SGOS 5 Series
Developed using SGOS 5.3.1.4

Implementing Exception Pages

What are Exception Pages?

Exception pages are Web pages (messages) sent to users under specific conditions. The ProxySG offers multiple built-in exception pages that you can modify for your company's particular needs. Default pages include `authentication_failed`, `policy_denied`, and so on (you can see the full list using the Management Console by going to **Policy > Exceptions** and clicking **View** for **Current Exceptions**). Additionally, you can define custom exception pages. These pages can reference substitution variables such as authenticated username, client IP address, time, date, and so on. This document describes how to create custom exception pages that can be used in a policy.

Note: *The **Notify User** action object available in policy allows for the customizing of the HTML users receive when the policy is triggered. These are created with combinations of policy and exception pages. For information on creating standard Coaching, Splash or Compliance notification policies and pages, see the ProxySG technical brief "Creating Notification Policies: Coaching, Splash, and Compliance."*

Why Implement Exception Pages?

Exception pages provide user feedback during error conditions as well as being a tool to implement advanced policies (such as notify actions). For example, you can create an exception page that warns users about the Web site they are attempting to access and sets a cookie so a different exception page (perhaps with a more severe warning for repeat offenders) displays if the policy is triggered again. Or exception pages for common errors can be customized to provide end user troubleshooting/reporting instructions.

How it works

Exception pages are returned to a Web browser request in place of the requested content. When a policy rule's conditions are met, and the exception action enabled, the proxy returns the exception content with appropriate substitution variables to the end user. The browsing application treats this as a response from the origin server. Depending on the type of exception, the browser may display the contents of the page, follow a redirection URL to another page, or display an error message to the user. User transactions that result in an exception can be logged, allowing tracking of notification and other interactions as required by corporate policy.

Installing Custom Exception Pages Overview

Custom exception pages are implemented by first creating an HTML file with acceptable variables and installing it to your ProxySG, then launching the Visual Policy Manager (VPM) and configuring a Web Access layer that specifies a **Destination** (the policy trigger), and an **Action**. Your Web Access Layer can also trigger the exception based on **Source**, (for a specific user or group), **Time**, or **Service**.

Exceptions may only be returned on connections the ProxySG has intercepted. To do this, go to **Services > Proxy Services**, select the service (such as HTTP), set it to **Intercept**, and click **Apply**. For the exceptions to be successfully returned on HTTPS traffic as well, the service must be intercepting and an HTTPS-Intercept policy must trigger to decrypt the connection's SSL.

In order to record the user reaction to the exception, access logging must be enabled. To do this, go to the **Configuration > General > Access Logging** page, select **Enable Access Logging**, and click **Apply**.

About the Default Proxy Policy

On the Management Console **Configuration > Policy > Policy Options** page you can set the default policy option to **Deny** or **Allow**. The two options provide two different approaches; however, as the **Return Exception** action object does not modify the **Allow** or **Deny** state, the examples provided will function as expected within existing policy allow/deny settings. For more details on developing effective policies, see the Policy Best Practices tech brief.

About the Variables

The HTML code examples for the exception pages described in this document use a few common variables, defined below. For a full list of variables that may be used in policy messages, see the CPL Guide, Appendix D.

Variable	Creates
$(exception.details)	Detailed explanation text for the exception, often including other substitution variables such as the URL-hostname and category.
$(exception.contact)	The name/email of the of the policy administrator
$(client.address)	The IP Address of the requesting machine
$(user)	The name of the requestor
$(url.host)	The requested URL's hostname portion. This is suggested in place of the full URL to avoid cross-site-scripting attacks.
$(category)	The category of the requested URL

About Exception Pages

Exception pages are defined within a hierarchy. There are two main types of exception pages in the hierarchy:

