Downloading and Configuring WebFilter

What is URL Filtering?

URL filtering is a type of transaction content filtering that limits a user's Web site access through a policy that is associated with a specific URL or URL topic category. URL filtering running on a ProxySG (On-Proxy) provides performance and policy extensions not found with a standalone URL solution. Because the Internet is ever changing, the Blue Coat ProxySG periodically downloads updates from the master WebFilter database so that your policy can incorporate new and updated sites. Plus WebFilter provides a real-time rating service for newly published web sites, providing an "on the fly" service not seen with other solutions.

Why Enable URL Filtering?

Companies cannot ignore the loss of productivity and the liability associated with unmanaged Web surfing. The ProxySG offers the capability to control access to undesirable sites on a category basis. More than 69 categories enable security administrators to deploy a consistent Web access policy. The entire WebFilter database can be loaded onto the ProxySG appliance to offer optimized performance.

URL filtering also provides an additional defense layer against malware that can be downloaded to a user's system simply by opening a Web site (drive-by installation). By denying known-bad URLs, and enabling automatic updates of new known-bad URLs, drive-by installations of malware can be thwarted.

WebFilter accomplishes this by using a honey grid of systems with multiple threat detection techniques to review every user request for hidden malware sources and determine reputations. The honey grid is called WebPulse and this cloud computing service contains the WebFilter master database, the Dynamic Real-Time Rating (DRTR) service, plus the Dynamic Background Rating (DBR) for threat detection, deep content inspection and reputation analysis.

Besides ProxySG, the benefits of WebFilter for URL filtering and malware host blocking from WebPulse threat detections are available on ProxyClient to remote users. As a client agent, all user requests access the cloud WebFilter database and real-time rating service. This provides central policy management to remote users for URL filtering that includes malware host blocking from WebPulse grid detections.

Configuring WebFilter URL Content Filtering

There are four parts to implementing the WebFilter database on ProxySG:

① Obtain the Blue Coat WebFilter License

② Enable Content Filtering on the ProxySG

③ Configure Policy for WebFilter Categories using the Visual Policy Manager

Note: *The HTTP proxy service* ***Action*** *option must be set to* ***Intercept*** *in order for the policy to work. To do this, use the* ***Configuration > Services > Proxy Services*** *page of the Management Console and modify the HTTP service as needed.*

Note: *To launch the VPM, go to* ***Configuration > Policy > Visual Policy Manager*** *and click* ***Launch****.*

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:

- A default proxy transaction policy of **Deny** prohibits proxy-type access through the ProxySG appliance; instead, you must create policies to explicitly grant access on a case-by-case basis.
- A default proxy transaction policy of **Allow** permits most proxy transactions. If your policy is set to **Allow**, you must create policies to explicitly deny access on a case-by-case basis. Please note: if protocol detection is enabled (the default), HTTP CONNECT transactions are only allowed if they are tunneling SSL; if protocol detection is disabled, HTTP CONNECT is only allowed on port 443.

This document assumes the **Allow** default proxy policy; in task four you select URL categories to deny. If your default proxy policy is **Deny**, you would, instead, select URL categories to allow, and all others would, by default, be denied.

