Websense Integration Service

Reporting Installation and Configuration
for Blue Coat® Appliances

Websense® Web Security
Websense Web Filter

v7.5

©1996–2010, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010
Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Blue Coat and ProxySG are registered trademarks of Blue Coat Systems, Inc.

Microsoft, Windows NT, Windows 2000, Windows 2003, Windows XP, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc., in the United States and other countries. Sun, Sun ONE and all Sun ONE based trademarks and logos are trademarks of Sun Microsystems, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

The following is a registered trademark of Novell, Inc., in the United States and other countries: Novell Directory Services.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries.

Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (**http://www.apache.org**).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

WinPcap

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2009 CACE Technologies, Davis (California).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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 generate summary and detailed 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 Websense Log Server
- Using Websense reporting tools to understand Internet usage and the value of Internet filtering

Hardware and software requirements

Specific hardware requirements vary according to your network size and volume of Internet traffic. For complete information, see the *Deployment Guide for Websense Web Security Solutions* (*Deployment Guide*), available at www.websense.com/docs, which provides hardware and software requirements. 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 SP2
    (Standard or Enterprise)
  - Windows Server 2003, SP2
    (Standard or Enterprise)
  - Windows Server 2008 (x86)
    (Standard or Enterprise)
- **Database engines supported**:
  - Microsoft SQL Server 2008
  - Microsoft SQL Server 2005 SP2 or SP3 (Standard, Enterprise, or 64-bit edition) (recommended)
  - Microsoft SQL Server Desktop Engine (MSDE) 2000 SP 4 (suitable for smaller networks)
    MSDE is available for download from www.websense.com. See the following article for details: http://www.websense.com/support/article/t-kbarticle/Installing-MSDE-with-Websense-software-version-8-1258048438423.
- **Web browsers supported**: necessary for using TRITON - Web Security
  - Internet Explorer 7 or 8
  - Mozilla Firefox 3.0.x - 3.5.x
- **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.

- **TRITON - Web Security**: 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 TRITON - Web Security 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 6) is installed and running in the network.
2. Log on to the installation machine with **domain** and **local** administrator privileges. The installation machine must be joined to the same domain as the database engine machine.

   If you will use a Windows trusted connection to communicate with the database engine to access the Websense Log Database, your logon account must also be a trusted account on the database engine machine with proper database privileges. Specify this same account in the Database Information screen (Step 9) when choosing to use Windows trusted connection to access the Log Database.
3. Close all applications and stop any antivirus software.
4. Download the Websense Reporting Installer for Blue Coat from mywebsense.com.
5. Double-click the downloaded file and then click **Run** when prompted. The installer starts automatically.

> **Note**
> If the installation program displays error messages that it is having difficulty locating other machines, disable any firewall running on the installation machine.

6. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
7. On the **WebsenseAdministrator Password** screen, enter a password for the WebsenseAdministrator user and then click **Next**.

   It is a best practice to enter a password that is *very strong* (at least 8-characters long, containing all of the following: uppercase characters, lowercase characters, numbers, and symbols).

WebsenseAdministrator is the default TRITON - Web Security user with unconditional Super Administrator privileges (access to all administrative functions). This account cannot be removed and its permissions cannot be changed. When logging on to TRITON - Web Security for the first time, do so as WebsenseAdministrator.

Important

Do not lose this password. Only other Super Administrator users can reset the WebsenseAdministrator password. If no other Super Administrator users exist, you must visit MyWebsense (www.mywebsense.com) and enter your subscription key to reset the password. For more information, see the TRITON - Web Security Help.

8. On the **Multiple Network Cards** screen (appears only if multiple network interface cards are detected by the installer), select the IP address of the network interface card (NIC) to be used by Websense software on this machine.
9. On the **Database Information** screen, enter the hostname or IP address of the machine on which a supported database engine is running. If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

   After entering the IP address of the database engine machine, choose how to connect to the database:

   - **Trusted connection**: use a Windows account to log into the database. Enter the user name and password of a trusted account with local administration privileges on the database machine. If you are using MSDE, it is a best practice to connect using a database account rather than trusted connection.

     Important

     The account you specify for trusted connection here must be the same as that used to log onto this machine at the beginning of this installation procedure (Step 2).