-> Built-in

-> User-defined

The general form of an exception definition is as follows:

```
(exception.<exception-id>
   (contact "") ; defines the $(exception.contact) variable
   (details "") ; the exception reason as $(exception.details)
   (format ""); defines the format of the on HTML exception
   (help "") ; defines the $(exception.help) variable
   (summary "") ; defines message for the $(exception.summary)
   (http ; specific settings for HTTP/HTTPS exceptions
   (code "") ; HTTP response code (typically 200, 307, or 403)
   (contact "" ; HTML specific contact info (ex: mailto link)
   (details "") ; HTML specific details text
   (format "") ; the HTML exception format with variables
   (help "") ; defines the $(exception.help) variable text
   (summary ""); a short name for the exception: $(exception.summary)
   )
   )
```

How to Implement Exception Pages

There are two parts to implementing exception pages

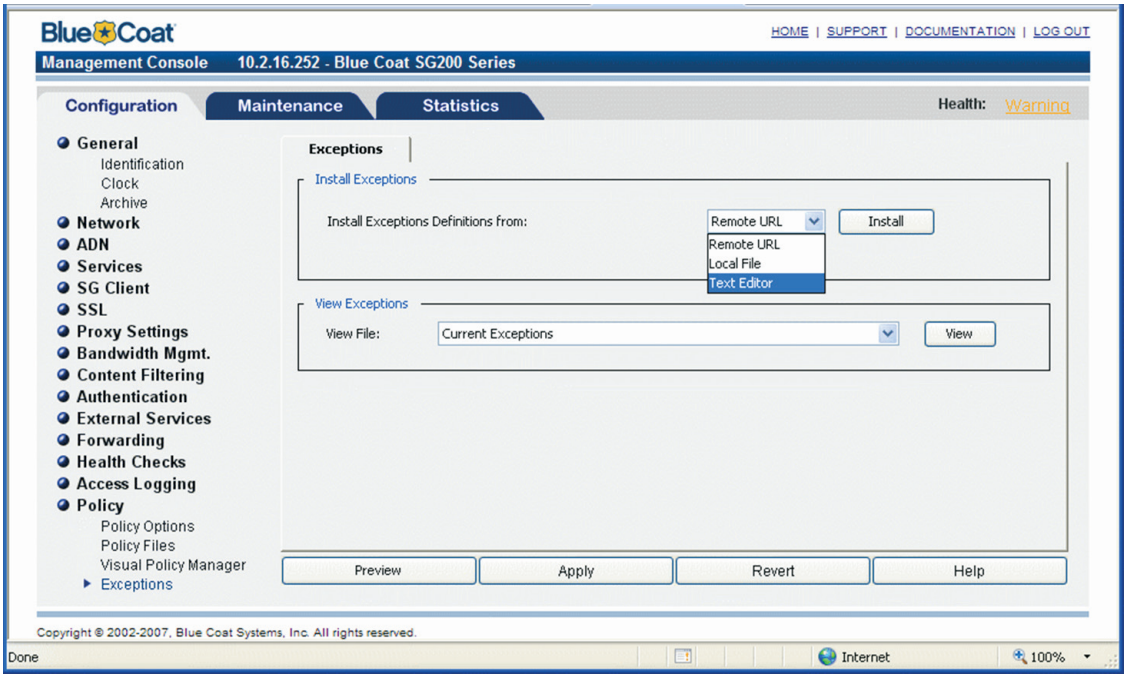
① Create the exception page as desired and install it on the ProxySG

