred while the appliance was attempting to communicate with an external ICAP server.
icap_error	504	A network problem occurred, the ICAP service might be misconfigured, or the ICAP server might have reported an error.
internal_error	500	The appliance encountered an unexpected error that resulted in the inability to handle the current transaction.
invalid_auth_form	403	The submitted authentication form is invalid. The form data must contain the username, password, and valid original request information.
invalid_request	400	The request received by the appliance was unable to handle the request because it detected that there was something fundamentally wrong with the syntax of the request.
invalid_response	502	The server's response could not be processed because of a malformed response or a misconfiguration.
license_exceeded	403	Access is denied because a license has been exceeded on the proxy, and the request is not permitted.
license_expired	403	The requested operation cannot proceed because it would require the usage of an unlicensed feature.



Exception Type	HTTP Response Code	Issued When...
method_denied	403	The requested operation utilizes a method that has been explicitly denied because of the service properties associated with the request.
not_implemented	501	The protocol cannot handle the requested operation because it utilizes a feature that is not currently implemented.
notify	200	Used internally by the VPM. You do not need to customize the text of this exception, since in this case the entire HTML response is generated by VPM and is not taken from the exception definition.
notify_missing_cookie	403	This exception is returned when a Notify User action is being used to notify the user, and the user has disabled cookies in the Web browser.
policy_denied	403	policy_denied is a synonym for deny.
policy_redirect	302	A redirect action is matched in policy.
radius_splash_page	200	The user is authorized. Click the refresh button on the browser to proceed to the requested site. The user/ session ID is \$(x-radius-splash-username)/\$(x-radius-splash-session-id)
redirected_stored_requests_not_supported	403	This applies to forms authentication with POST requests only): The origin server returned a redirect for the request. The appliance is configured to not allow stored requests to be redirected.
refresh	200	A refresh (using the HTTP Refresh: header) is required. The refresh exception (by default) refreshes the originally requested URL (or in some cases, its post-imputed form).
server_request_limit_exceeded	503	Too many simultaneous requests are in progress to \$(url.host).
silent_denied	403	An exception(silent_denied) is matched in policy. This exception is pre-defined to have no body text, and is silent in that it results in only the status code being sent to the client.
server_authentication_error	500	Internal error. The appliance encountered an internal error while preparing to send the username/password upstream. This error can only occur when the appliance "server authentication" feature is enabled.
ssl_client_cert_expired: Expired SSL Client Certificate	503	A web site presents an incorrect or invalid certificate or a configuration error has occurred.
ssl_client_cert_ocsp_check_failed OCSP Error On Client Certificate	503	An error occurred while checking the revocation status of the certificate.

Exception Type	HTTP Response Code	Issued When...
ssl_domain_invalid: SSL Certificate Host Mismatch	409	There was a failure contacting a web site through HTTPS because the certificate has a common name that does not match the web site's domain name.
ssl_failed: SSL Certificate Verification Error	503	A secure connection could not be established to an web site. This typically occurs when a web site that is not configured to accept SSL connections.
ssl_server_cert_expired: Expired SSL Server Certificate	503	A Web site presents an incorrect or invalid certificate or a configuration error has occurred.
ssl_server_cert_ocsp_check_failed OSCP Error On Server Certificate	503	An error occurred while checking the revocation status of the certificate.
ssl_client_cert_revoked: Revoked SSL Client Certificate	503	The client presents a revoked certificate or a configuration error has occurred.
ssl_client_cert_ocsp_status_unknown: Unknown OSCP Status of Client Certificate	503	An OSCP check returned unknown status for a client certificate.
ssl_client_cert_untrusted_issuer Untrusted SSL Client Certificate	503	A Web site presents an incorrect or invalid certificate or a configuration error has occurred.
ssl_server_cert_ocsp_status_unknown: Unknown OSCP Status of Server Certificate	503	The server certificate revocation status is unknown. This is caused by a certificate revocation check for which the server does not have a status.

Exception Type	HTTP Response Code	Issued When...
ssl_server_cert_revoked: Revoked SSL Server Certificate	503	A Web site presents a revoked certificate or a configuration error has occurred.
ssl_server_cert_untrusted_issuer: Untrusted SSL Server Certificate	503	A Web site presents an incorrect or invalid certificate or a configuration error has occurred.
tcp_error	503	A network error occurred attempting to communicate with an upstream host.
transformation_error	403	The server sends an unknown encoding and the appliance is configured to do content transformation.
unsupported_encoding	406	The client makes a request with an Accept- Encoding: Identity;q=0, ... header. Only uncompressed content is available in cache, the appliance is not configured to compress the content, or the compression license is expired, or the client request results in to Accept- Encoding: Identity;q=0 because of the combination of request and configured policy.
unsupported_protocol	406	The protocol used in the request is not understood.
upstream_407_rejected	407	An authentication challenge (HTTP status code 407 "Proxy authentication required") from an upstream OCS was blocked.
virus_detected	200	Virus was detected in the content.
data_leak_detected	200	<p>A violation of DLP policy was detected in the content.</p> <p>The ICAP response must contain the following:</p> <ul style="list-style-type: none"> <li>■ X-Violations-Found in the HTTP header</li> <li>■ dlp string in the Server header</li> </ul>

Most built-in exceptions can be initiated directly through the `policy exception()` property. However, some require additional state that makes initiating them either problematic or out of context.