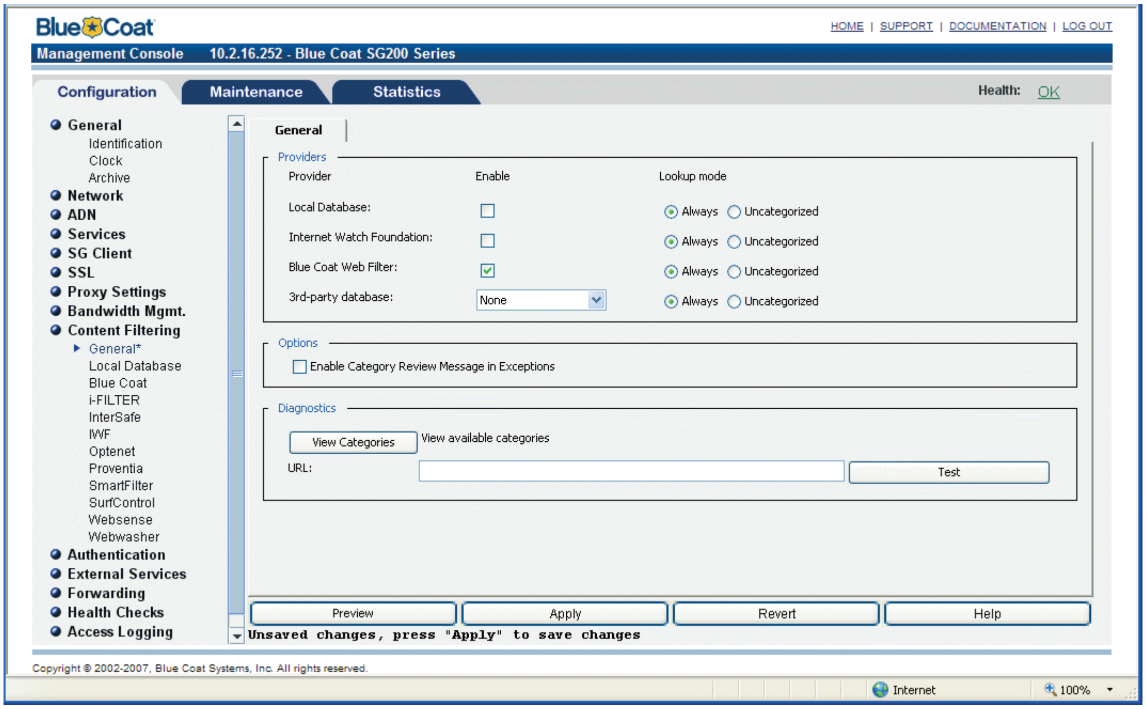
For more information on developing effective policies, see the Policy Best Practices tech brief.

Part 1 – Obtain the Blue Coat WebFilter License

Blue Coat WebFilter URL content filtering requires a purchased license for use of its database. For evaluation purposes you can receive a free 60-day license. Use the Blue Coat Systems Contact Request page to begin the evaluation process.

Part 2 – Enable Content Filtering on the ProxySG

To enable content filtering using the Blue Coat ProxySG Management Console:



Management Console 10.2.16.252 - Blue Coat SG200 Series

Health: OK

General

Providers

Provider	Enable	Lookup mode
Local Database:	□	● Always ○ Uncategorized
Internet Watch Foundation:	□	● Always ○ Uncategorized
Blue Coat Web Filter:	☑	● Always ○ Uncategorized
3rd-party database:	None	● Always ○ Uncategorized

Options

□ Enable Category Review Message in Exceptions

Diagnostics

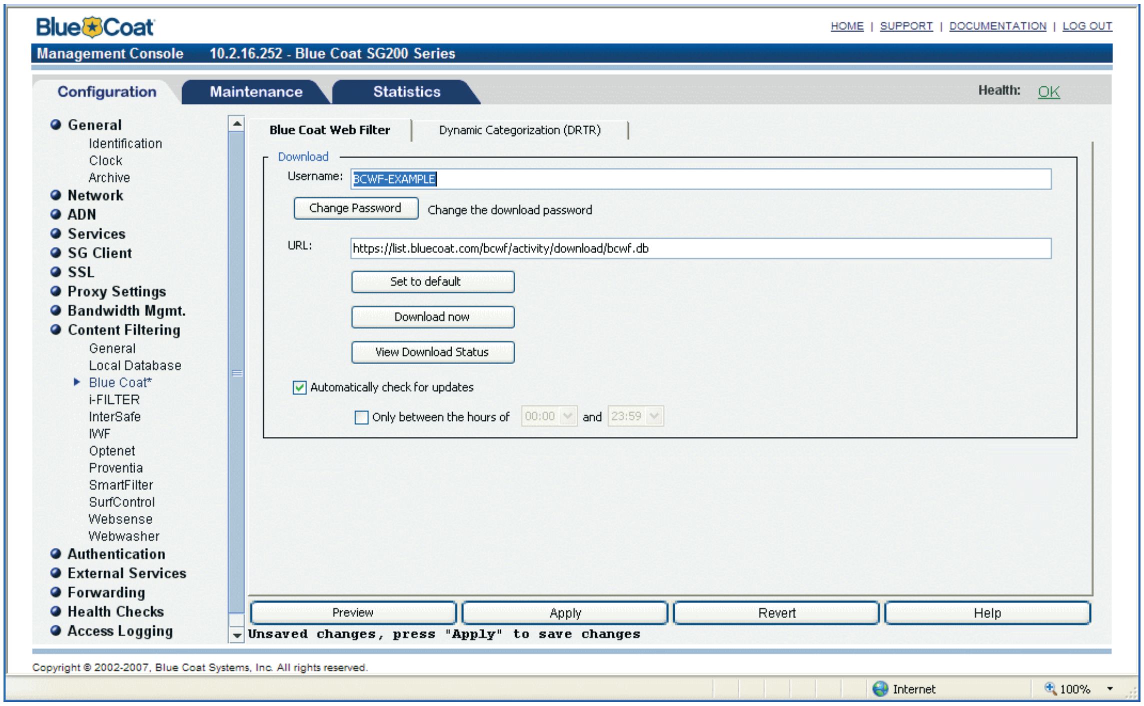
View Categories View available categories