② Create a policy referencing the exception page

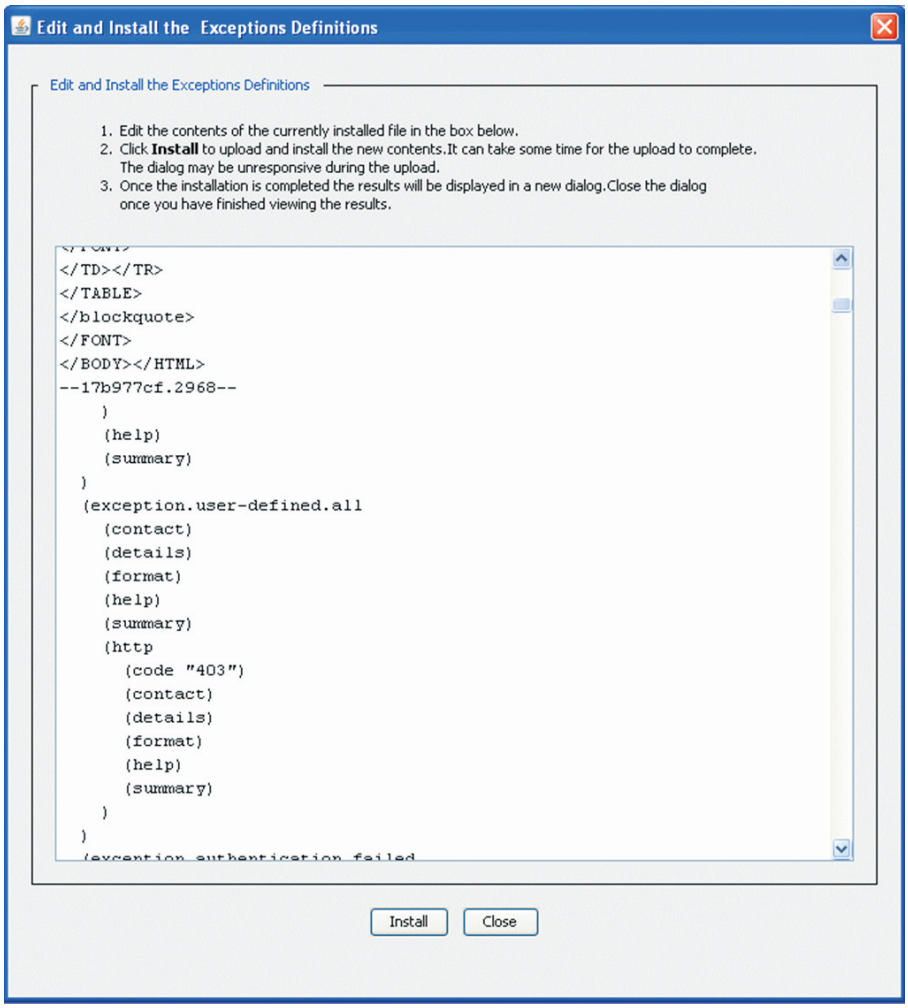
Part 1 – Create and Install an Exception Page

Once you have created the HTML exception page that you want (an example page is provided in step 2 below) you install it using the Blue Coat Management Console:

❶ Go to **Policy > Exceptions**.



2. Select **Text Editor** from the **Install Exceptions Definitions from** dropdown list and click **Install**. The **Edit and Install the Exceptions Definitions box** appears.



