



## Creating SmartFilter Software Policies

---

This chapter provides information about creating SmartFilter software policies. It contains the following topics:

- [Configuring SmartFilter Software Policy Types, page 7-1](#)
- [Defining SmartFilter Software Policies, page 7-3](#)
- [Defining Available Forbidden File Extensions, page 7-9](#)
- [Controlling IP-Based URL Access, page 7-11](#)
- [Defining Search Sites, page 7-12](#)
- [Identifying Restricted Words and Phrases, page 7-15](#)
- [Creating a Message for a Coached Category, page 7-18](#)
- [Creating a Message for a Denied Category, page 7-19](#)

### Configuring SmartFilter Software Policy Types

SmartFilter software affords enterprise administrators the ability to compose multiple Internet filtering policies to meet the varying filtration requirements across an organization. You can configure SmartFilter software to perform these tasks:

- Create and specify a policy to Allow All, meaning that no blocking, coaching, or delay action is applied to any SmartFilter software category.
- Create and specify a policy to Deny All, meaning that all HTTP access is blocked.
- Create and specify a customized policy that affords blocking, coaching, and delay actions on a per category basis.

These policy types are exclusive. That is, only one can be selected at a time for any given policy. You can configure SmartFilter software to simultaneously have one or more Allow All, Deny All, and customized policies, but any single policy can be of only one type.

The most often employed policy type is the customizable policy. With customizable policies, the administrator can create policies with these unique features:

- Category blocking along with unique time of day (TOD) and day of week (DOW) specifications
- Category coaching with unique TOD and DOW specifications
- Category delay with unique TOD and DOW specifications

- File extension blocking with unique TOD and DOW specifications
- Blocking of personal page access with unique TOD and DOW specifications

## Precedence of Multiple Policies

Because SmartFilter software supports individual users belonging to multiple groups and allows different policies to be applied to different groups, it is possible that a user can have multiple, and possibly conflicting, policies assigned to them. To address this issue, SmartFilter software enforces precedence behavior defining what action is to be taken. [Table 7-1](#) shows that precedence.

**Table 7-1 SmartFilter Software Policy Precedence**

Condition	Effect
Users have one or more policies applied to them, one of which is the Allow All policy.	Access is allowed.
Users have one or more policies applied to them (not including the Allow All policy), one of which is the Deny All policy.	Access is denied.
Users are accessing a URL that has been exempted by the administrator, and none of the conditions above are true.	Access is allowed.
Users enter an IP-based URL, and these accesses have been denied globally, with none of the above conditions being true.	Access is denied.
The URL is in a category defined as blocked by one or more policies, and none of the above conditions are true.	The URL is blocked.
Access is to a file type that has been forbidden by one or more policies applied to the users, and none of the above conditions are true.	Access is blocked.
The access is a search word or phrase that has been denied by one or more of the policies applied to the users, and none of the above conditions are true.	The search site request is blocked.
The URL is in a category defined as coached by one or more of the policies, and none of the above conditions are true.	The URL is coached.
The URL is in a category defined as delayed by one or more of the policies, and none of the above conditions are true.	The URL is delayed by the amount specified for that category.
The access is to an uncategorized personal page and such accesses have been denied globally, with none of the above conditions being true.	Access is denied.

## Multiple URL Categorizations

A URL often has multiple categorizations in the SmartFilter list. This happens because the content of many sites legitimately falls into a number of categories. SmartFilter software policies allow administrators to define different actions for categories within a policy. Therefore, a single URL identified within multiple categories might have different, possibly conflicting, actions assigned to it. To address this, SmartFilter software enforces the following precedence of actions:

- Blocking takes precedence over coaching.
- Coaching takes precedence over delaying.
- Delay takes precedence over allowing.

## Defining SmartFilter Software Policies

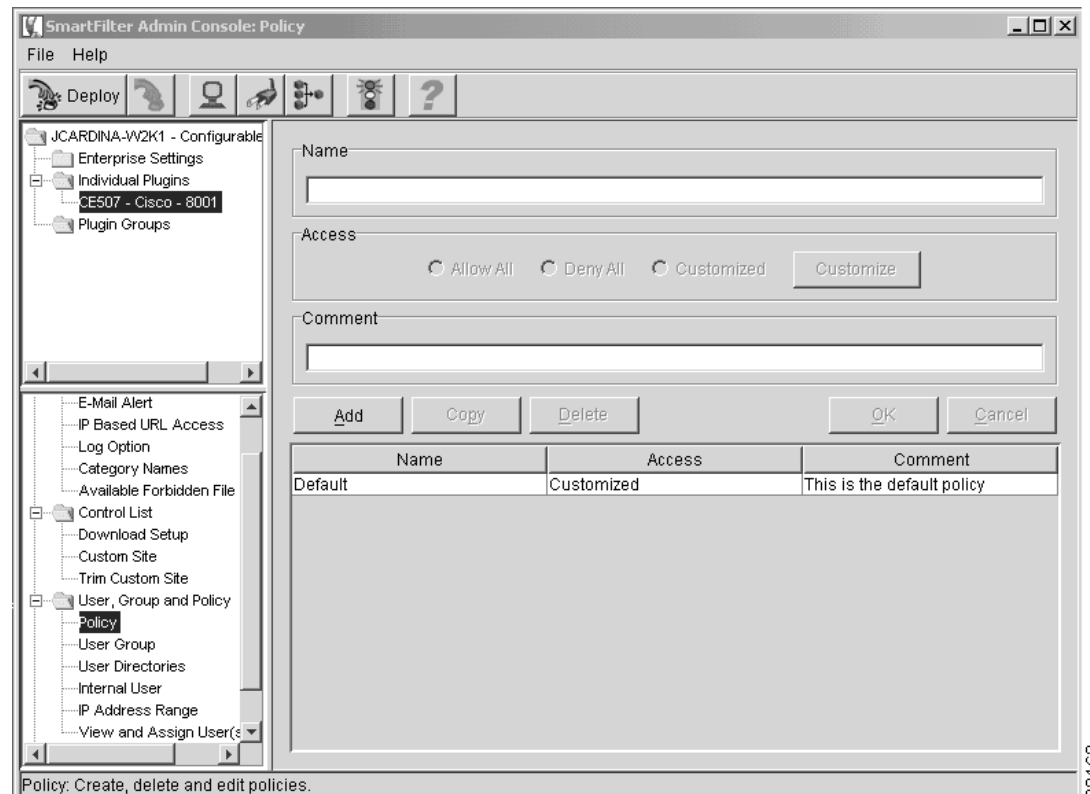
The Policy window, shown in [Figure 7-1](#), contains information about the SmartFilter software policies you have set up for your site.



