WEBSENSE INTEGRATION SERVICE

Reporting Installation and Configuration
for Blue CoatAppliances

v7

Websense Integration Service Reporting Installation and Configuration for Blue CoatAppliances

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published January 22, 2009
Printed in the United States of America

Trademarks

WinPcap

Contents

1 Websense Reporting for Blue Coat Appliances

When running a Blue Coat appliance, you can choose the Websense Master Database of URLs as the basis for Internet filtering. The Websense Master Database classifies millions of URLs into categories for filtering.

This requires that you configure certain Blue Coat settings, to enable regular downloads of the Websense Master Database, and establish filtering policies.

You also can install the Websense Integration Service and Websense reporting tools on a Windows server to get summary and detail reports of the Internet activity in your network, and to see how the Websense Master Database combines with your Blue Coat appliance to protect your network from security threats, legal liability, and unproductive Internet usage.

This document provides instructions for

- Installing the Websense reporting tools
- Configuring the Blue Coat appliance to use the Websense Master Database, and download regular updates
- Configuring the Blue Coat appliance to send records of Internet filtering activity to the Websense Log Server
- Use Websense reporting tools to understand Internet usage and the value of Internet filtering

Hardware and software requirements

The specific hardware requirements vary according to your network size and volume of Internet traffic. For complete information, see the Websense *Deployment Guide,* available at www.websense.com/docs, provides hardware and software requirements. Specifically, review the recommendations for reporting installations, which is the information that applies to this environment.

Software requirements are listed below.

- **Operating Systems supported**:
  - Windows Server 2003, R2 (Standard or Enterprise)
  - Windows Server 2003, SP1 (Standard or Enterprise)
  - Windows Server 2003 (Standard or Enterprise)

- **Database engines supported**:
  - Microsoft SQL Server 2005 SP2 (Workgroup, Standard, Enterprise, or 64-bit edition) (recommended)
  - Microsoft SQL Server 2000 SP 4
  - Microsoft SQL Server Desktop Engine (MSDE) 2000 SP 4 (suitable for smaller networks) MSDE is available for download from www.websense.com. See kb.websense.com/article.asp?article=3492&p=12 for details.
- **Web browsers supported**: necessary for using Websense Manager
  - Internet Explorer v7
  - Mozilla Firefox v2
- **Adobe Acrobat**. Necessary for viewing reports generated in PDF format.
- **Microsoft Excel**: Necessary for viewing reports generated in XLS format.

Websense component installation

Several components are installed to support Websense reporting from a Blue Coat appliance.

- **Policy Broker and Policy Database**: Manage and store configuration settings and client data.
- **Policy Server**: Enables communication between the Blue Coat appliance and the Websense Integration Service.
- **User Service**: Populates user-related tables in the Websense Log Database.
- **Websense Manager**: Provides a Web-based interface for generating reports, configuring directory service communication, and defining delegated administration roles that allow other administrators to report on specific clients.
- **Log Server**: Receives records of Internet activity from the Blue Coat appliance, and updated lists of category, protocol, and risk class names from the Websense Master Database. Sends this information to the Log Database.
- **Log Database**: Stores and manages information sent by Log Server, and provides the information requested for reports.
- **Apache Web Server**: Enables reporting functionality.
- **Apache Tomcat Server**: Enables Websense Manager functionality.
- **Websense Integration Service**: Receives Master Database category information from your Blue Coat appliance and passes it to the Websense Policy Broker, which sends it to the Log Database for reporting.

Use the following steps to install Websense components on a Windows server.

1. Make sure a supported database engine (see *Hardware and software requirements*, page 5) is installed in the network.
2. Log on to the installation machine with local and domain administrator privileges.
3. Download the v7 installer for the Blue Coat appliance from www.websense.com.
4. Extract the files and the installer launches automatically.