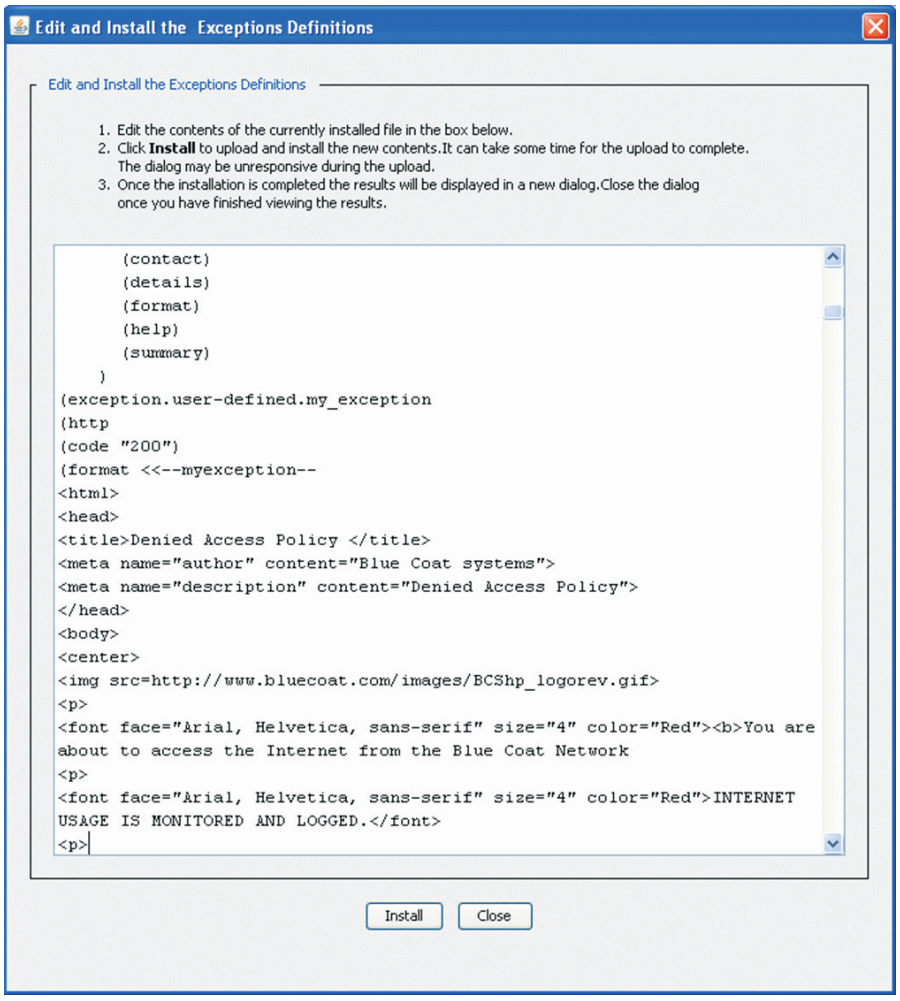
3. Scroll down until you find the following section. Insert your user-defined exception before the last "**)**" character where indicated below:

```
(exception.user-defined.all
   (contact)
   (details)
   (format)
   (help)
   (summary)
   (http
   (code "403")
   (contact)
   (details)
   (format)
   (help)
   (summary)
   )
   <---------------------- insert your custom-defined HTML exception page here
   )
```

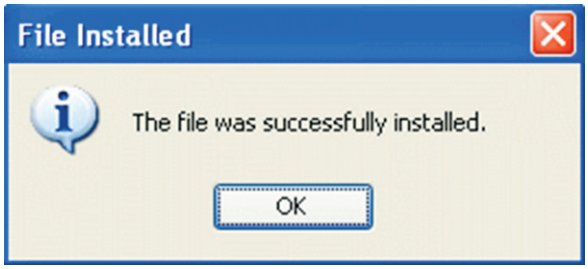
The example below is called `my_exception`. In the indicated section described above, add the following code and customize to suit your needs:

```
(exception.user-defined.my_exception
   (http
   (code "200")
   (format <<--myexception--
   <html>
   <head>
   <title>Denied Access Policy </title>
   <meta name="author" content="Example Company">
   <meta name="description" content="Denied Access Policy">
   </head>
   <body>
   <center>
   <p>
   <font face="Arial, Helvetica, sans-serif" size="4" color="Red"><b>You are about to access the Internet from the Example Company Network
   <p>
   <font face="Arial, Helvetica, sans-serif" size="4" color="Red">INTERNET USAGE IS MONITORED AND LOGGED.</font>
   <p>
   <font face="Arial, Helvetica, sans-serif" size="3" color="Red"><b> Your IP address: $(client.address)
   <br>Your username: $(user.name)</b></font>
   <p>
   <font face="Arial, Helvetica, sans-serif" size="4" color="red">YOU HAVE BEEN DENIED ACCESS TO THIS SITE. PLEASE READ OUR
   SECURITY POLICY AT http://intranet.example.com/up.html
   <p>
   For any comments email <A href='mailto:support@example.com?subject=Barred web page $(url), IP address: $(client.address), User ID:
   $(user)'>Customer Service Center</a></font>
   <p>
   </center>
   </body>
   </html>
   --myexception--
   )
   )
   )
```