Tip

SmartFilter software provides a default policy that denies access to the following categories 7 days a week, 24 hours a day: sex, nudity, drugs, criminal skills, hate speech, gambling, extreme, and anonymizers.

**Figure 7-1** Policy Window



83162

Use the Policy window for these tasks:

- [Defining a Deny All or Allow All SmartFilter Software Policy](#)
- [Defining a Customized Policy](#)
- [Copying a Policy](#)
- [Deleting a Policy from the List](#)

## Defining a Deny All or Allow All SmartFilter Software Policy

To add a Deny All or Allow All SmartFilter software policy, follow these steps:

- 
- Step 1** Click **Add**.
- The cursor moves to the Name field.
- Step 2** Enter the name of the policy.
- Step 3** Define the access for the policy by clicking either the **Allow All** or the **Deny All** radio button:
- Allow All—All HTTP traffic is allowed. This option takes precedence over the Deny All option.
  - Deny All—Blocks all HTTP traffic.
- The option you chose appears in the Access column of the table.
- Step 4** Click in the Comment field and enter a brief note about the policy. This step is optional.
- Step 5** Click **OK**.
- The policy you entered appears in the table.
- 

## Defining a Customized Policy

With SmartFilter software, you can easily tailor user access to the Internet to fit your organization's unique culture and objectives. Pick and choose the categories that you want to filter, coach, delay, or allow. From denying access to gambling sites and pornography to allowing access to travel sites during lunch hours, and delaying downloads from MP3 sites, SmartFilter software gives you flexibility and control.

SmartFilter software also provides ten user-defined categories that allow you to further tailor access by defining and filtering sites not included in the SmartFilter Control List. You can also exempt any site that you would like specific groups or individuals to access quickly and easily.

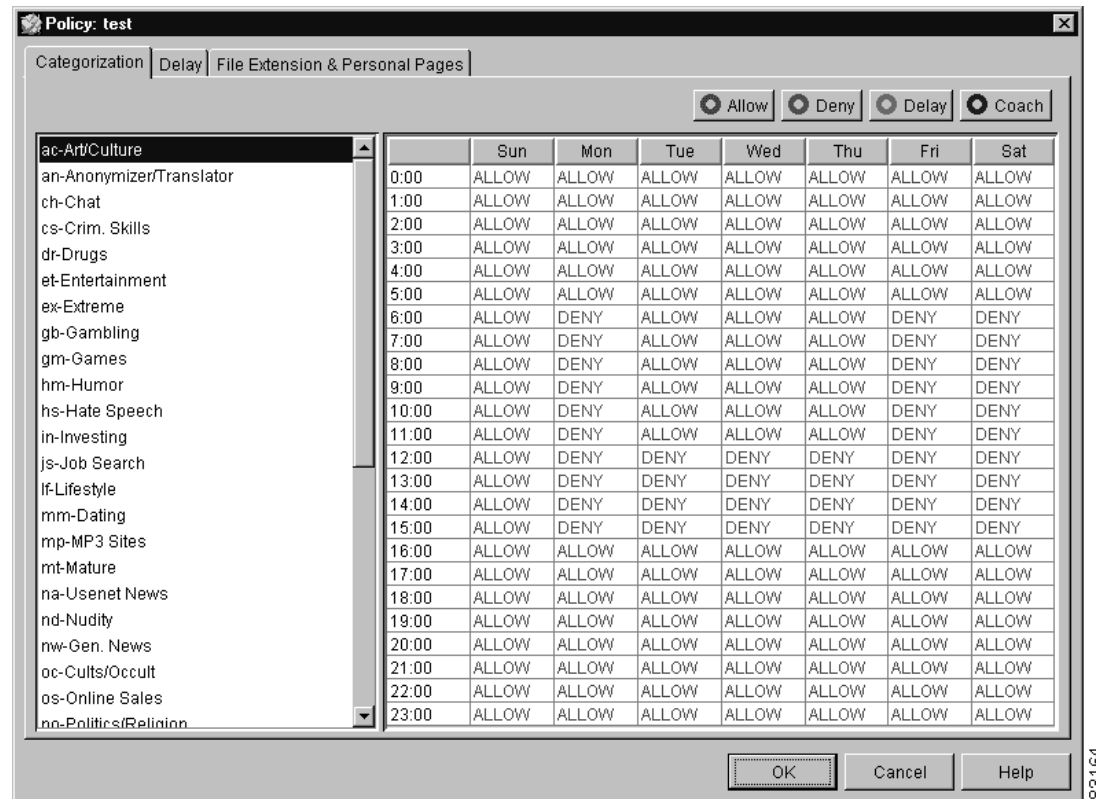
To define a customized SmartFilter software policy, follow these steps:

- 
- Step 1** In the SmartFilter Admin Console Policy window, click **Add**.
- The cursor moves to the Name field.
- Step 2** Enter the name of the policy.
- Step 3** Click in the Comment field and enter a brief note about the policy. This step is optional.
- Step 4** Define the access for the policy by clicking **Customized** radio button.

Step 5 Click **OK**.

The Categorization tab of the Policy Access window, shown in [Figure 7-2](#), appears.

**Figure 7-2** Categorization Tab of the Policy Access Window



## Configuring Access Parameters for Customized Policies

To configure the access parameters for customized policies, follow these steps:

Step 1 From the Categorization tab of the Policy Access window, choose the category.



**Note** You can choose multiple categories at a time by using the **Shift** or **Ctrl** keys.

Step 2 Choose the day of the week and the time of day for the policy by clicking in the field and dragging the mouse.

Step 3 Click one of the filter buttons at the top of the window.

- **Allow**—Allows access to the category you chose during the days and times you selected.
- **Deny**—Denies access to the category you chose during the days and times you selected.
- **Delay**—Delays access to the category you chose during the days and times you selected. The length of the delay time is configurable under the Delay tab.

- **Coach**—Provides coached access to the category you chose during the days and times you selected. Coached access means that you provide, through SmartFilter software, guidelines or special instructions to your users when they attempt to access a category to which you have assigned a coach policy.