5. Follow the onscreen instructions. As you proceed, consider the following:
   a. **Database engine location**: Enter the IP address or name of the machine running either Microsoft SQL Server or Microsoft SQL Server Desktop Edition (MSDE). Both the SQL Server and the SQL Server Agent must be running when you install the Websense software.
   b. **Database access**: Websense, Inc., recommends using a SQL database account with MSDE. The account must have administrator rights to configure the Log Database.
   c. **IP Address**: If the installation machine has multiple IP addresses, the installer asks you to select the IP address for Websense Log Server to use.
   d. **Integration Service Port**: Enter a port number for the Websense Integration Service communication with your appliance, or accept the default, 55080.

      Make a note of the port you assign here. You will need it when you configure the appliance.
6. When the installation is complete, click **Finish**.
7. Configure the appliance for filtering and reporting. See *Configure Blue Coat for Websense filtering and reporting*, page 8 .
8. Configure Websense reporting. See *Configuring Websense Software for Reporting*, page 13.

Removing Websense components

If you need to move the reporting service to another machine, first uninstall Websense components, as follows.

1. Stop the Websense Integration Service.
   a. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
   b. In the **Services** pane, right-click the **Websense Integration Service**.
   c. Select **Stop**.
2. Go to **Start > Settings > Control Panel > Add or Remove Programs**.
3. Select **Websense Web Security / Web Filter** from the list.
4. Follow the onscreen instructions to remove selected components or the entire installation.
5. Install the Websense components on a new machine. See *Websense component installation*, page 6.
6. Open the **General** tab.
   a. Mark the **Websense Enable** check box.
   (CLI option: config.wsfilter.enable)
   b. Enter a URL in the **Redirect Blocked Requests to This URL** field.
   (CLI option: config.wsfilter.redirect)

      This URL should provide with information about the organizations Internet use policy and reasons why the requested site was blocked.
   c. Click **Commit Changes** to save your updates.
   d. Click **Commit Changes** to save your updates.

Configure Blue Coat for Websense filtering and reporting

Follow the steps below to configure the Blue Coat appliance for Websense communication, reporting, and logging functions.

Filtering configuration

Use the following steps to enable the Blue Coat appliance to use the Websense Master Database for filtering.

1. Open the Blue Coat Management console.
2. From the navigation pane, select **Content Filtering > General**.
3. If desired, mark the check box for **Local Database**.

   When you mark this option, Blue Coat attempts to categorize the requested URL if the Websense Master Database cannot do so. Refer to the Blue Coat Help for more information.
4. In the **3rd party database** drop-down list, select **Websense**.
5. Accept the defaults for other settings.
6. Click **Apply** to save the changes.

Websense database download and reporting configuration

To configure the Blue Coat appliance to communicate with the Websense Download Server and to configure logging:

1. In the navigation pane of the Blue Coat Management console, select **Content Filtering > Websense**:
2. Enter your Websense subscription key in the **License key** field.
3. In the **Download Server** field, enter **download.websense.com**.
4. In the **Contact e-mail** field enter the email address of the administrator Websense, Inc., should contact in case of any subscription concerns.
5. Click **Download Now** to download the Websense Master Database.

   Initially, the full Master Database is downloaded. After that, downloads typically include only changes and additions to the database.

   Click **View Download Status**, as needed, to view the progress of the download.
6. Mark the **Automatically check for updates** check box.

   Automatic update checking is available for SGOS 4.3.x and later 4.x versions only.
7. To set a download time other than midnight, mark the **Only between the hours of** check box., and then select start and end times for the downloads.
8. Accept the default setting for **Always apply regular expressions**.

   Keep in mind that applying regular expressions can slow performance. See the Blue Coat Help for information on regular expressions.

9. In the Websense Reporter area, configure communication with Websense Integration Service.
   a. Mark the **enabled** check box. This activates the **Integration Service Host** and **Port** fields.

> **Note**
> To stop Websense logging, remove the check mark from **enabled**. The logging stops after a few moments.

   b. In the **Integration Service Host** field, enter the IP address of the machine where you installed Websense components.
   c. In the **Port** field, enter the port specified during installation (default **55080**).
   d. Mark the **Log forwarded client address** check box if you want to log the IP address of the machines making Internet requests.
10. Click **Apply** to save the settings.