   - **Database account**: use a SQL Server account to log into the database. Enter the user name and password for a SQL Server account that has administrative access to the database. The SQL Server password cannot be blank, or begin or end with a hyphen (-). It is a best practice to connect to your database engine using a database account rather than a trusted connection.

     Note

     The database engine (both SQL Server and SQL Server Agent) must be running to install Websense reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

10. On the **Log Database Location** screen, accept the default location for the Log Database, or select a different location. Then, click **Next**.

    If the database engine is on this machine, the default location is the Websense directory (`C:\Program Files\Websense`). If the database engine is on another machine, the default location is `C:\Program Files\Microsoft SQL Server` on that machine.

    It is a best practice to use the default location. If you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files. The path entered here is understood to refer to the machine on which the database engine is located.

    Important

    The directory you specify for the Log Database must already exist. The installer cannot create a new directory.

11. On the **Optimize Log Database Size** screen, select options to control the size of the Log Database, which can grow quite large. Select either or both of the following options and then click **Next**.

    - **Log Web page visits**: Enable this option to log a record of each Web page requested rather than each separate file included in the Web page request. This creates a smaller database and allows faster reporting. Deselect this option to log a record of each separate file that is part of a Web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.
    - **Consolidate requests**: Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):
        - Domain name (for example: www.websense.com)
        - Category
        - Keyword
        - Action (for example: Category Blocked)
        - User/workstation

12. On the **Directory Service Access** screen, specify an account to be used by Websense User Service for transparent identification.

    Enter the domain, user name, and password of an account that is a Domain Admin on the domain controller. This must be the domain controller for the users you wish to apply user- or group-based filtering policies to. User Service uses this account to query the domain controller for user information.

    Note

    User information on domain controllers trusted by the domain controller in question will also be accessible.

If you choose not to specify a Domain Admin account now (by leaving the fields blank), you can specify it after installation, using TRITON - Web Security. For more information, see *Troubleshooting > User Identification* in the TRITON - Web Security Help.

13. On the **Integration Service Port** screen, enter a port (default is 55080) to be used for communication between the Websense Integration Service and Blue Coat appliance.

    You must configure the Blue Coat appliance to use the port entered here (must be in the range 1024-65535; by default, it is 55080).

> **Important**
>
> Make note of this port number. You will need to enter it in the Blue Coat Management console to configure reporting. See *Websense database download and reporting configuration*, page 14.

14. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

    The installation path must be absolute (not relative). The default installation path is C:\Program Files\Websense\

    The installer creates this directory if it does not exist.

> **Important**
>
> The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

The installer compares the installation's system requirements with the machine's resources.

- Insufficient disk space prompts an error message. The installer closes when you click **OK**.
- Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

15. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed. The following components should be listed:

    - Policy Broker
    - Policy Server
    - User Service
    - Log Server
    - TRITON - Web Security
    - Integration Service

16. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
17. On the **Installation Complete** screen, click **Done**.
18. If you chose to use a Windows trusted connection to access the Log Database, set the **Log on as** property of the Apache2Websense and ApacheTomcatWebsense services to the trusted account you specified during installation (in Step 9):
    a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).
    b. Right-click the **Apache2Websense** service and select **Properties**.
    c. In the service properties dialog box, select the **Log On** tab.
    d. Under **Log on as**, select **This account** and enter the domain\username and password (twice) of the trusted account you specified during installation.
    e. Click **OK**.
    f. A message appears informing you the account you specified has been granted the Log On As A Service right. Click **OK**.
    g. A message appears information you the new logon name will not take effect until you stop and restart the service. Click **OK**.
    h. Click **OK** to exit the service properties dialog box.
    i. Right-click the **Apache2Websense** service and select Restart.
    j. Repeat this procedure (from Step b) for the **ApacheTomcatWebsense** service.
19. If you stopped your antivirus software, restart it.
20. Configure the appliance for filtering. See *Filtering configuration*, page 13.
21. Configure the appliance for reporting. See *Websense database download and reporting configuration*, page 14.
22. Configure Websense reporting. See *Configuring Websense Software for Reporting*, page 19.

Upgrading Websense components

To upgrade prior version Websense components, run the current version Websense Reporting Installer for Blue Coat (Reporting Installer) on the machine running those components.