**Note** Coaching works with all Internet Explorer browsers and with Netscape browsers, Version 6.0 or later.

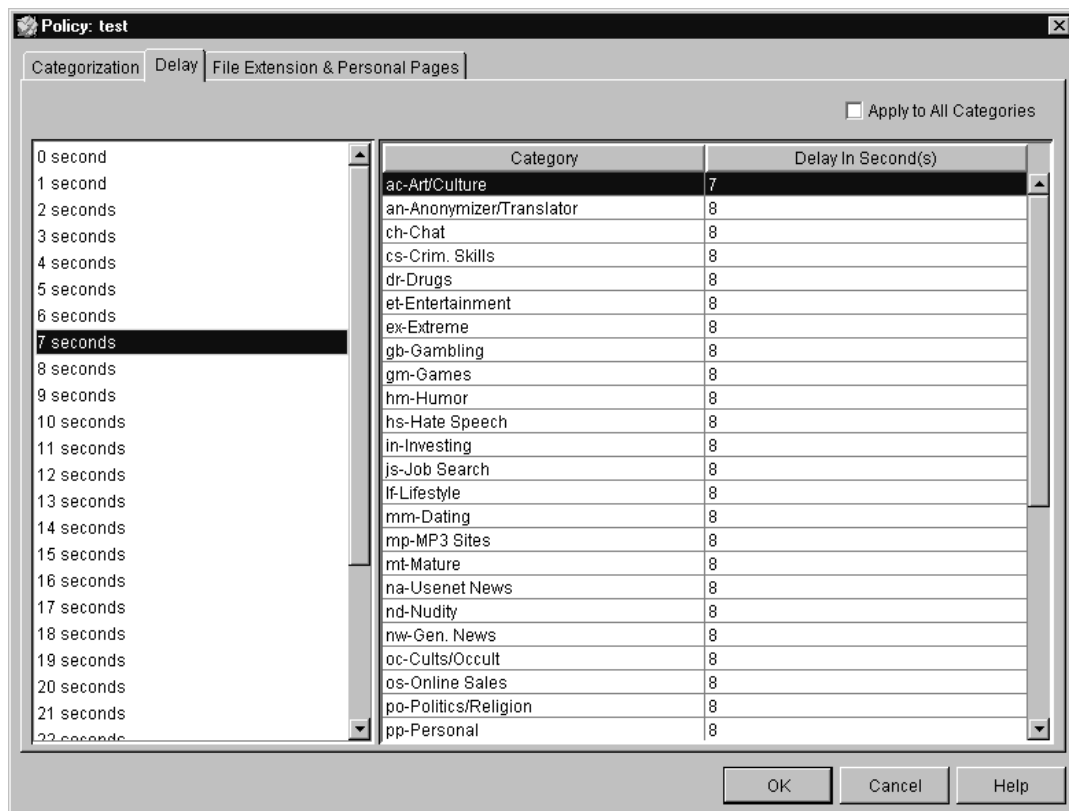
**Step 4** Repeat this step for each set of categories for which you want to customize access.

## Configuring Delay Time for Customized Policies

To configure the delay time for the customized policies, follow these steps:

**Step 1** Click the **Delay** tab, shown in [Figure 7-3](#), of the Policy Access window to adjust the default delay time of 0 seconds.

**Figure 7-3** Delay Tab of the Policy Access Window



**Step 2** Choose the category that you want to change.



**Note** If you want a time delay to apply to all categories, click the **Apply to All Categories** check box at the top of the window.

**Step 3** Choose a value from 1 to 30 seconds.

The value appears in the Delay in Second(s) column.



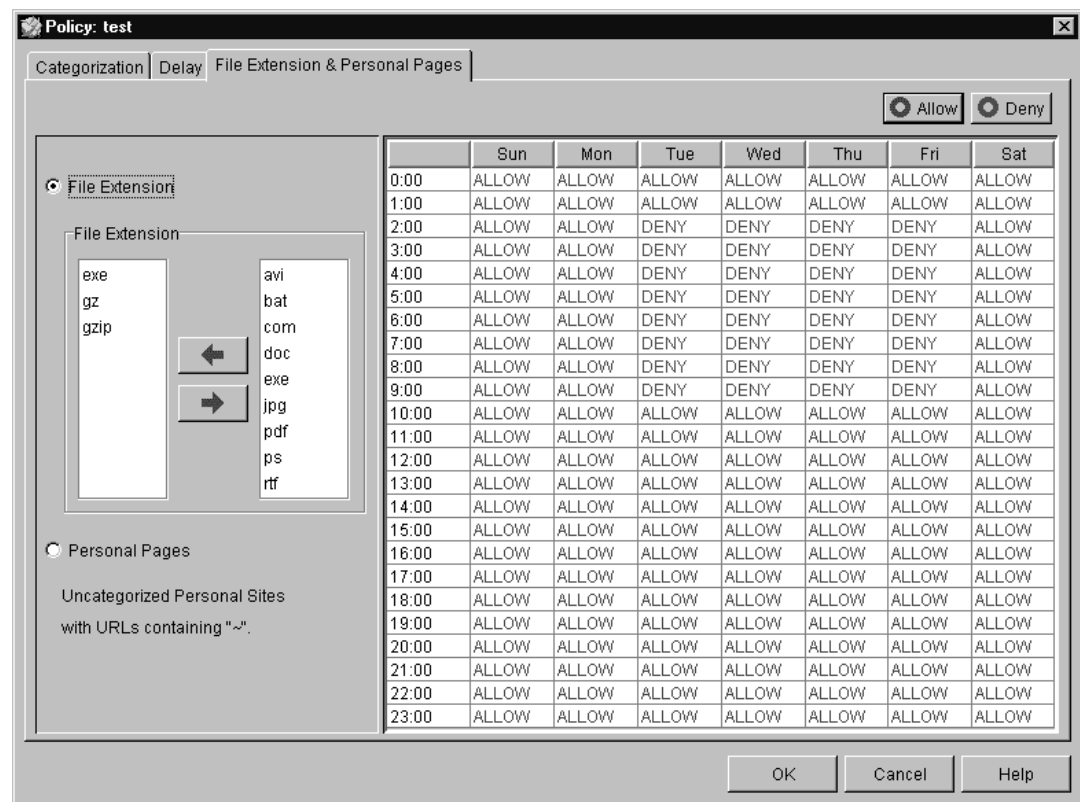
**Note** The length of the delay may be longer than expected because of multiple connections needed to obtain the various items on the page. For example, if there are ten images on a page and the delay is set at 10 seconds, the first page takes 10 seconds, followed by an additional 10 seconds for each image. This would result in a total delay time of 110 seconds for the page.

## Configuring File Extensions and Personal Pages for Customized Policies

To set parameters for file extensions or personal pages for customized policies, follow these steps:

**Step 1** Click the **File Extension & Personal Pages** tab of the Policy Access Window, shown in [Figure 7-4](#), to set additional parameters.

**Figure 7-4** File Extension Tab of the Policy Access Window



83166




---

**Note** If you wish to add a file extension that does not currently appear in the list, see the [“Defining Available Forbidden File Extensions”](#) section on page 7-9.

---

**Step 2** Click the **File Extension** radio button.

**Step 3** Choose one or more file extensions from the list in the File Extension area and click the **Left Arrow** button.

The file extensions you chose appear in the list on the left in the File Extensions area. Access parameters are applied to any files having the file extensions that you chose. Access to all files with the extensions you have chosen in this step is either allowed or denied based on the day of the week and the time of day you choose in [Step 4](#) and the policy option you choose in [Step 5](#).