Log facility configuration

Use the following steps to create a Websense log facility and configure the Blue Coat appliance to send Internet filtering records to the Websense Log Server.

1. In the Blue Coat Management console, select **Access Logging** > **Logs**.
2. Click **New** to open the Create Log dialog box.
3. Fill in the fields as follows:
   a. **Log Name**: Enter **Websense** or another name that is meaningful to you.
   b. **Log Format**: Select **Websense**.
   c. **Description**: Enter a description for the Websense log facility.
   d. **Log file limits**: Accept the default settings.
4. Click **OK** to accept the entries and close the Create Log dialog box.
5. Click **Apply** to save the settings.
6. To verify your settings, select **Access Logging > Logs** in the navigation pane, then click the **General Settings** tab. The information here should reflect the entries and selections from Step 3.
7. Select **Access Logging > Logs**, and then click the **Upload Client** tab.
8. Define logging parameters as follows.
   a. Under **Log**, select the Websense log facility created in Step 3.
   b. Under **Client type**, select **Websense Client**.
   c. Click **Settings** to identify the machine where Websense components are installed.
      - In the **Host** field, enter the IP address of the machine where you installed Websense components.
      - In the **Port** field, accept the Blue Coat default port (55805).
      - Click **OK** to save the settings and close the dialog box.

d. Accept the default settings in the **Transmission Parameters** panel.

   If you find later that log transmissions are backing up, increase the number of seconds in the **Send partial buffer after** field to reduce the backup.

   If you need to speed log transmissions, decrease the number of seconds.

9. Click **Apply** to save the settings.
10. Click the **Upload Schedule** tab.
11. Define upload parameters for your Websense log facility.
    a. Select the Websense log facility you created in Step 3 from the **Log** drop-down list.
    b. In the **Upload type** panel, select **continuously**.
12. Accept the default values for **Wait between connect attempts** and **Time between keep-alive log packets**. You can change the values later, if needed.

> **Note**
> The keep-alive time identifies how frequently the Blue Coat proxy sends a Keep-Alive packet to the Websense Log Server to maintain an open connection. A value of zero (0) disables the connection if no log records are transmitted within a certain time frame. When logged information needs to be uploaded, Blue Coat reestablishes the connection.

13. Ignore the settings in the **Rotate the log file** area.

    These settings do not apply when you select continuously as the upload type.

    If you change the upload type to periodically, refer to Blue Coat documentation or Blue Coat technical support for assistance.
14. Click **Apply** to save the settings.

Default logging policy configuration

After you configure the Blue Coat Log facility, identify the default logging policy for Websense.

1. In the Blue Coat Management console navigation pane, select **Access Logging > General**.
2. On the **Default Logging** tab, set the logging policy.
   a. Select **HTTP/HTTPS**, and then click **Edit**.
   b. Select **Websense (Websense Log Server)**, and then click **OK**.
   c. Select **FTP**, and then click **Edit**.
   d. Select **Websense (Websense Log Server)**, and then click **OK**.
3. Click **Apply** to save the settings.

Test the logging

1. At the Websense installation machine, browse the Internet for a few minutes to generate traffic to be logged.
2. While browsing, examine one of the following directories, depending on the Log Insertion Method selected in the Log Server Configuration utility, Database tab:
   - **<install path>\bin\Cache\Bcp** if BCP is the insertion method
   - **<install path>\bin\Cache** if ODBC is the insertion method

   You should see files with the name **log*.tmp** being generated as traffic is logged. After several minutes these files should disappear. If they do, then you know that traffic is being received from the Blue Coat appliance.
3. If this does not show traffic, use TestLogServer, another utility installed with Websense components, for additional troubleshooting.

   For details on using this utility, go to www.websense.com/SupportPortal.