The following are exceptions that cannot be initiated through the `exception()` property:

- `authentication_failed`
- `authentication_failed_password_expired`
- `authentication_redirect_from_virtual_host`
- `authentication_redirect_to_virtual_host`

- authentication\_success
- dynamic\_bypass\_reload
- license\_expired
- ssl\_domain\_invalid
- ssl\_failed

To view the content of a built-in exception, enter the following commands at the #(config) prompt:

```
 #(config) exceptions
 #(config exceptions) show exceptions configuration_error
 configuration_error exception:
 all protocols:
 summary text:
     SG configuration error
 details text:
     Your request could not be processed because of a configuration error: $(exception.last_error)
 help text:
     The problem is most likely because of a configuration error, $(exception.contact) and provide
     them with any pertinent information from this message.
 http protocol:
     code: 403
```

## User-Defined Exceptions

User-defined exceptions are created and deleted by the administrator. If a user-defined exception is referenced by policy, it cannot be deleted. The default HTTP response code for user-defined exceptions is 403.

For users who are explicitly proxied and use Internet Explorer to request an HTTPS URL, an exception body longer than 900 characters might be truncated. The workaround is to shorten the exception body.

An exception body less than 512 characters might cause a page does not exist 404 error. If this occurs, use the `exception.autopad()` property to pad the body to more than 513 characters. For more information, refer to the *Content Policy Language Reference*.

## About Exception Definitions and Hierarchy

Each exception definition (whether built-in or user-defined) contains the following elements:

- Identifier: Identifies the type of exception. "Built-in Exceptions" on page 183 lists the built-in exception types. For user-defined exceptions, the identifier is the name specified upon creation.

- **Format:** Defines the appearance of the exception. For an HTTP exception response, the format is an HTML file. For other protocols, where the user agents are not able to render HTML, the format is commonly a single line.
- **Summary:** A short description of the exception that labels the exception cause. For example, the default policy\_denied exception summary is "Access Denied".
- **Details:** The default text that describes reason for displaying the exception. For example, the default policy\_denied exception (for the HTTP protocol) detail is:

Your request has been denied by system policy.

- **Help:** An informative description of common possible causes and potential solutions for users to take. For example, if you want the categorization of a URL reviewed, you can append the `$(exception.category_review_url)` and `$(exception.category_review_message)` substitutions to the `$(exception.help)` definition. You must first enable this capability through content filtering configuration. For information on enabling review categorization, refer to the *SGOS Administration Guide*.
- **Contact:** Used to configure site-specific contact information that can be substituted in all exceptions. Although it is possible to customize contact information on a per exception basis, customizing the top-level contact information, which is used for all exceptions, is sufficient in most environments.
- **HTTP-Code:** The HTTP response code to use when the exception is issued. For example, the policy\_denied exception by default returns the 403 Forbidden HTTP response code.

**Note:** Fields other than Format must be less than 8000 characters. If they are greater than this, they are not displayed.

When defining the above fields, you can use substitution variables that are particular to the given request. Some of the above fields are also available as substitutions:

- `$(exception.id)`
- `$(exception.summary)`
- `$(exception.details)`
- `$(exception.help)`
- `$(exception.contact)`

Additionally, the Format, Summary, Details, Help and Contact fields can be configured specifically for HTTP, or configured commonly for all protocols.

The Format field, the body of the exception, is not available as a substitution. However, the Format field usually includes other substitutions. For example, the following is a simple HTML format:

`$(exception.id): $(exception.summary)`

`Request: $(method) $(url)`

Details: `$(exception.details)`  
Help: `$(exception.help)`  
Contact: `$(exception.contact)`

Some additionally useful substitutions related to exceptions are:

- `$(exception.last_error)`: For certain requests, the ProxySG appliance determines additional details on why the exception was issued. This substitution includes that extra information.
- `$(exception.reason)`: This substitution is determined internally by the appliance when it terminates a transaction and indicates the reason that the transaction was terminated. For example, a transaction that matches a DENY rule in policy has its `$(exception.reason)` set to "Either 'deny' or 'exception' was matched in policy".

## About the Exceptions Hierarchy

Unlike the error pages in previous SGOS releases, exceptions are not required to have its entire contents defined. Exceptions are stored in a hierarchical model, and parent exceptions can provide default values for child exceptions. There are two parent exceptions from which other exceptions are derived, `exception.all` and `exception.user-defined.all`

Each built-in and user-defined exception derives its default values from the all exception. For example, by default the built-in exceptions do not define the format field. Instead, they depend on the all exception's format field definition. To change the format text for all built-in and user-defined exceptions, customize the format field for the all exception.

The user-defined.all exception is the parent of all user-defined exceptions, but it is also a child of the all exception. Configuring `exception.user-defined.all` is only necessary if you want certain fields to be common for all user-defined exceptions, but not common for built-in exceptions.