---

**Note** If you want to remove a file extension from the list on the left, choose it and click the **Right Arrow** button.

---

**Step 4** Choose the day of the week and the time of day for which you want to set the policy by clicking in the field and dragging the mouse.

**Step 5** Click **Allow** or **Deny** at the top of the window.

- Allow—Allows access to the file extension that you chose during the days and times you selected.
- Deny—Denies access to the file extension that you chose during the days and times you selected.

**Step 6** Click the **Personal Pages** radio button.

Personal pages are defined as personal sites that are identified by a tilde (~) in the URL of the personal site.




---

**Note** This option does not refer to the Personal Pages category. It refers instead to uncategorized URLs that contain a tilde (~).

---

**Step 7** Choose the day of the week and the time of day for which you want to set the policy by clicking in the field and dragging the mouse.

**Step 8** Click **Allow** or **Deny** at the top of the window.

- Allow—Allows access during the days and times you chose.
- Deny—Denies access during the days and times you chose.

**Step 9** Click **OK**.

The Policy window, shown in [Figure 7-1](#), reappears.

---

## Copying a Policy

Copying an existing policy is particularly useful if you are creating customized policies that are similar but not exact. To copy an existing policy in the Policy window (see [Figure 7-1](#)), follow these steps:

- 
- Step 1** Choose the policy that you want to copy.
- Step 2** Click **Copy**.
- The information associated with the policy (name, access, and comment) appears in the fields.
- Step 3** Enter a new name for the policy.
- Step 4** Click **OK**.
- Step 5** Choose the policy you just named.
- Step 6** Enter the information for the new policy.
- Enter a new comment.
  - Define the access.
- Step 7** Click **OK**.
- 

## Deleting a Policy from the List

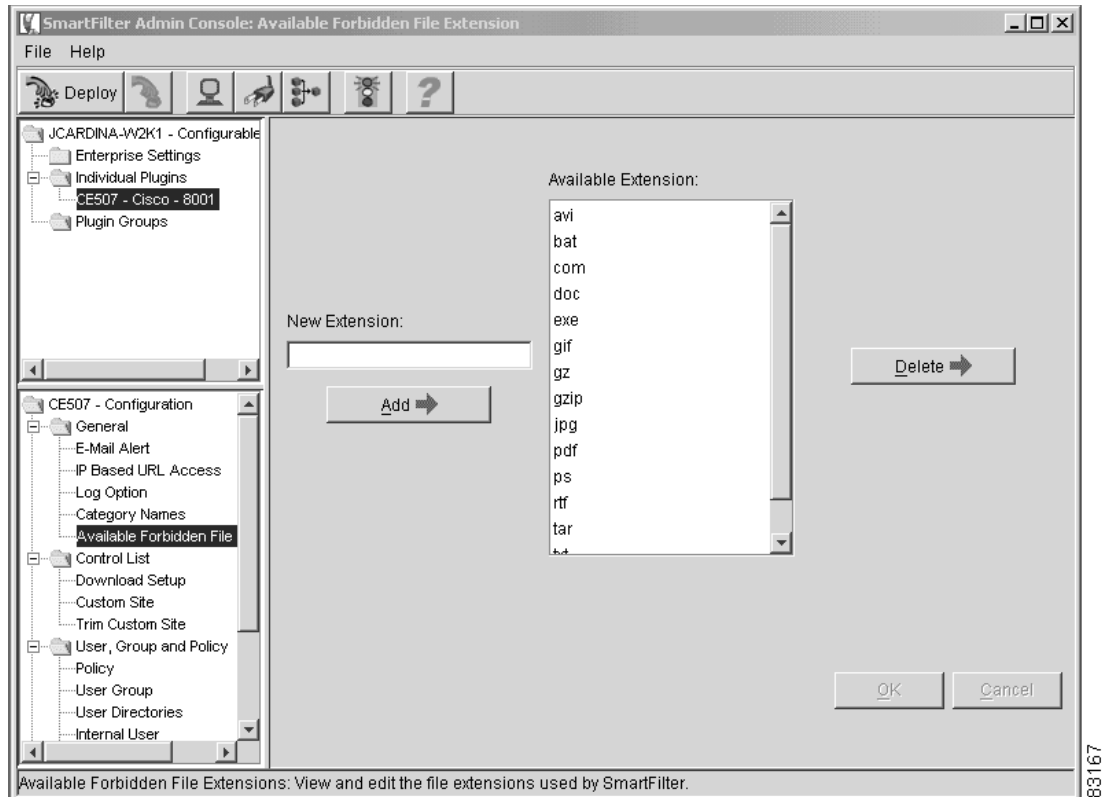
To delete a policy from the Policy window (see [Figure 7-1](#)), follow these steps:

- 
- Step 1** Choose the policy that you want to delete.
- Step 2** Click **Delete**.
- A warning or confirmation message appears, asking if you are sure you want to delete the policy.
- Click **Yes** to delete the policy from the table.
  - Click **No** to leave the policy in the table.
- 

## Defining Available Forbidden File Extensions

You can block URL access based on the file extension being referenced in the request. The Available Forbidden File Extension window, shown in [Figure 7-5](#), displays the file extensions that are available to be classified as forbidden. SmartFilter software defines several default forbidden file extensions.

Figure 7-5 Available Forbidden File Extension Window



You can block individual file extensions on a policy-by-policy basis. To forbid file extensions, see the [“Defining a Customized Policy”](#) section on page 7-4.

## Adding File Extensions to the List

To add file extensions to the list, follow these steps:

- 
- Step 1** Click in the New Extension field.
- Step 2** Enter the file extension that you want to forbid.
- Be sure to omit the dot (“.”) when entering the extension. For example, if you want to add GIF files to the list, enter “gif” and not “.gif.”
- Step 3** Click **Add** >.
- The extension you entered is added to the list.
- Step 4** Click **OK**.
-

## Removing File Extensions from the List

To remove a file extension from the list, follow these steps:

**Step 1** Click the file extension you want to delete from the list.

**Step 2** Click **Delete** >.

The extension that you chose is removed from the list.



**Note** You do not receive a warning message.

**Step 3** Click **OK**.

## Controlling IP-Based URL Access

The IP-Based URL Access window, shown in [Figure 7-6](#), contains information about how your site controls access to URLs by IP address. The default configuration denies URL access by IP address. You can change the configuration, however, to allow URL access by IP address by clicking one of the following radio buttons:

- Allow—Allows all IP address URLs.
- Deny—Denies all IP address URLs.



**Tip**

Choosing **Deny** means that any URL that contains IP addresses are blocked. If you want to allow access to valid sites by their IP addresses, exempt those sites by configuring the Custom Site window.