Verify the Master Database downloads

The Websense Master Database organizes millions of URLs and IP addresses into categories that you can use for filtering. You can verify that the database has downloaded successfully, as follows.

1. In the Blue Coat Management console navigation pane, select **Content Filtering > General**.
2. Click **View Categories** to see a complete list of Websense parent categories and subcategories.
3. Enter a **URL**.
4. Click **Test** to find out its category in the Websense Master Database

User authentication

To generate Websense reports that show user names, you must set up user authentication for your Blue Coat appliance, see Blue Coat documentation. For additional information, contact Blue Coat Technical Support.

After configuring the Blue Coat appliance for user authentication, be sure to configure Websense Manager with directory service information. For information on required Websense configuration, see *Configure Settings*, page 14.

Policy configuration

Use the Blue Coat Management Console to configure policies that specify which Websense categories network users are permitted to access, and when. The Blue Coat Technical Brief on *Downloading and Configuring Websense* provides instructions, from which the following information is taken.

1. Open the Blue Coat Visual Policy Manager.
2. Add a new rule under any previously defined Web Access Layer by clicking **Add Rule**.

   See Blue Coat documentation for information on using the Visual Policy Manager.
3. Right-click in the **Destination** field and choose **Set**.

4. Click **New** and **Select categories**.
5. In the Category Listing, select Adult Material, Gambling, Illegal or Questionable and Sports categories to test this policy.
6. Click on **OK** to display a pop-up window showing the selected URLs and the new category list,
7. Install the policy to the ProxySG by clicking on **Install Policies**.

For additional information, contact Blue Coat Technical Support.

Note

Although Websense Manager includes options for configuring policies, those options do not apply to users filtered by Websense Master Database embedded on a Blue Coat appliance.

2 Configuring Websense Software for Reporting

After installing Websense components for your Blue Coat appliance integration, you should review the Log Server Configuration utility to verify that the settings meet your needs. Additionally, you must configure the following settings in Websense Manager to enable reporting features.

- Log Database to assure that database maintenance tasks are performed according to your needs and schedule.
- Reporting preferences to enable distribution of scheduled reports and self-reporting
- Directory services in order to generate reports on user and group activities.
- Delegated administration roles if you plan to permit other members of the organization to generate reports on specific groups of employees.

When this configuration is complete, you can view high-level reports on the Status > Today and Status > History pages, as well as generate and schedule both presentation reports and investigative reports.

Verify Log Server Configuration

The Log Server Configuration utility lets you configure many aspects of Log Server operation. Verify that the default settings are appropriate for your organization.

This utility is accessed from the installation machine by going to the Windows Start menu and selecting **Programs > Websense > Utilities > Log Server Configuration**.

The utility consists of 5 screens, selected by clicking the tabs at the top.

- **Connection** presents options for creating and maintaining a connection between Log Server and other Websense components.
- **Database** lets you configure how Log Server works with the Log Database.
- **Settings** lets you manage the log cache file creation options, and specify whether Log Server tracks the individual files that make up each Web site requested, or just the Web site.
- **Consolidation** lets you enable consolidation and set consolidation preferences. Consolidation decreases the size of your Log Database by combining Internet requests that share their domain name, category, keyword, action, and user/computer. Consolidation increases reporting speed while decreasing precision.
- **WebCatcher** lets you choose whether to submit unrecognized URLs and security URLs to Websense, Inc., for analysis and possible inclusion in future Master Database updates.

For complete details on the settings in the Log Server Configuration utility, click the Help button in the utility window. This information can also be found in the Websense Manager Help.

Open Websense Manager

Open Websense Manager by clicking the Websense icon on the desktop of the installation machine. Alternatively, you can open it from a browser on any computer in the network.

1. Enter the following in the address bar: **https://<IP address of installation machine>:9443/mng**
2. Enter **WebsenseAdministrator** as the user name, and the password that you established during installation.
3. Use the pages in Websense Manager to configure key settings to enable reporting, as described in *Configure Settings*.