The following example demonstrates using the exception inline command to configure the `$(exception.contact)` substitution for every HTTP exception:

```
# (config exceptions) inline http contact EOF
For assistance, contact <a href="mailto:sysadmin@example.com">sysadmin</a>EOF
```

The following example configures a different `$(exception.contact)` substitution for every HTTP exception:

```
# (config exceptions) user-defined inline http contact EOF
For assistance, contact <a href="mailto:policyadmin@example.com">policyadmin</a>EOF
```

## Installing and Viewing Exceptions

Refer to the following to learn about installing and viewing exceptions:

- "About the Installable List of Exceptions" on the facing page
- "Creating and Editing Exceptions" on page 192
- "Viewing Exceptions" on page 194

## About the Installable List of Exceptions

The Exceptions Installable List uses the Structured Data Language (SDL) format. This format provides an effective method to express a hierarchy of key/value pairs. For example, the following is SDL file before customization:

```
(exception.all
  (format "This is an exception: $(exception.details)")
  (details "")
  (exception.policy_denied
    (format "")
    (details "your request has been denied by system policy")
  )
)
```

This SDL file defines an exception called `policy_denied` that defines the `$(exception.details)` substitution as "Your request has been denied by system policy". Because the exception does not define the format field, it inherits the format field from its parent exception (`exception.all`). When the `policy_denied` exception is issued, the resulting text is: This is an exception: your request has been denied by system policy.

Suppose you want to customize the `$(exception.contact)` substitution for every HTTP exception. Edit the `exception.all` component.

**Note:** The default HTTP format and built-in exception definitions have been removed for example purposes.

```
(exception.all
  (contact "For assistance, contact your network support team.")
  (details "")
  (format "$(exception.id): $(exception.details)")
  (help "")
  (summary "")
  (http
    (code "200")
    (contact "")
    (details "")
    (format <<EOF
<format removed>
  EOF
  )
    (help "")
    (summary "")
  )
<built-in exceptions removed>
)
```

To add the `$(exception.contact)` information, modify the contact substitution under the `http` node:

## Symantec: A Division of Broadcom

```
(exception.all
  (contact "For assistance, contact your network support team.")
  (details "")
  (format "${exception.id}: ${exception.details}")
  (help "")
  (summary "")
  (http
    (code "200")
    (contact "For assistance, contact <a href='mailto:sysadmin@example.com'>sysadmin</a>")EOF
    (details "")
    (format <<EOF
<format removed>
  EOF
  )
  (help "")
  (summary "")
<built-in exceptions removed>
  )
)
```

Consider the following conditions when modifying installable lists:

- Every exception installable list must begin with a definition for `exception.all`.
- In the exceptions' installable list, all definitions must be enclosed by `exception.all` and its accompanying closing parenthesis:

```
(exception.all
(exception.policy_denied)
)
```

- Keep the definition strings under the enclosed parentheses short, no longer than one line if possible.
- Symantec strongly recommends downloading the existing exceptions installable list, then modifying it.

## Creating and Editing Exceptions

You can create or edit an exception with the CLI or through installable lists using the Management Console.

**Note:** You cannot create user-defined exceptions for patience pages.

### Using the CLI

To create or edit an exception using the CLI, issue the following commands:

```
# (config) exceptions
# (config exceptions) create definition_name
```



```
# (config exceptions) edit definition_name
# (config exceptions user-defined.definition_name) http-code HTTP_response_code
# (config exceptions user-defined.definition_name) inline ?
contact Set the $(exceptions.contact) substitution
details Set the $(exceptions.details) substitution
format Set the format for this exception
help Set the $(exceptions.help) substitution
http Configure substitution fields for just HTTP exceptions
summary Set the $(exception.summary) substitution
# (config exceptions user-defined.definition_name) inline contact eof
string eof
# (config exceptions user-defined.definition_name) inline details eof
string eof
# (config exceptions user-defined.definition_name) inline format eof
string eof
# (config exceptions user-defined.definition_name) inline help eof
string eof
# (config exceptions user-defined.definition_name) inline summary eof
string eof
```

To delete a user-defined exception, enter the following commands:

```
# (config) exceptions
# (config exceptions) delete exception_name
ok
```

**Note:** You cannot delete a user-defined exception that is referenced by policy. You must remove the reference to the exception from the policy before deleting the exception.

## Using the Management Console

The Management Console allows you to create and install exceptions with the following methods:

- Using the ProxySG Text Editor, which allows you to customize the existing exceptions file
- Creating a local file on your local system; the appliance can browse to the already created file and install it.
- Using a remote URL, where you place an already-created exceptions list on an FTP or HTTP server to be downloaded to the appliance.

When the Exceptions file is customized, it updates the existing exceptions already on the appliance. The configuration remains in effect until it is overwritten by another update; it can be modified or overwritten using CLI commands.

To install an exceptions definition using the Management Console:

## Symantec: A Division of Broadcom

1. Select **Configuration > Policy > Exceptions**.
2. From the Install Exceptions Definitions From drop-down list, select the method used to install the exceptions configuration.
3. Click **Install**.
  - Installing from a Remote URL: Enter the fully-qualified URL, including the filename, where the configuration is located. To view the file before installing it, click **View**. Click **Install**. View the installation status; click **OK**.
  - Installing by browsing to a Local File: Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **Close**.
  - Installing a policy file using the ProxySG Text Editor: In SDL format, create a custom policy to be installed (added to the existing exceptions file).
4. Click **OK**.

## Viewing Exceptions

You can view the exceptions defined on the ProxySG appliance, including how the defined HTML appears to users.