4. Once you have pasted the code, click **Install** to save your changes.



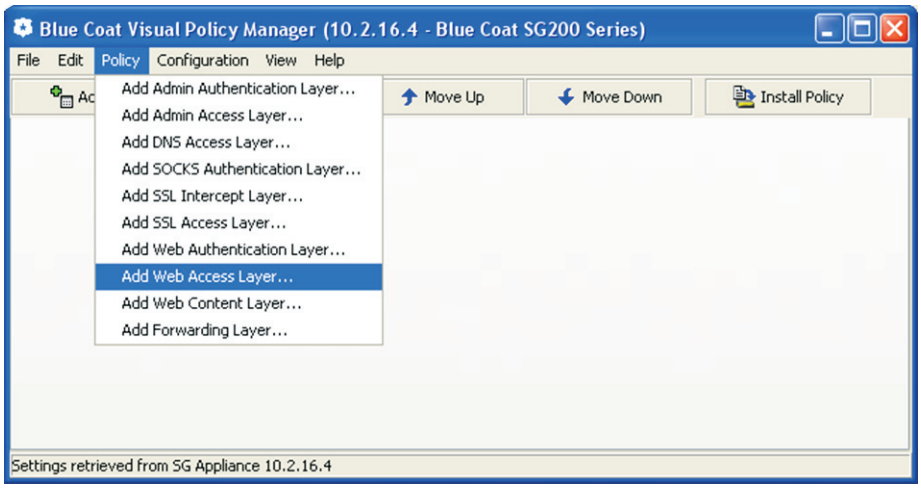
5. Click **OK** when you see the following successful installation message.



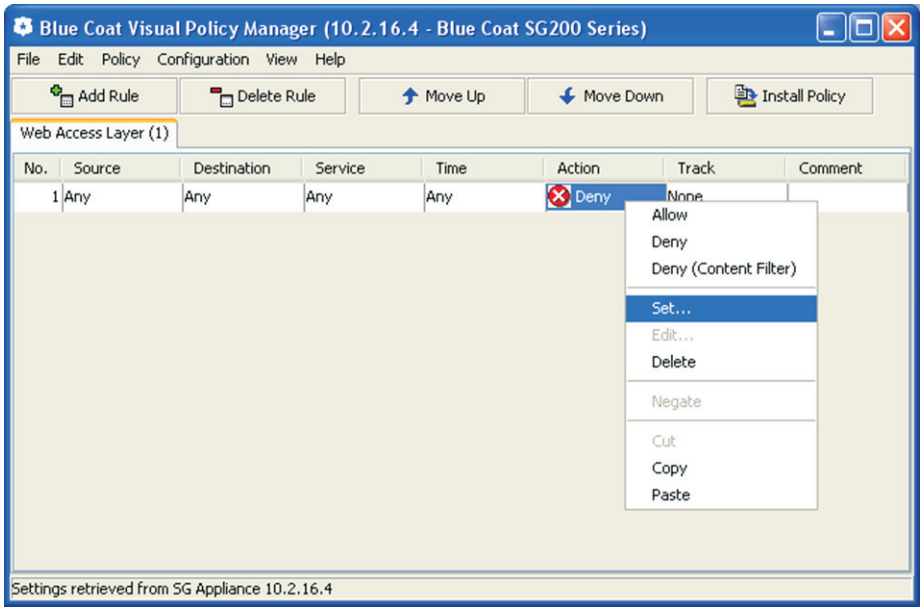
Part 2 – Create a Policy Referencing the Exception Page

1. Open the Visual Policy Manager from the Blue Coat Management Console: Go to **Policy > Visual Policy Manager** and click **Launch**.
2. In the **Policy** menu, click **Add Web Access Layer** to create a Web access policy. Name the layer appropriately, and click **OK**.