Configure Settings

In Websense Manager, use the Settings tab to set key configuration options.

1. In the left navigation pane, click **Settings**.
2. Click **Reporting > Log Database**.

   Use the options on the **Log Database** page to configure database rollover options, maintenance activities and schedule, and other crucial database functions. Click **Help > Explain the Page** for details.
3. On the Settings tab, go to **Reporting >Preferences**.

   Use the **Preferences** page to configure the email server to use for distributing scheduled reports. You can also use this page to enable network users to generate reports of their own Internet activity (self-reporting). Click **Help > Explain the Page** for details.
4. On the Settings tab, go to **General > Directory Service**.

   Use the Directory Service page to configure that directory service that authenticates network users. This information is required for:

   - Generating reports that identify the users, groups, domains, or organizational units associated with Internet activity. If this information is not provided, only IP addresses are available to identify the origin of Internet requests.
   - Enabling network users to log on and generate reports on their own Internet activity (self-reporting).

   Click **Help > Explain the Page** for details.
5. On the Settings tab, go to **General > Logon Directory**.

   Use the **Logon Directory** page to configure the directory service that authenticates all administrators who will access Websense Manager with their network logon credentials. Click **Help > Explain the Page** for details.

   Be sure to notify those administrators of the address for accessing Websense Manager from their browser, and that they should use their network credentials to log on.
6. Click **Save All** to implement the changes cached on each page.

Define delegated administration roles

Delegated administration allows you to create an administrative role for a logical group of clients, and assign administrators who can generate reports for those clients.

There are 2 aspects to defining delegated administration roles:

First, decide how administrators will access Websense Manager to generate reports.

- Configure the Logon Directory, as described above. Then, inform the administrators of the address for accessing Websense Manager from their browser, and that they should use their network credentials to log on.
- Create special Websense user accounts, defining a user name and password that each administrator uses only to access Websense Manager. To create these accounts:
  1. In Websense Manager, click the **Main** tab in the left navigation pane.
  2. Go to **Policies > Delegated Administration**.
  3. Click the **Manage Websense User Accounts** button above the Delegated Administration page.

     Click **Help > Explain This Page** on any page for details on that page.

After configuring the Logon Directory page or creating Websense user accounts, create delegated administration roles. For each role, assign administrators and the clients they can report on. Following is the general procedure for configuring roles. For detailed instructions, click **Help > Explain This Page**, as needed.

1. In Websense Manager, go to **Policies > Delegated Administration**.
2. Click **Add**, and then enter the role name and description.
3. Click **OK** to cache the role name and open the Edit Role page.
4. In the **Administrators** area, add the individuals who will be generating reports on the clients assigned to this role.
5. In the **Managed Clients** area, add the users, groups, computers, and networks the administrators in this role can report on.
6. In the **Reporting Permissions** area, select the reporting options available to all administrators in this role.

   If you did not add any managed clients, be sure to select **Report on all clients** in this area to assure that delegated administrators reports are not empty.
7. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Generate and view reports

Websense Manager can provide several reporting tools for use in evaluating the effectiveness of your filtering policies. For detailed information on using these reporting features, use the **Help** menu in Websense Manager.

The **Today** page appears first when you open Websense Manager. It shows the operating status of Websense software, and can display charts of filtering activities in the network since midnight.

This page also includes a section called Health Alert Summary that presents messages about various elements of the Websense software. Additional information about these messages can be found on the **Alerts** page. Since your Blue Coat integration does not use all the features available in a full Websense Web Security or Websense Web Filter installation uses, there may be several messages in this area.

Some messages can be hidden via the Alerts page. However, messages about the missing Filtering Service and missing subscription key cannot be hidden. These items are not needed for your Blue Coat integration, so there is no cause for concern.

The **History** page shows charts of filtering activities in the network for up to 30 days, depending on the amount of information in the Log Database. These charts do not include today's activities.