To view exceptions using the Management Console:

1. Select **Configuration > Policy > Exceptions**.
2. From the View Exceptions field, View File drop-down list, select the page to view.
  - Current Exceptions—Displays all of the exceptions as they are currently defined.
  - Default Exceptions Source—Displays the default exceptions.
  - Exceptions Configuration—Displays a page from which you can click links to view how exceptions appear in HTML to users.
  - Results of Exception Load—Displays the results of the last installable list load, including any errors and warning to be fixed.
3. Click **View**. A new browser appears with the current requested information.
4. Click **Apply**.

To view exceptions in the CLI, use the following commands:

```
# (config exceptions user-defined.test) show exceptions userdefined.test
$(exception.id):
test
$(exception.summary):
Connection failed
$(exception.details):
Connection failed with stack error
```

```
$(exception.contact):  
Tech Support
```

# Managing Peer-to-Peer Services

This section describes the ProxySG solution for managing and blocking peer-to-peer traffic.

## About Peer-to-Peer Communications

The use of peer-to-peer (P2P) technologies and services consumes an estimated 60% of broadband ISP bandwidth. By design, most P2P services are port-agnostic, which makes attempting to block them at the firewall extremely difficult. One peer finds another IP address and port that is willing to share the file, but different peers can use different ports. Furthermore, P2P is not based on any standards, which makes it nearly impossible for network administrations to control or even detect.

Although P2P provides some practical business uses in enterprises, unmanaged P2P activity creates risks:

- Excessive bandwidth consumptions affects mission-critical applications.
- Exponential security risk of exposure to viruses, spyware, and other malicious content.
- The threat of legal action concerning the unlawful downloading of copyrighted music and movies.

Managing P2P is a dynamic challenge, as the administrator must be able to evaluate both P2P use and enterprise requirements.

## About the ProxySG Solution

The ProxySG appliance recognizes P2P activity relating to P2P file sharing applications. By constructing policy, you can control, block, and log P2P activity and limit the bandwidth consumed by P2P traffic.

Neither caching nor acceleration are provided with this feature.

## Deployment

To effectively manage P2P activity, the appliance must be deployed to intercept outbound network traffic and the firewall configured to block outbound connections that are not initiated by the appliance.

- The appliance intercepts outbound TCP network connections, as routed through an L4 switch or an appliance in bridging mode.
- Configure ProxySG HTTP, SOCKS, and TCP tunnel services for destination ports to be monitored.
- Create firewall rules that allow only outbound connections that are initiated by the appliance.
- You can block all known P2P ports and define policy to stop P2P traffic attempting to come through over HTTP

**Note:** This features does not include additional configurations for intercepting or controlling UDP traffic.

## Policy Control

This section lists the policy used to manage P2P.

You can add the following objects to a Web Access Layer:

- "P2P Client" on page 60
- "Client Protocol" on page 87

### Supported CPL triggers:

- `http.connect=`
- `p2p.client=`

### Supported CPL properties:

- `force_protocol()`
- `detect_protocol.protocol()`
- `detect_protocol.[protocol1, protocol2, ...]()`
- `detect_protocol(all|none)`
- `detect_protocol(protocol1, protocol2, ...)`

The following properties can be used in conjunction with the P2P-specific CPL:

- `allow, deny, force_deny`
- `access_server(yes|no)`—If the value is determined as no, the client is disconnected.
- `authenticate(realm)`—Unauthenticated clients are disconnected.
- `socks_gateway(alias_list|no)`
- `socks_gateway.fail_open(yes | no)`
- `forward(alias_list|no)`—Only forwarding hosts currently supported by TCP tunnels are supported.
- `forward.fail_open(yes|no)`
- `reflect_ip(auto|no|client|vip|ip_address)`

For complete CPL references, refer to the *Content Policy Language Reference*.

## Policy Example

The following policy example demonstrates how to deny network traffic that the appliance recognizes as P2P:

```
<proxy>  
p2p.client=yes deny
```

## P2P History Statistics

You can construct policy that controls, blocks, and logs peer-to-peer (P2P) activity and limits the bandwidth consumed by P2P traffic. The following section explains how to view P2P statistics, using either the Management Console or the CLI.

Some P2P statistics (P2P client connections and total bytes sent and received over a period of time) can only be viewed through the Management Console (see "P2P Clients" below and "P2P Bytes" on the facing page).

## P2P Data

The P2P Data tab on the Management Console displays P2P statistics, either all P2P services at once or one service at a time.

The following table details the statistics provided through the Management Console **P2P Data** tab and the CLI.

### P2P Data Statistics

Status	Description
Current Tunneled Sessions	The current number of P2P client connections using native transport
Current HTTP Requests	The current number of HTTP requests from P2P clients
Total Tunneled Sessions	The cumulative number of P2P client connections using native transport since the appliance was last rebooted.
Total HTTP Requests	The cumulative number of HTTP requests from P2P clients since the appliance was last rebooted.
Total Bytes Received	The total number of bytes received from all P2P clients.
Total Bytes Sent	The total number of bytes sent to all P2P clients.

To view P2P data statistics:

1. In the Management Console, select **Statistics > Protocol Details > P2P History > P2P Data**. The default view shows all P2P protocols.
2. (Optional) To view the statistics for a specific P2P protocol, make a selection from the **Protocol** drop-down list.