URL:

Unsaved changes, press "Apply" to save changes

Copyright © 2002-2007, Blue Coat Systems, Inc. All rights reserved.

1. Go to **Content Filtering > General**. Select **Blue Coat WebFilter** in the **Providers** area and click **Apply**. Click **OK** to close the confirmation box.



Username: BCWF-EXAMPLE

Change the download password

URL: https://list.bluecoat.com/bcwf/activity/download/bcwf.db

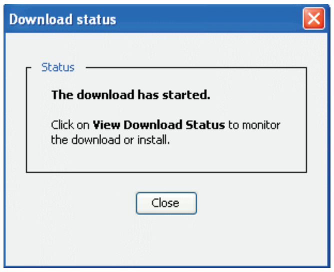
☑ Automatically check for updates

□ Only between the hours of 00:00 and 23:59

```
Unsaved changes, press "Apply" to save changes
```

Copyright © 2002-2007, Blue Coat Systems, Inc. All rights reserved.

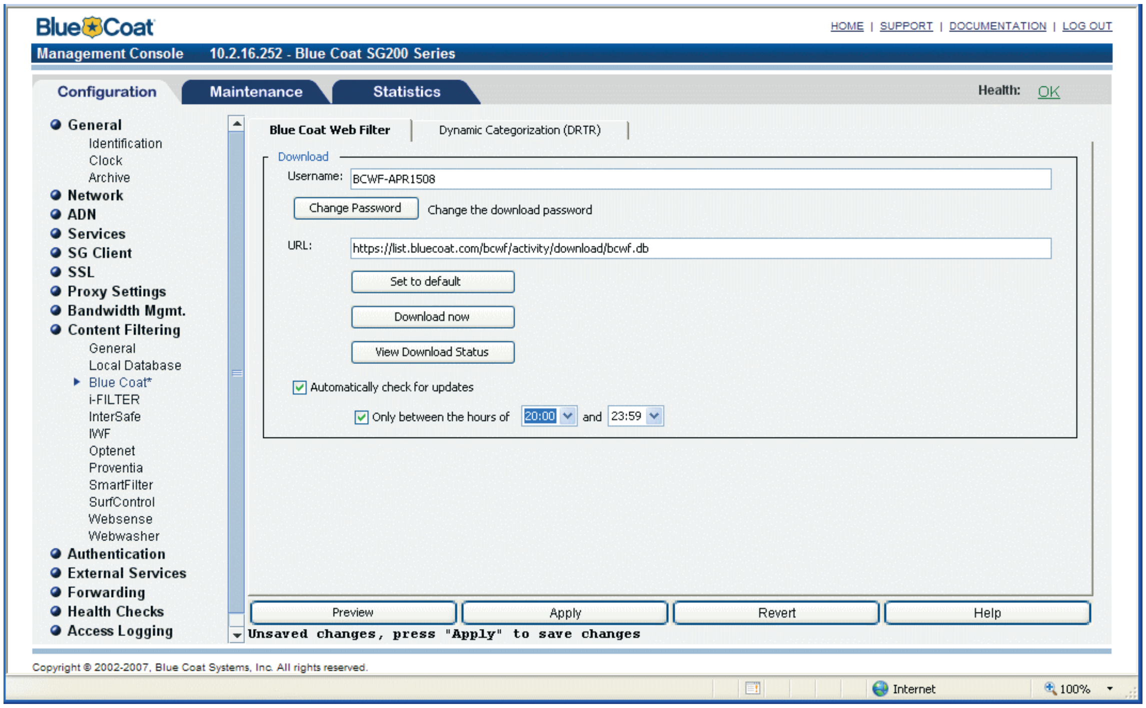
❷ Go to **Content Filtering > Blue Coat Web Filter**. Enter your username and password as supplied by Blue Coat and click **Apply**. Click **OK** to close the confirmation box.