The **Presentation Reports** page offers a list of report definitions. Some are tabular reports, some combine a bar chart and a table. To generate a presentation report:

1. Select a report from the list.
2. Click **Run**.
3. Select the date range.
4. Click **Run Now**.

In addition to generating predefined charts, you can copy them and apply a customized report filter that identifies specific clients, categories, protocols, or actions to include. Mark report definitions that you use frequently as Favorites to make them easier to find. You can also schedule any presentation report to run at a particular time or on a repeating cycle.

The **Investigative Reports** page lets you browse through log data interactively. The main page shows a summary-level bar chart of activity by risk class. Click the different elements on the page to update the chart or get a different view of the data.

- Click the risk class name and then select a finer level of detail related to that risk class. For example, you might choose to show activity by user for the Legal Liability risk class.
- Click a user name on the resulting chart to view more detail about that user.
- Choose a different option from the **Internet use by** list to change the summary bar chart.
- Fill in the fields just above the bar chart to display two levels of information at one time. For example, starting with a summary chart of categories, you might choose **10**, **User**, and **5** to display activity for the top 5 users in the top 10 categories.
- Click a bar or number to open a detail report for that item (risk class, category, user, or other).
- Click **Favorite Reports** to save a particularly useful report format for future use, or to generate a previously saved Favorite.

Other Websense Manager options

Websense Manager includes many other features that are used with a full Websense Web Security or Websense Web Filter installation. Only the features described above are effective when reporting on Internet activity filtered by your Blue Coat integration. If you make changes in other areas of Websense Manager, they will be ignored.

3 Troubleshooting

Use this section to find solutions to common issues with the Blue Coat integration before contacting Technical Support.

The Websense Web site features an extensive Knowledge Base, available at www.websense.com/global/en/SupportAndKB/. Search for topics by keyword or reference number, or browse the most popular articles.

Internet requests are not being logged

If reports are empty, the Blue Coat appliance is not configured correctly to communicate with the Log Server. Ensure that the Log Server IP address and port settings are correct. In the Blue Coat Management console, go to Access Logging > Log, and click the **Upload Client** tab to define logging parameters (see *Log facility configuration*, page 9).

Also, go to the Websense installation machine and verify that the Log Server is running via the Windows Services dialog box.

Reports do not show category information

Blue Coat is not configured correctly for communication with the Websense Integration Service. Check the Integration Service IP address and port settings to make sure they are correct. See *Websense database download and reporting configuration*, page 8, for more information.

SQL user account cannot create SQL Server Agent jobs

If you are using Microsoft SQL Server 2005 as your database engine and receive an error stating that the SQL user account does not have permission to create SQL Server Agent jobs:

1. Exit the installer.
2. Use the Microsoft SQL Server Management Studio to update the permissions to provide membership in the **public** and **SQLAgentUserRole** roles in the msdb database, and the **DBCreator** fixed server role.

   For instructions on setting these permissions, go to www.websense.com/SupportPortal, and then search for the article on configuring SQL Server user permissions in SQL Server 2005.

Support

For assistance during installation and configuration of Websense software, consult the following resources.

Online Help

Select the **Help** option within the program to display detailed information about using the product.

Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

Technical Support

Technical information about Websense products is available online 24 hours a day, including:

- latest release information
- searchable Websense Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the Web site at:

www.websense.com/SupportPortal/

For additional questions, fill out the online support form at:

www.websense.com/SupportPortal/Contact.aspx

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

Location	Contact information
North America	+1 858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 57 32 32 27
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 51 70 93 47

Location	Contact information
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884-4200
Latin America and Caribbean	Contact your Websense Reseller.

For telephone requests, please have ready:

- Websense subscription key
- Access to Websense Manager
- Access to the machine running Filtering Service, the machine running reporting tools, and the database server (Microsoft SQL Server or MSDE)
- Permission to access the Websense Log Database
- Familiarity with your network's architecture, or access to a specialist
- Specifications of machines running Filtering Service and Websense Manager
- A list of other applications running on the Filtering Service machine