## P2P Clients

The P2P Clients tab displays dynamic graphical statistics for client connections received in the last 60-minute, 24-hour, or 30-day period.

The P2P client statistics are available only through the Management Console.

To view P2P client statistics, select **Statistics > Protocol Details > P2P History > P2P Clients**. Optionally, to set the graph scale to a different value, select a value from the Graph scale should drop-down list.

## P2P Bytes

The P2P Bytes tab displays dynamic graphical statistics for the total number of bytes sent to and received from P2P clients in the last 60-minute, 24-hour, or 30-day period.

To view P2P byte statistics, select **Statistics > Protocol Details > P2P History > P2P Bytes**.

To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

## Proxy Authentication

While P2P protocols do not support native proxy authentication, most P2P clients support SOCKS v5 and HTTP 1.1 proxies. P2P proxy authentication is supported only for clients using these protocols (that are configured for proxy authentication).

For information about proxy authentication, refer to the *SGOS Administration Guide*. For a list of P2P clients suspected of not supporting SOCKS v5 with authentication, see the Release Notes for this release.

## Access Logging

P2P activity is logged and reviewable. Refer to the *SGOS Administration Guide*.

# Managing QoS and Differentiated Services

Policy files contain the policies (triggers and actions) that manage every aspect of the ProxySG appliance, from controlling user authentication and privileges to disabling access logging or determining the version of SOCKS.

This section describes how to create policy to manipulate Quality of Service (QoS) information.

## About the ProxySG Solution

The ProxySG appliance supports QoS detection, which is becoming a more prevalent control point for network layer traffic. Previously, the QoS information was lost—or not detected—when the appliance terminated the client connection and issued a new connection to server. QoS support allows you to create policy to examine the Type of Service (ToS) fields in the IP header to determine the QoS of the bits. The policy then either tests and matches ToS information and performs an action, or performs an action to manipulate ToS information based on something else in the rule (such as a user group).

You can apply QoS policy to any protocol supported on the appliance.

## About DSCP Values

Policy matches are based on Differentiated Services Code Point (DSCP) values, which network devices use to identify traffic to be handled with higher or lower priority. Identifying and matching values might trigger defined policy actions that either set a different DSCP value or preserve or echo existing DSCP values to use for outbound connections, thus regulating the QoS for different user classes (see descriptions in subsequent sections).

The ProxySG policy requests a QoS level. Whether or not a level of QoS can be achieved depends upon your network/router configurations, which must also allow the level of requested QoS.

ToS is an eight-bit field in the IP header; the first six bits are used and the final two are reserved for other TCP specification and control. The first six bits constitute the DSCP value. For most networks, the DSCP values adhere to a standard set. The following table lists these values.

Name	DCSP Value	Description
Default	000000 (0)	Best effort (Precedence 0)
CS1	001000 (8)	Precedence 1
AF11	001010 (10)	Assured Forwarding Class 1, Low Drop Rate
AF12	001100 (12)	Assured Forwarding Class 1, Medium Drop Rate
AF13	001110 (14)	Assured Forwarding Class 1, High Drop Rate
CS2	010000 (16)	Precedence 2
AF21	010010 (18)	Assured Forwarding Class 2, Low Drop Rate
AF22	010100 (20)	Assured Forwarding Class 2, Low Drop Rate



Name	DCSP Value	Description
AF23	010110 (22)	Assured Forwarding Class 2, Low Drop Rate
CS3	011000 (24)	Precedence 3
AF31	011010 (26)	Assured Forwarding Class 3, Low Drop Rate
AF32	011100 (28)	Assured Forwarding Class 3, Medium Drop Rate
AF33	011110 (30)	Assured Forwarding Class 3, High Drop Rate
CS4	100000 (32)	Precedence 4
AF41	100010 (34)	Assured Forwarding Class 4, Low Drop Rate
AF42	100100 (36)	Assured Forwarding Class 4, Medium Drop Rate
AF43	100110 (38)	Assured Forwarding Class 4, High Drop Rate
CS5	101000 (40)	Precedence 5
EF	101110 (46)	Expedited Forwarding—low drop rate, low latency
CS6	110000 (48)	Precedence 6
CS7	111000 (56)	Precedence 7

Before creating policy, verify that your network adheres to these values. Other DSCP values are possible. You can specify a numerical range from 0 to 63. However, Symantec recommends using the above classifications, as most applications are associated to these classes already, which makes defining policy an easier task.

The conceptual definitions of the different classes are:

- **Best Effort**—This is the default DSCP value if an application does not specify any quality of service. The network delivers these packets if it can, but with no special assigned priority. You can use other DSCP values to specify priorities that are either above or below the Best Effort class; however, in most cases DSCP is used to specify priorities that are better than Best Effort.
- **Class Selector**—These values are defined in RFC 2474 and are designed to be backward compatible with the older Precedence field defined in RFC 791. Larger precedence values indicate packets that are more important than packets with smaller values of precedence; therefore, low-valued packets are dropped when a link becomes congested. Most common, Precedence 7 is reserved for link-layer and routing protocol keep-alive messages, and precedence 6 is reserved for other IP routing packets, both of which must get through for the network to function correctly.
- **Assured Forwarding**—This is defined in RFC 2597. Assured Forwarding (AF) allows you to specify both the relative priority and the drop sensitivity of traffic with a Precedence class. For example, AF31 specifies low drop-rate with in the CS3 Precedence class.
- **Expedited Forwarding**—This is defined in RFC 2598. Expedited Forwarding (EF) is usually reserved for premium traffic, or traffic that requires a virtual leased line. This traffic is higher priority than AF, but lower priority than precedence 6 and 7 routing messages.