- Lookup—Performs a reverse lookup on the IP address. It then queries the Control List based on a new URL created by replacing the IP address of the original URL with the result of the reverse Domain Name System (DNS) lookup.

If you choose **Lookup**, the Lookup Failure Default options become available.

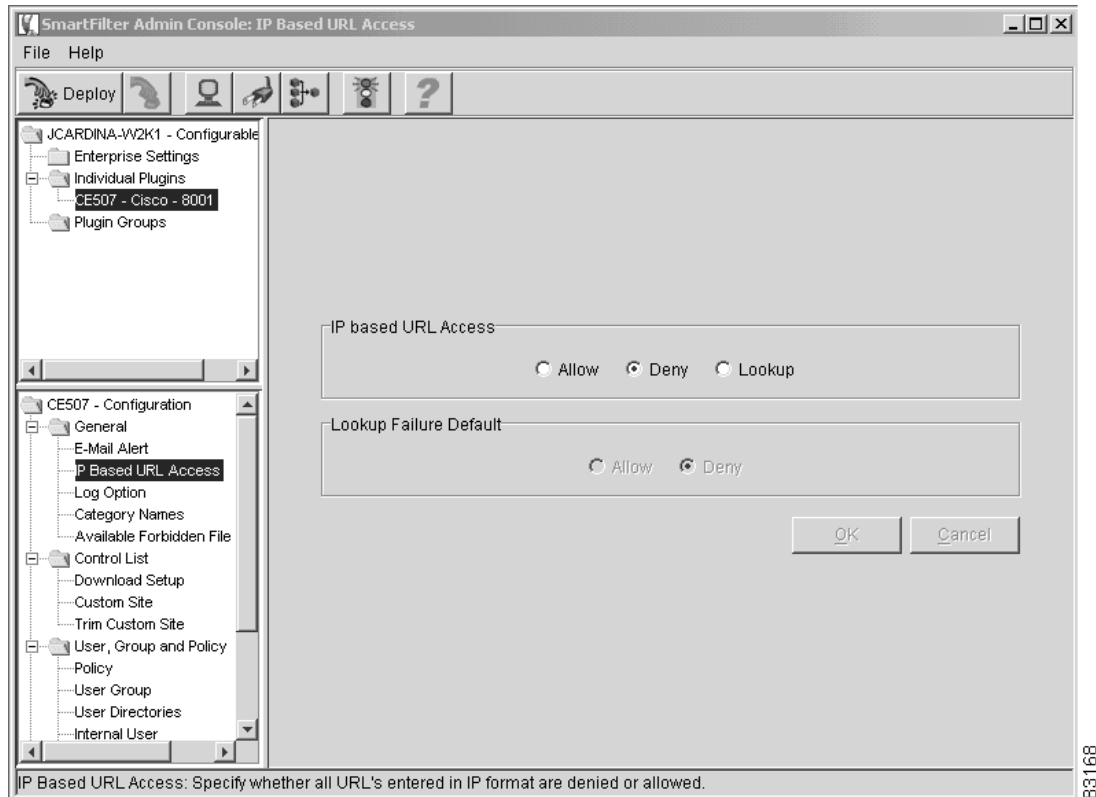
- Allow—Allows any IP address that fails a reverse DNS lookup.
- Deny—Denies any IP address that fails a reverse DNS lookup.



**Tip**

It is recommended that you set the Lookup Failure Default option to **Deny**.

Figure 7-6 IP-Based URL Access Window



## Defining Search Sites

The Search Site window, shown in [Figure 7-7](#), identifies a list of search engines and their Common Gateway Interface (CGI) keywords. The Search Site window works together with the Restricted Phrase window.

If the search site and its CGI keyword that you want to restrict are not in the list provided by SmartFilter software, you can determine the CGI keyword by going to the search site and entering a text string. When the search results window appears, look at the resulting URL. The characters directly before the text string in the URL make up the CGI keyword. For example, if you use Lycos to search for the word “stamps,” a portion of the URL is “?query=stamps.” The CGI keyword is “query=.”

If you have not configured a search engine and defined its corresponding CGI keyword, no action is taken for that search engine, even if you have defined restricted words or phrases. For example, if you have configured yahoo.com and defined its corresponding CGI keyword and a user tries to search for a restricted word or phrase using that search site, the search is not permitted. On the other hand, if you have not configured yahoo.com and defined its corresponding CGI keyword and a user tries to search for a restricted word or phrase using that search site, the search is permitted.

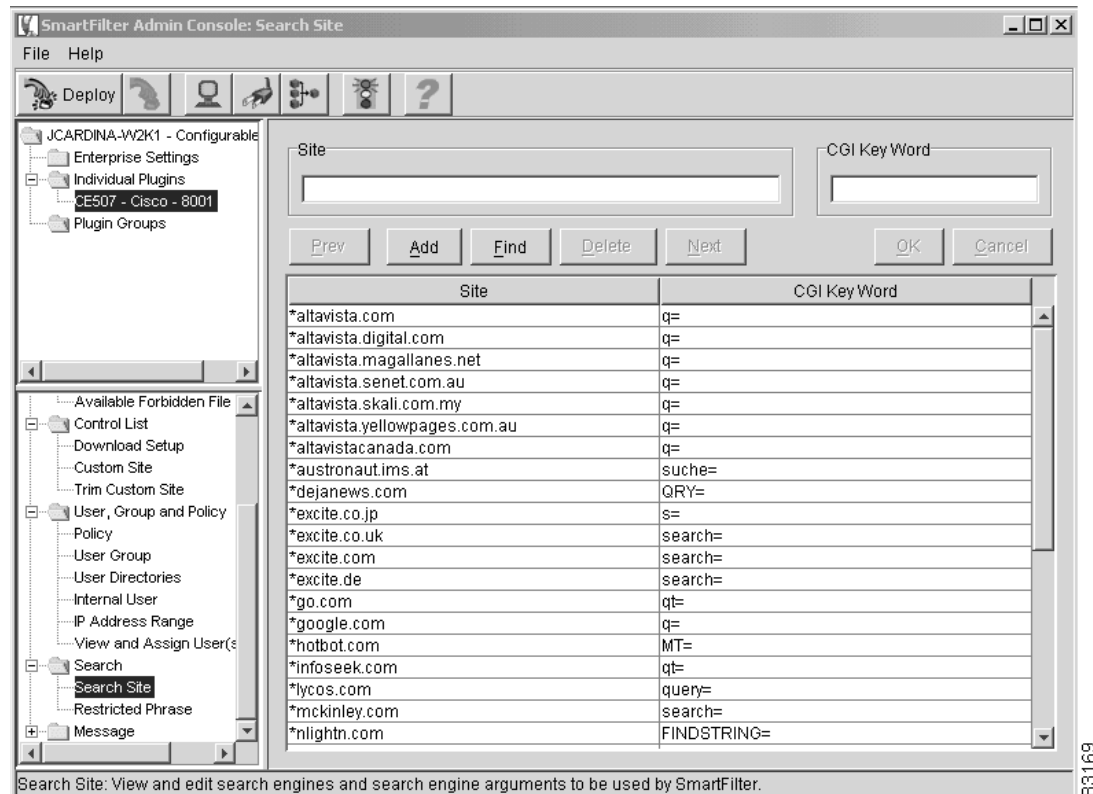
Use the Search Site window for these tasks:

- [Adding a Search Site](#)
- [Changing a CGI Keyword for a Search Site](#)

- [Finding a Search Site](#)
- [Deleting a Search Site and Its CGI Keyword](#)

For instructions on configuring restricted words and phrases, see the “[Identifying Restricted Words and Phrases](#)” section on page 7-15.

**Figure 7-7 Search Site Window**



In the Search Site window, you can perform these tasks:

- Add a search site and its corresponding CGI keyword.
- Find a search site and its corresponding CGI keyword. (You might want to search for a site before adding it, in case you already had it in your custom sites list. Or you may want to find a site so that you can update it or delete it.)
- Delete a search site and its corresponding CGI keyword.

## Adding a Search Site

To add a search site and its corresponding CGI keyword, follow these steps:

**Step 1** Click **Add**.

The cursor moves to the Site field.

**Step 2** Enter the name of the search site.

Be sure to include an asterisk (\*) at the beginning of the search site name.

- Step 3** Press **Tab** to reach the CGI Key Word field and enter the CGI keyword.
- Step 4** Click **OK**.

The search site that you entered appears in the table at the bottom of the window.

---

## Changing a CGI Keyword for a Search Site

To change the CGI keyword associated with a search site, follow these steps:

---

- Step 1** Click in the table at the bottom of the Search Site window.  
The site and existing parameter appear in the fields at the top of the window.
- Step 2** Click in the CGI Key Word field and enter the new CGI keyword.
- Step 3** Click **OK**.  
The keyword you entered appears in the CGI Key Word column.
- 

## Finding a Search Site

To find a search site in the Search Site window, follow these steps:

---

- Step 1** Click **Find**.  
The cursor moves to the Site field.
- Step 2** Enter the name of the search site.  
Be sure to include an asterisk (\*) at the beginning of your search criteria.
- Step 3** Click **OK**. One of the following occurs.
- A message appears telling you that no row is found.
  - The table displays only rows that match the search criteria you entered.
- Step 4** Click **Cancel** to display the entire list of search sites.
-

## Deleting a Search Site and Its CGI Keyword

To delete a search site from the table, follow these steps:

- 
- Step 1** Choose the search site that you want to delete.
- Step 2** Click **Delete**.
- If you chose only one item, the site is removed from the table and a warning message does not appear.
  - If you chose more than one item, a message appears, asking if you are sure you want to delete the rows. Click **Yes** to delete the rows. Click **No** to return to the table.
- 

## Identifying Restricted Words and Phrases

The Restricted Phrase window contains information about phrases (individual words and multiple word phrases) that you want to restrict.

Assigning search words and phrases to categories is a global decision that pertains to all policies that use categories to which restricted words and phrases have been applied.

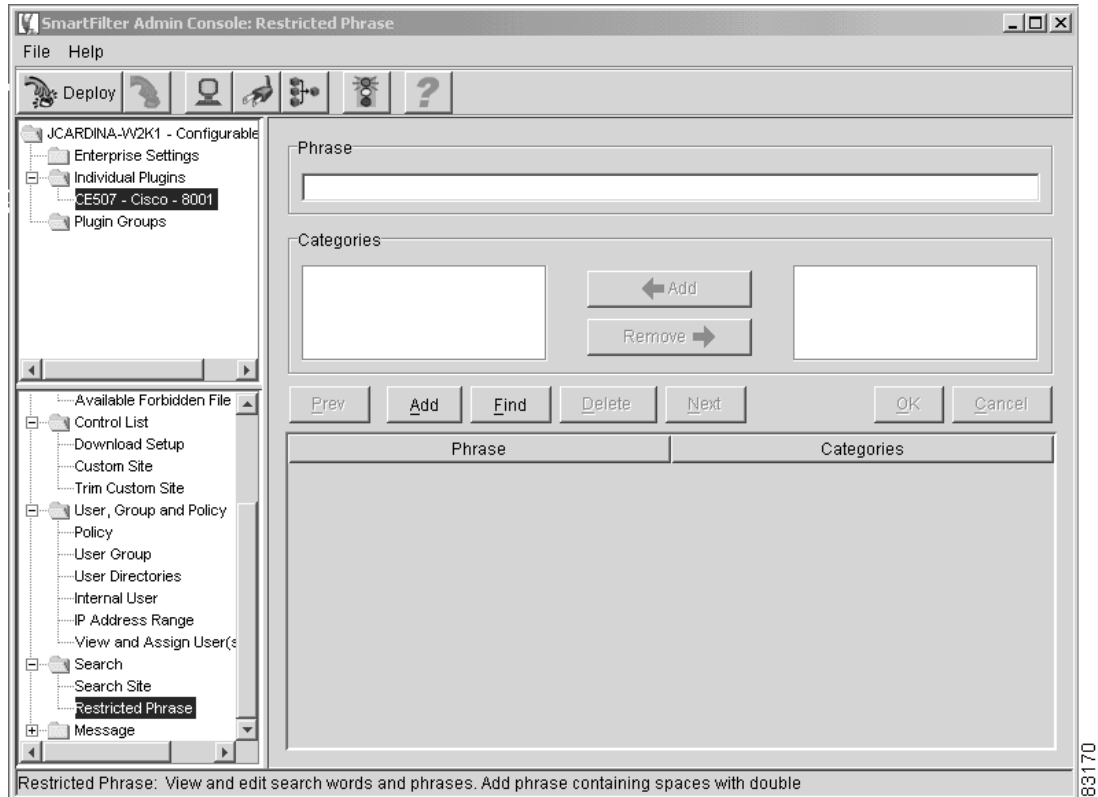
Phrases are restricted if they are an exact match. Phrase matches have precedence over word matches. For example, if you add the phrase “Jolly Roger’s cookbook” to the criminal skills (cs) category, add the word “cookbook,” and then add the word “cookbook” to the entertainment (et) category, and a user enters only the word “cookbook,” the word is restricted for the entertainment (et) category but not for the criminal skills (cs) category because the phrase is not an exact match.