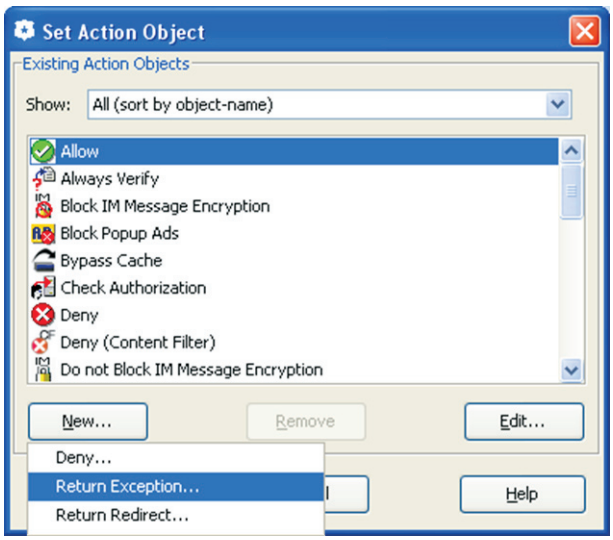
   NOTE: *To help maintain scalability, Blue Coat recommends giving relevant names to layers and objects.*



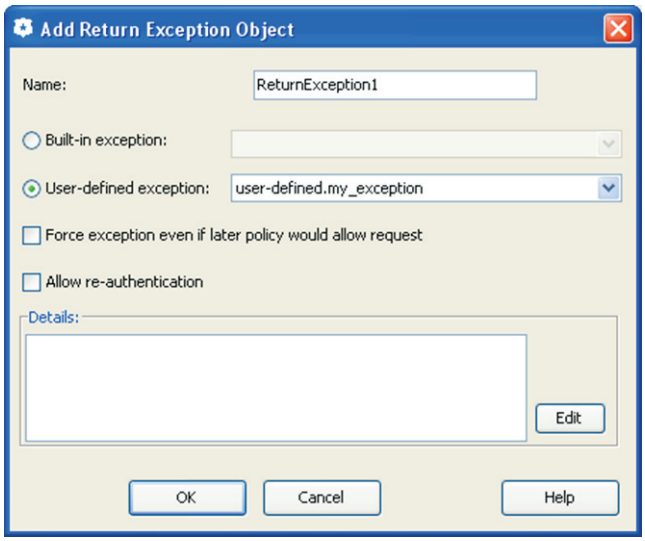
3. To define the action which returns your user-defined exception, right-click the **Action** setting and select **Set**. The **Set Action Object** box appears.



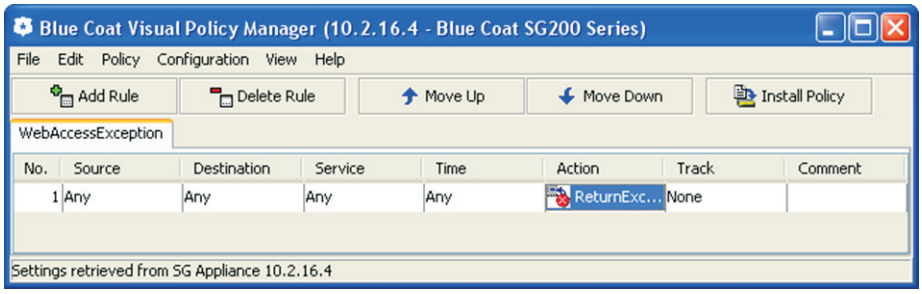
4. Click **New** and select **Return Exception**. The **Add Return Exception Object** box appears.



5. Select **User-defined exception**, pick your custom exception from the drop-down list, and click **OK** to return to the **Set Action Object** box.



6. The **Set Action Object** dialog appears with the newly defined action object. Click **OK** again to set the action object and return to the Visual Policy Manager.



7. Click Install Policy to install, and then click OK in the confirmation box. Close the Visual Policy Manager.

Test the exception page

To test the exception page, go to a URL denied by your policy and you see the custom HTML page; an example is shown here:

Conclusion

The Blue Coat ProxySG allows you to utilize exception pages to warn, advise, or require compliance from users. The administrator can make use of built-in exception pages that are pre-defined by the operating system or they can create their own custom exception pages. The ProxySG provides flexibility for a company to control users when accessing Web pages ensuring greater user productivity and compliance with corporate security policies.

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000