## About QoS Policy Tasks

This section describes what is achievable through QoS policy and provides basic examples.

### Testing Incoming QoS

Policy triggers test the incoming packets of a client request or a server response. After the appliance identifies the DSCP value, other policy in the rule dictates what, or if, any action is required. A common scenario is to create several bandwidth classes (Configure > Bandwidth Mgmt > BWM Classes) and allow the DSCP value to dictate which bandwidth applies to the transaction.

#### Example Policy

Three client connection DSCP Source objects associated with three bandwidth management level Action objects.

A example that tests QoS and assigns a BWM action

The above example generates the following CPL:

```
<Proxy>
  client.connection.dscp=(ef) limit_bandwidth.client.outbound(High)
  client.connection.dscp=(cs3,af31,af32,af33) limit_bandwidth.client.outbound(Medium)
  client.connection.dscp=(cs1) limit_bandwidth.client.outbound(Low)
```

### Caching Behavior

Detecting the QoS cannot occur for cached content. In the case of a cache hit, when no server connection is established, no server connection DSCP value is available for policy checks.

### Multiple Connections

Some services use multiple client to server connections. When a service uses multiple connections, the triggers to test the inbound DSCP value apply to the primary control connection, which is (usually) the first connection opened by the client and the corresponding connection (if any) opened to the server. For example:

FTP connections are comprised of a control connection and a data connection.

## Setting the Outgoing QoS

You can create policy to preserve, echo, or set the DSCP value.

### Preserving the DSCP Value

This is the default ProxySG appliance policy. Using the appliance as the frame of reference, the Preserve property instructs the appliance to preserve the incoming client DSCP values, on a per-packet basis, when making an outbound server connection and preserve the inbound server values when sending traffic back to the client.

Preserving is valuable for protocols that have multiple connections. For example, FTP connections consist of a control and a data connection; the independent connections might have a differing DSCP values. Preserving the FTP connections prevents the appliance from altering one or both of the connections and disrupting the FTP protocol transmission.

While the default policy of preserving the QoS level passes traffic through without any adjustments to QoS, this behavior is different than pre-SGOS 5.1.3 behavior in which QoS data was lost at the point where the appliance intercepted the traffic. The preserve property allows for the monitoring of QoS-related network information.

The appliance preserves client-to-server and server-to-client DSCP values (default)

## Example Policy

```
<proxy>
  client.connection.dscp(preserve) server.connection.dscp(preserve)
```

## Echoing the DSCP Value

Echoing is similar to preserving in that the outbound DSCP value remains the same as the inbound connection. The difference is that the point of reference is the appliance, not specifically the client-to-appliance connection. When policy is set to echo, the appliance returns the client's inbound DSCP back to the client or returns the server's inbound DSCP back to the server.

A deployment for which echoing is useful is reverse proxy, in which you want to let the client select the DSCP value in its request and then echo the reply back to that client with the same DSCP, even if the server does not set any DSCP on the packets it sends to the proxy.

The following diagram illustrates two different connections. The blue arrows represent a connection initiated by a client, with the policy set to echo. The red arrows represent a connection initiated by server, again with policy set to echo. Regardless of the DSCP value of the response, the QoS of the appliance back to the initiator remains the same as the sent value.

## Example Policy

```
<proxy>
  user=A client.connection.dscp(echo)
```

## Setting the DSCP Value

QoS policy properties allow you to set outgoing (with the appliance as the point of reference) DSCP values. At present, the appliance supports setting one DSCP value for all connections in a transaction (the only exception is the preserve property). If a cache hit occurs for one of the connection types, thus negating the requirement for a server connection, the default value (Best Effort) is assigned.

## Real Solutions: Combining QoS Policies

Applying QoS policies to different connections in your network helps control traffic network traffic flow. Consider the following example:

A branch sales office is comprised of a VP of Sales and various sales personnel. The VP requires a moderately higher QoS server connection.

## Symantec: A Division of Broadcom

The office has an appliance deployed as its WAN proxy.

At the core offices, a ProxySG appliance 810 fronts a database server farm, which contains inter-company collateral.

Therefore, the policy instructs the appliance to echo the connections between the clients and the proxy; that is, they receive the same QoS level as they requested over the WAN. Then, the policy instructs the appliance to make the server connection with a QoS level of CS2, except when user VP\_Sales is identified. The VP is granted a QoS level of CS4, which in this case is defined as a higher QoS than CS2. The following diagram illustrates this example.

Setting DSCP values, based on user level, from the appliance to users

### Example Policy

```
<proxy>
  client.connection.dscp(echo)
  user=vp_sales server.connection.dscp(CS4)
  server.connection.dscp(cs2)
```

## DSCP for ADN Tunnels

Through policy, you can manage DSCP values for upstream and downstream server connections over ADN tunnels.