Because the Restricted Phrase window works together with the Search Site window, it is important to define the search engines and their CGI keywords. If you have not defined a search engine and its corresponding CGI keyword, no action is taken for that search engine, even if you have defined restricted words or phrases. For example, if you have defined yahoo.com and its corresponding CGI parameter and a user tries to search for a restricted word or phrase, the search is not permitted. On the other hand, if you have *not* defined yahoo.com and its corresponding CGI keyword, and a user tries to search for a restricted word or phrase, the search is permitted. For instructions on defining search sites, see the [“Defining Search Sites” section on page 7-12](#).

In the Restricted Phrase window, shown in [Figure 7-8](#), you can perform these tasks:

- Add a word or phrase to restrict.
- Find a restricted word or phrase. (You might want to search for a word or phrase before adding one in case you already had it in your list. Or you might want to find one so that you can update it or delete it.)
- Delete a word or phrase.

Figure 7-8 Restricted Phrase Window



## Adding a Restricted Word or Phrase

To add a word or phrase to restrict, follow these steps:

**Step 1** Click **Add**.

The cursor moves to the Phrase field.

**Step 2** Enter the word or phrase that you want to restrict.



**Note** You can enter more than one word at a time using spaces as delimiters between words. If you enter a phrase, enter it in quotation marks.

**Step 3** Add or remove categories for the word or phrase.

- To add a category, choose the category that you want to attach to the word or phrase from the list on the right, and click **Add**.
- To remove a category, choose the category that you want to remove from the word or phrase from the list on the left, and click **Remove**.

**Step 4** Click **OK**.

The word or phrase that you entered appears in the table at the bottom of the window.

---

## Changing the Category for a Restricted Word or Phrase

To change the category associated with a restricted word or phrase, follow these steps:

**Step 1** Choose the restricted word or phrase for which you want to change categories, using any of the following methods:

- Choose one from the table.
- Click the **Find** button.

**Step 2** Choose the word or phrase in the table.

The categories associated with the word or phrase appear in the Categories field.

**Step 3** Add or remove categories for the word or phrase.

- To add a category, choose the category that you want to attach to the URL from the list on the right, and click **Add**.
- To remove a category, choose the category that you want to remove from the URL from the list on the left, and click **Remove**.

**Step 4** Click **OK**.

The word or phrase that you entered appears in the table with the changes you made.

---

## Finding a Restricted Word or Phrase

To find a restricted word or phrase in the Restricted Phrase window, follow these steps:

**Step 1** Click **Find**.

The cursor moves to the Phrase field.

**Step 2** Enter the restricted word or phrase.

**Step 3** Click **OK**.

One of the following occurs.

- A message appears telling you that no row is found.
- The table displays only rows that match the search criteria you entered.

**Step 4** Click **Cancel** to display the entire list of plug-in definitions.

---

## Deleting a Restricted Word or Phrase

To delete a restricted word or phrase from the Restricted Phrase window, follow these steps:

- Step 1** Choose the restricted word or phrase that you want to delete.



**Note** If you choose only one item to be deleted, you do not receive a warning message. If you choose more than one item, a warning message appears, asking if you are sure you want to delete the rows.

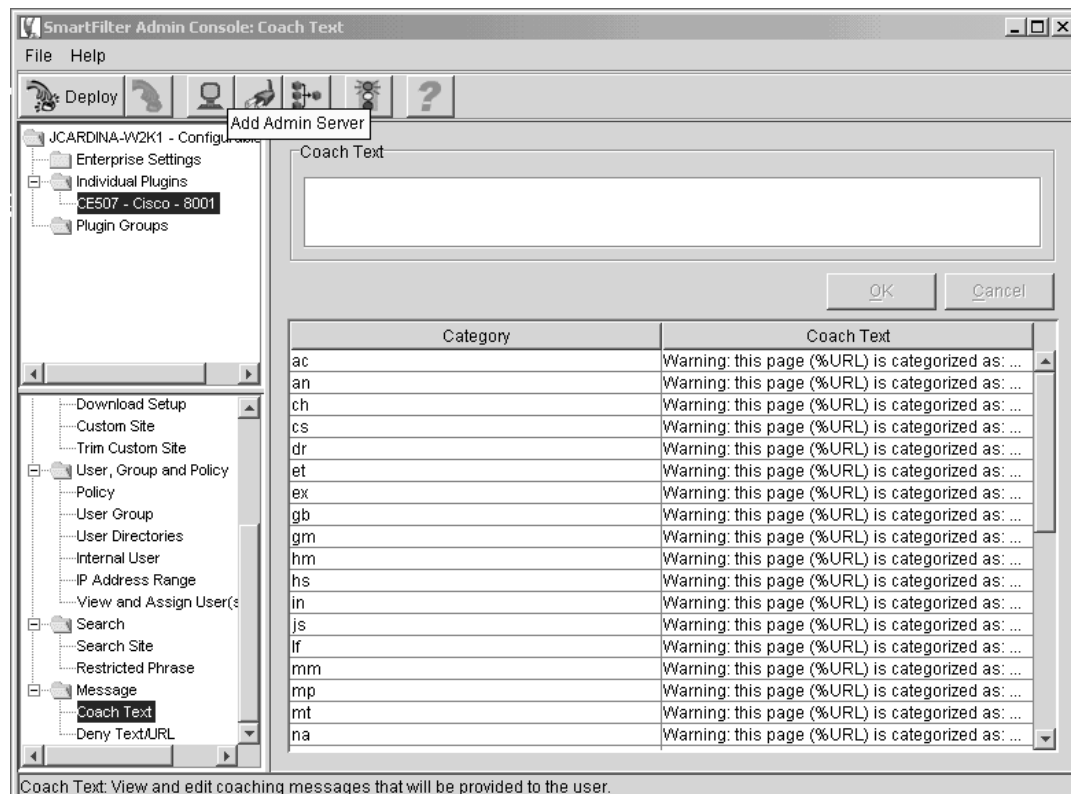
- Step 2** Click **Delete**.

The word or phrase is removed from the table.

## Creating a Message for a Coached Category

The Coach Text window, shown in [Figure 7-9](#), contains the specific message that appears to users when they attempt to access a site for which you have allowed coached access. You can compose a unique message, in text or HTML format, for each category. The message applies globally across all policies and appears whenever a coached category is requested. Using the Coach Text window, you can enter a message for one or more categories at a time.

**Figure 7-9** Coach Text Window



33171

To update a coaching message for one or more categories, follow these steps:

**Step 1** Choose the category for which you want to enter a message.

The cursor moves to the Coach Text field.



**Note** You can choose more than one category at a time by using the **Shift** or **Ctrl** keys.

**Step 2** Enter the message that you want to appear when users attempt to access sites in the category you have chosen. You can use text or HTML format. SmartFilter software offers two keywords to help enhance the content of the error or coach messages: %REASON and %URL.