The download has started.

Click on **View Download Status** to monitor the download or install.

❸ Click **Download now**. A status box displays. Click **Close** to dismiss the box. Downloading the database takes a few minutes. Once complete, a new option, **Blue Coat**, displays in the Visual Policy Manager as an Add Request URL Category Object option (configured in Part 3, below).



Username: BCWF-APR1508

URL: https://list.bluecoat.com/bcwf/activity/download/bcwf.db

☑ Automatically check for updates

☑ Only between the hours of 20:00 and 23:59

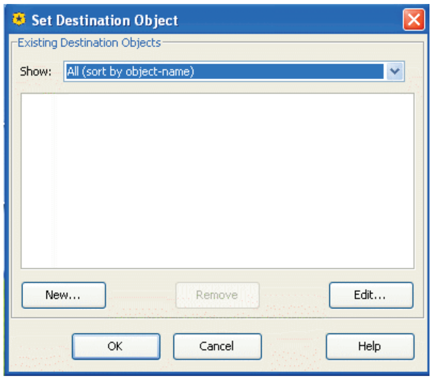
```
Unsaved changes, press "Apply" to save changes
```

4. (Optional) Automatic update checks 24 hours a day are enabled by default. To configure a specific time span for automatic checks: On the Blue Coat Web Filter page select the **Only between the hours of** option and select the hours between which you want update checks to happen. Click **Apply** to save the changes. Click **OK** to close the confirmation box.

Part 3 – Configure Policy for Web Filter Categories

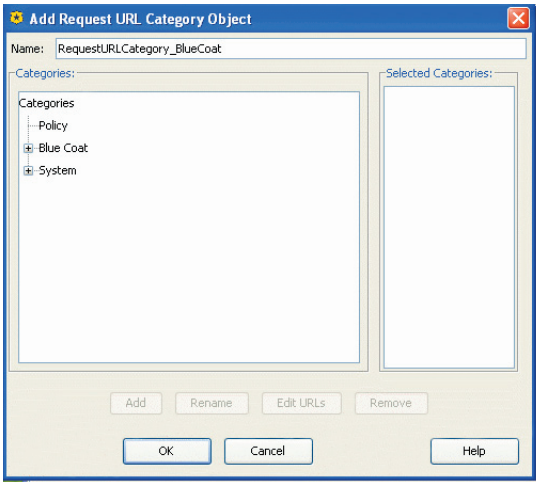
Configure policy for Web Filter categories using Visual Policy Manager (VPM):

1. Begin by right-clicking **Policy** and adding a Web Access Layer OR add a new rule under any previously defined Web Access Layer by clicking **Add Rule**.



Show: All (sort by object-name)

2. Right-click the **Destination** setting and select Set. The Set Destination dialog displays.



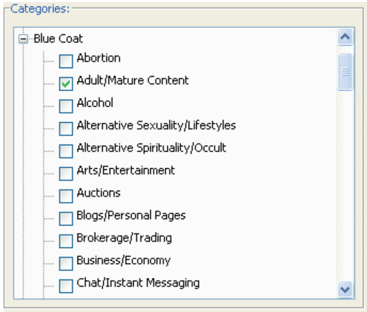
Add Request URL Category Object

Name: RequestURLCategory_BlueCoat

Categories:
- Categories
  - Policy
  - Blue Coat
  - System

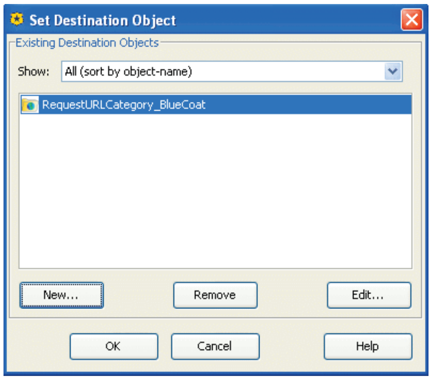
Selected Categories:

3 Click **New** and select **Request URL Category**. The Add Request URL Category object dialog displays. Name the object `RequestURLCategory_BlueCoat`; for example.