## Policy Components

You can use the following VPM objects to write DSCP policy:

- Objects (the cross-references are to the object descriptions in Chapter 3: "The Visual Policy Manager" on page 33):
  - Web Access and DNS Access layers: "Client Connection DSCP " on page 54 source object
  - Web Access, DNS Access, Web Content, and Forwarding layers: "Server Connection DSCP" on page 80 destination object
  - Web Access and DNS Access layers: "Set Client Connection DSCP " on page 116 action object
  - Web Access and Forwarding layers: "Set Server Connection DSCP " on page 121 action object
  - Forwarding layer: "Set ADN Connection DSCP" on page 114 action object

## CPL Components

The following are the CPL triggers and properties:

### Triggers

- `client.connection.dscp = 0..63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | best-effort | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef`

Valid layers: <proxy>, <dns-proxy>, <forward>

- `server.connection.dscp = 0..63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | best-effort | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef`

Valid layers: <proxy>, <dns-proxy>, <cache>

## Properties

- `adn.connection.dscp(0..63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | best-effort | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | preserve)`

Valid layers: <forward>

- `client.connection.dscp(0..63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | best-effort | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | echo | preserve)`

Valid layers: <proxy>, <dns-proxy>

- `server.connection.dscp(0..63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | best-effort | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | echo | preserve)`

Valid layers: <proxy>, <dns-proxy>, <cache>, <forward>

## Access Logging

The following access log formats are associated with QoS activity:

- `x-cs-connection-dscp`: The incoming client DSCP value.
- `x-rs-connection-dscp`: The incoming server DSCP value.
- `x-sc-connection-dscp-decision`: The `client.connection.dscp` () property value, or preserve or echo.
- `x-sr-connection-dscp-decision`: The `server.connection.dscp` () property value, or preserve or echo.

# Providing Read-Only Access in the Management Console

This section describes how you can provide a user with read-only access in the Management Console. You can use any realm that supports BASIC credentials such as Local, Windows SSO, Novell SSO, LDAP, IWA, RADIUS, to log in administrative users.

This example uses the local realm so that on-box authentication is always available. When an external authentication server is used, the user is denied access to the Management Console, if the authentication server cannot be accessed successfully.

To provide read-only access using a local realm, you need to perform the following tasks:

- Create a local realm.
- Create a list that includes usernames and passwords for members whom you wish to provide read-only access in the Management Console.
- Connect the list to the local realm.
- Create policy to enforce read-only access to members included in the list.

Use the steps below to complete the tasks detailed above.

Create a local realm:

1. Select the **Configuration > Authentication > Local > Local Realms** tab.
2. Click **New** to add a new realm. In this example the realm is named MC\_Access.
3. Using the CLI, create a list of users who need read-only access. The list must include a username and password for each user.
4. Enter configuration mode in the CLI; this example creates a list called Read\_Access.

```
#(config)security local-user-list create Read_Access
```

Edit the list to add user(s) and to create usernames and passwords. This example adds a user named Bob Kent.

```
#(config)security local-user-list edit Read_Access
#(config)user create Bob_Kent
#(config)user edit Bob_Kent
#(config)password 12345
```

5. Connect the user list (created in Step 2) to the local realm (created in Step 1).
6. In the **Configuration > Authentication > Local > Local Main** tab, select MC\_Access from the **Realm** name drop-down menu.
7. Select Read\_Access from the **Local** user list drop-down menu.

8. Use the for creating policy to enforce read-only access to the users in your list:
9. Launch the VPM.
10. Create an Admin Authentication Layer (or add a new rule in an existing layer). This layer determines the authentication realm that will be used to authenticate users who access the Management Console of the appliance.
11. Add a new Authentication action object. Select the local realm you created in step 1.
12. Add an Admin Access Layer with a **User** source object.
13. Enter the name of the user for whom you want to provide read-only access.
14. Click **OK** in both dialogs.
15. In the Action column, right click and select **Allow Read-only Access**.
16. Click **Apply Policy**.

The user can now log in the Management Console as a user with read-only access.

# Setting Policy for Content and Content-Type Filtering

Filtering on content and content type is a security feature that focuses on permitting or denying file downloads based on a variety of factors, such as file extensions, content-type, response headers, and apparent data type, to name but a few.

This section describes four techniques to consider when setting file filtering on the appliance:

- "Filtering Based on URL Extension" below
- "Filtering Based on HTTP Content-Type Response Header" on the facing page
- "Filtering Based on Apparent Data Type" on the facing page
- "Filtering Based on the http.response.data Condition" on the facing page

Each technique offers its own advantages and disadvantages; no single approach is better than another.

A sample configuration using some of the techniques listed above is provided. To view the sample configuration, see "Sample Configuration" on page 210.

The best practice for content and content-type filtering depends on the particular content type that you want to filter, and whether you are writing white-list or black-list style policy. As a result, you should consider using a combination of techniques for setting reliable policies that will effectively accommodate your organization's needs.

Although the suggestions for implementing content and content-type filtering should offer added protection to your network, you might want to also consider using an ICAP server, which offers more reliable protection.

In addition to filename extensions and content analysis, the intrinsic behaviors of browsers and platforms—and the different ways they deal with files—should also be considered when setting policies for your organization. For the purpose of this discussion, however, browsers and platforms are not being discussed.