- %REASON is replaced with the category names that caused the URL to be restricted. These names are configurable as described in the “[Defining a Customized Policy](#)” section on page 7-4.
- %URL is replaced with the URL that the user entered. For example, if you entered the following for an error message:

The following url: %URL was denied because it matched the following categories:  
%REASON.

the user would see a message such as this:

The following url: http://playboy.com was denied because it matched the following categories: Nudity, Online Sales, Entertainment.

**Step 3** Click **OK**.

The message that you entered appears in the table under the Coach Text column.



**Note** If the Coach Text column in the table is empty, the following default message is displayed to the user.

Warning: this page is categorized as <Category Name> If you wish to continue click here: <URL>

The phrase “If you wish to continue...” is appended to all coaching messages whether you choose to configure them or not.

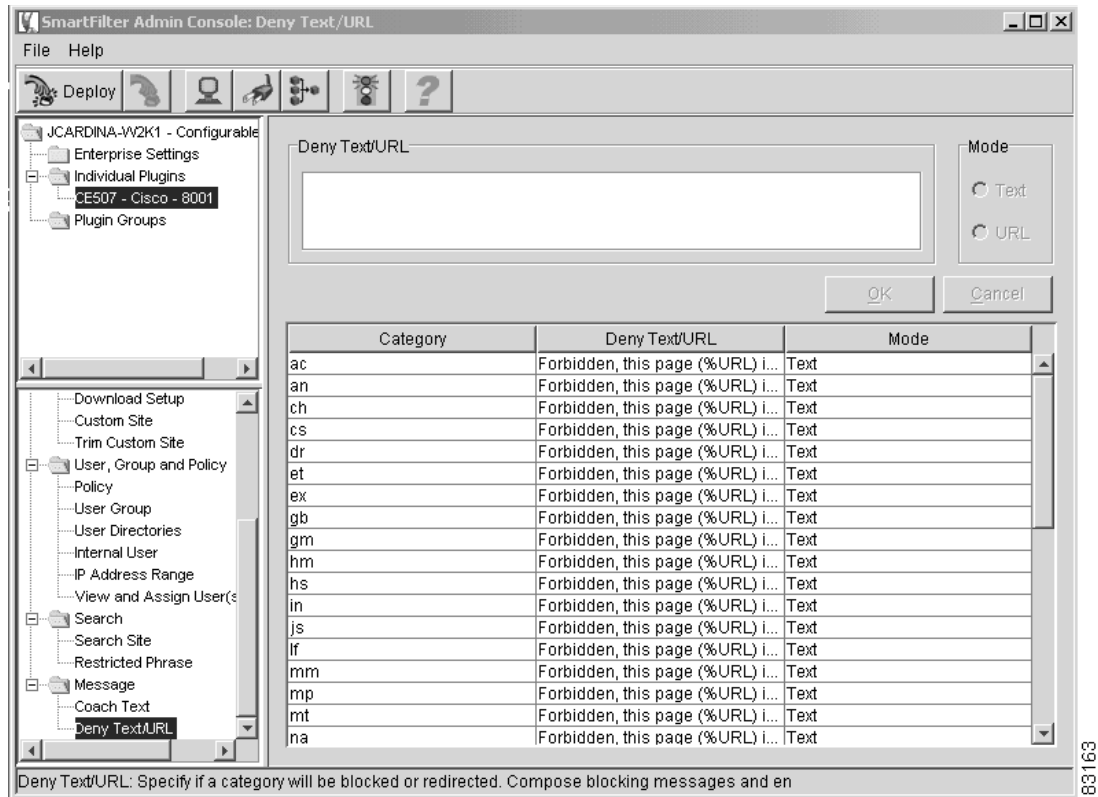
## Creating a Message for a Denied Category

The Deny Text or URL window, shown in [Figure 7-10](#), contains the specific message or a URL to which users are redirected when they attempt to access a site for which you have denied access.

The message or redirection option applies globally for a given category across all policies. You can choose to display a message or a redirection URL for a particular category, but not both.

Redirection diverts users to a separate page when they have attempted to access a categorized URL that is blocked. A benefit of redirection (as opposed to a text message) is that it allows you to present more information than can be easily displayed in a short text or HTML formatted message.

Figure 7-10 Deny Text or URL Window



## Entering a Message for One or More Categories

To enter a message for a particular category, follow these steps:

- Step 1** Choose the category for which you want to enter a message.

The cursor moves to the Deny Text/URL field.



**Note** You can choose more than one category at a time by using the **Shift** or **Ctrl** keys.

- Step 2** Click the **Text** radio button in the Mode area.

**Step 3** Enter the text (message) that you want to appear when users attempt to access sites in the category you have chosen.

SmartFilter software offers two keywords to help enhance the content of the error or coaching messages, %REASON and %URL.

- %REASON is replaced with the category name that caused the URL to be restricted. These names are configurable as described in the “Defining a Customized Policy” section on page 7-4.
- %URL is replaced with the URL the user entered. For example, if you entered the following as an error message:

The following url: %URL was denied because it matched the following categories:  
%REASON.

the user would see a message such as this:

The following url: http://playboy.com was denied because it matched the following categories: Nudity, Online Sales, Entertainment.

**Step 4** Click **OK**.

The message that you have entered appears in the table in the Deny Text/URL column, and the word “Text” appears in the Mode column.



**Note** If the text field is empty, the following default message is displayed to the user:  
Forbidden, this page is categorized as <Category Name>

## Redirecting Users to a URL

To redirect users to a particular URL when they attempt to access a denied category, follow these steps:

**Step 1** Choose the category for which you want to enter a message.

The cursor moves to the Deny Text/URL field.



**Note** You can choose more than one category at a time by using the **Shift** or **Ctrl** keys.

**Step 2** Click the **URL** radio button in the Mode area.

**Step 3** Enter the URL to which you want users to be redirected when they attempt to access sites in the category you have chosen. For example:

**http://mycompany.com/messages/sexmessage.html**



**Note** Be sure to include *http://* in the URL.

**Step 4** Click **OK**.

The URL that you have entered appears in the table in the Deny Text/URL column, and “URL” appears in the Mode column.

## Changing a URL Redirect to a Text Message

To change a URL redirect to a text message for one or more categories, follow these steps:

---

**Step 1** Choose the category for which you want to remove a URL.

The existing URL appears in the Deny Text/URL field.



---

**Note** You can choose more than one category at a time by using the **Shift** or **Ctrl** keys.

---

**Step 2** Click the **Text** radio button in the Mode area.

**Step 3** Click **OK**.

The URL is removed and the Deny Text/URL column in the table is blank.

---