Categories:
- Blue Coat
  - □ Abortion
  - ☑ Adult/Mature Content
  - □ Alcohol
  - □ Alternative Sexuality/Lifestyles
  - □ Alternative Spirituality/Occult
  - □ Arts/Entertainment
  - □ Auctions
  - □ Blogs/Personal Pages
  - □ Brokerage/Trading
  - □ Business/Economy
  - □ Chat/Instant Messaging

4 Open the Blue Coat tree to display category listings. Select the **Adult/Mature Content**, **Gambling**, and **Sports/Recreation** categories to test this policy.



Set Destination Object

Existing Destination Objects

Show: All (sort by object-name)

RequestURLCategory_BlueCoat

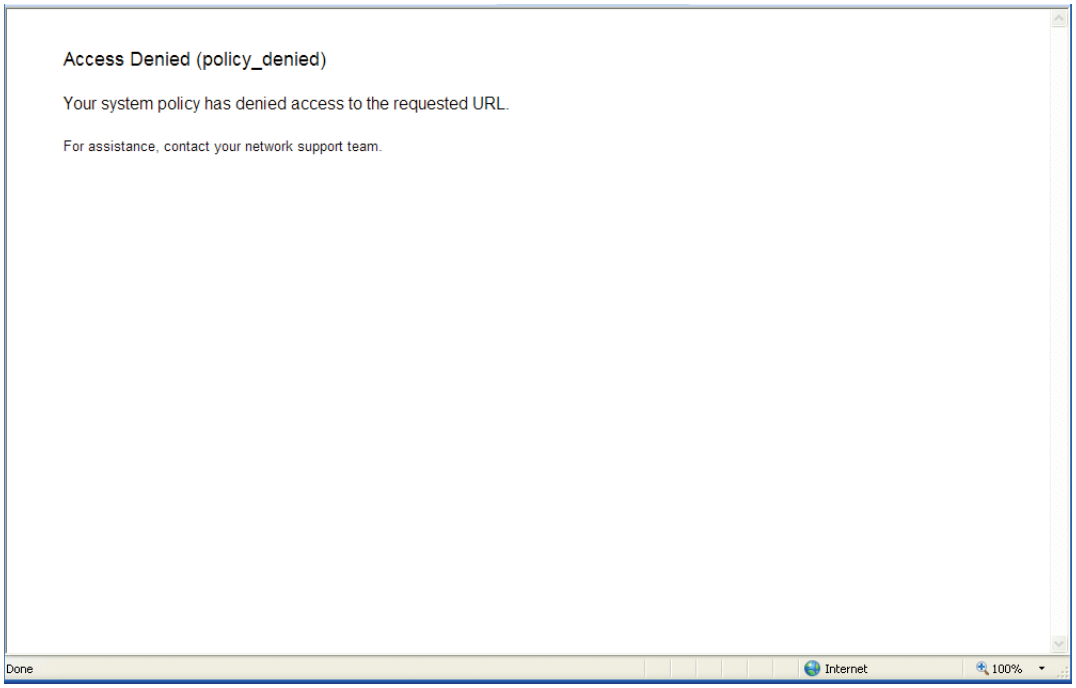
5 Click **OK** to add the Request URL Category object and dismiss the dialog. The Set Destination Object dialog re-displays.

6 Click **OK** to set the new object and dismiss the dialog. Click **Install Policy** to finish. Click OK to dismiss the confirmation box.

Testing Your Configuration

To test your configuration, simply open your browser and type in a category-related URL; for example, `www.sportsillustrated.com`. You can also test sites in the other categories as well. If you have configured the policy correctly, the Blue Coat policy denies you access to any site that is part of a restricted category; a page like the one shown below displays.

Note: *You can modify the error message shown below with a custom exception page. See the Blue Coat Tech Brief "Implementing Exception Pages" for details.*



Access Denied (policy_denied)

Your system policy has denied access to the requested URL.

For assistance, contact your network support team.

Conclusion

The Blue Coat ProxySG supports numerous vendors to run URL filtering "On-Proxy". The ProxySG supports automatic downloads of the WebFilter database, and integrates the database with powerful policy functionality. By establishing a URL filtering policy, productivity issues and malware prevention can be addressed.