You can define policy from both the Web Access Layer and the Web Content Layer:

- Rules defined in the Web Access Layer apply only when a client (such as a browser) accesses content.
- Rules defined in the Web Content Layer apply to the accesses noted above, but also when the appliance makes its own accesses to content to refresh its cache.

A browser that requests data through the appliance will always hit the <proxy> and <cache> layers if the layer guards are set to permit this condition. For more information on layer guards, refer to the *Content Policy Language Reference*.

## Filtering Based on URL Extension

Content filtering based on URL extension enables you to block files based on their filename extensions, such as .exe or .jpg. Although a common approach for filtering content, filtering based on URL extension is fairly unreliable, and the level of unreliability depends on the type of content you are filtering.



Filtering based on filename extensions is subject to false negatives, whereby the intended results differ from the actual results because the appliance fails to block the intended content. This is due to an unreliable relationship that exists between the syntax of the URL and the type of content being returned. Content that has an extension that does not match the actual content type will not be blocked when performing content filtering based only on URL extension. For example, blocking URLs with a .php extension will not block PHP content that has been given a different extension that has not been blocked.

Filtering based on filename extensions is also subject to false positives, whereby the intended results differ from the actual results that can occur when filename extensions are blocked. For example, perhaps you want to block Windows executable (.exe) files. If you simply block the .exe file extension, you might also block certain URLs that include executables as part of their URL path, for example `http://example.com/scripts/example.exe?a=1&b2`. These executables are used by the Web server to service a request. By blocking the Windows executable files, you inadvertently also block the legitimate URL executable files.

The main advantage of filtering based on the URL extension is that it can be done without contacting the origin server. All information required to process or deny the request URL condition is present in the client's request. Responses that are retrieved from the origin server are cached and can be returned by the appliance if another request for the URL's content is made.

## Filtering Based on HTTP Content-Type Response Header

Filtering based on HTTP Content-Type response header is generally more reliable than filtering based on URL extension, but this technique is also unreliable.

For example, consider a Web site developer who might not set the Content-Type header correctly for dynamically generated content. The actual results might be HTML text, even though returned content type claims to be text/plain.

For some content types, you might find multiple MIME types with the same meaning, which could result from a difference in spelling or using different names for the same content type.

In cases where URL extension filtering is accurate, the data returned is of a type that is generally denoted by that extension. In cases where the HTML header is accurate, the data returned is generally considered to qualify under that content-type classification.

## Filtering Based on Apparent Data Type

The Apparent Data Type feature identifies data content associated with Microsoft DOS and Windows executable files. Filtering based on apparent data type examines up to the first 256 bytes of data, then attempts to determine whether the content is a Windows executable or cabinet file. When used in a deny policy, the purpose of this object is to deny executable downloads and block drive-by installation of spyware.

## Filtering Based on the `http.response.data` Condition

Filtering based on the `http.response.data` condition in CPL is for advanced users who have expertise with file formats and regular expressions. Using CPL, you must define a substring or regular expression to match up to the first 256 bytes of the content type that you want to block.

The `http.response.data=` condition is defined in the *Content Policy Language Reference*.

## Sample Configuration

Company ABC wants to define rules that will identify and block video files. To do this, they will need to define rules to block file extensions, HTTP MIME Types or response headers related to the video type. They use a ProxySG appliance to implement this policy. To define their policy needs, Company ABC will need to define the following:

- In the Web Access Layer, define a rule identifying the file extensions to block.
- In the Web Access Layer, define a rule identifying the HTTP MIME types to block.
- If there are other video MIME types that are not listed in the rule above, you can define additional rules that match on the Content-Type response header in the Web Access Layer to block this content.

Although the product has the ability to filter based on apparent data types, the currently supported apparent data types do not match video content. As a result, that feature will be omitted from this example.

The following procedure focuses on the settings that are required to successfully implement Content-Type filtering. It does not fully describe the more intuitive wizard steps associated with the policy definition process. See "VPM Overview" on page 19 for specific details on configuring layers, rules, and objects.

To configure this policy, do the following:

1. Launch the VPM.
2. Define a rule identifying the file extensions to block:
  - a. Add a Web Access Layer. Because this policy is concerned with blocking certain files from entering the network, the Source information can be ignored.
  - b. Set a **File Extensions** destination object that contains the desired file extensions.
  - c. Add a **Deny** action object to block access to the content.
  - d. (Optional) Set a **Track** action and add comments.
3. Define a rule identifying the HTTP MIME types to block:
  - a. Add a new rule with an **HTTP MIME Types** destination object. Select the HTTP MIME types from the list, for example, video/x-ms-wmv.
  - a. Add a **Deny** action object to block access to the content.
  - b. (Optional) Set a **Track** action and comments.
3. Perform the following step if the Content-Type you want to filter is not listed in the HTTP MIME Type options:
  - a. Add a rule with a **Response Header** destination object. Specify whether to show All, Standard, or Custom header names. The Show selection filters the list of options that appear in the Header Name drop-down list. From the Header Name drop-down list, select Content-Type.

- b. Enter header regular expression information in the Header Regex field, for example, video/h264. You can add additional rules of this same type for any other Content Types to block that do not appear in the original HTTP MIME Type rule.
  - c. Add a **Deny** action object to block access to the content.
  - d. (Optional) Set a **Track** action and add comments.
4. Click **Apply Policy**.