Direct upgrade is supported from version 7.0 or higher of Websense software. For versions prior to 7.0, intermediate upgrades are needed as follows:

- version 5.5 > version 6.1 > version 6.3.2 > version 7.0 > version 7.5

For example, to move from version 6.1 to 7.5, the Websense components must be upgraded to version 6.3.2, then 7.0, and finally to 7.5.

To perform an intermediate upgrade, use the Reporting Installer for the intermediate version. For installation instructions, see the *Reporting Installation and Configuration for Blue Coat Appliances* guide for that version.

Important

After performing an intermediate upgrade from version 6.3.2 to 7.0, reboot the machine before upgrading it to version 7.5.

Complete the following steps to upgrade Websense components from version 7.0 or higher to version 7.5:

1. Make sure a supported database engine (see *Hardware and software requirements*, page 6) is installed and running in the network.
2. Log on to the installation machine with **domain** and **local** administrator privileges. The installation machine must be joined to the same domain as the database engine machine.

   If Websense Log Server uses Windows trusted connection to communicate with the database engine to access the Websense Log Database, you must log on to the installation machine using the same trusted account. Use the Windows **Services** dialog box to find which account is used by Log Server:

   a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).
   b. View the **Log On As** column for Websense Log Server. This is the account you should use.
3. Close all applications and stop any antivirus software.
4. Download the Websense Reporting Installer for Blue Coat from mywebsense.com.
5. Double-click the downloaded file and then click **Run** when prompted. The installer starts automatically.
6. The installer detects the presence of prior version components and asks if you want to upgrade them.
7. Follow the on-screen prompts to complete the upgrade process.

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 using the Windows **Services** dialog box:

   a. Open the Windows **Services** dialog box (usually, **Start > Administrative Tools** > **Services**).
   b. Right-click **Websense Integration Service**, and then choose **Stop**.

2. Use the Windows **Add or Remove Programs** dialog box to remove Websense components:
   a. Open the Windows **Add or Remove Programs** dialog box (usually, **Start > Control Panel > Add or Remove Programs)**.
   b. Select **Websense Web Security / Websense Web Filter** from the list, and then click **Change/Remove**.
   c. Follow the on-screen instructions to remove components.

> **Important**
>
> Select all components for removal. If you select only some of the components for removal, be aware that the Websense Reporting Installer for Blue Coat (Reporting Installer) cannot add those components back to the same machine. You would have to remove the remaining components and then run the Reporting Installer to install all components again.

3. Install the Websense components on another machine. See *Websense component installation*, page 6.

Configure Blue Coat for Websense filtering and reporting

Complete 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. (SGOS 5.x only) Select the **Configuration** tab.
3. From the navigation pane, select **Content Filtering** > **General**.
4. (Optional) 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.

   (SGOS 5.x only) If you enable Local Database, select a **Lookup mode**:

   - **Always**: consults the local database for every Web request.
   - **Uncategorized**: consults the local database only if a URL is otherwise uncategorized.

5. In the **3rd party database** drop-down list, select **Websense**.

   (SGOS 5.x only) Select a **Lookup mode** for the Websense database:

   - **Always**: consults the Websense database for every Web request.
   - **Uncategorized**: consults the Websense database only if a URL is otherwise uncategorized.

6. Accept the defaults for other settings.
7. 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, and 5.3 or later 5.x versions.

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**. 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 some other name that identifies this as relating to Websense logging.
   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**.

   On SGOS 5.x or later, select the **Configuration** tab to see the navigation pane mentioned above.
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 the Blue Coat documentation. For additional information, contact Blue Coat Technical Support.

After configuring the Blue Coat appliance for user authentication, be sure to configure TRITON - Web Security with directory service information. For information on required Websense configuration, see *Configure Settings*, page 20.

Policy configuration

Use the Blue Coat Management console to configure policies that specify which Websense categories network users are permitted to access and when access is permitted. 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 **OK** to display a pop-up window showing the selected URLs and the new category list.
7. Click **Install Policies** to install the policy to the Blue Coat appliance.

For additional information, contact Blue Coat Technical Support.

✓ **Note**

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

2 Configuring Websense Software for Reporting

After installing Websense reporting components to work with your Blue Coat appliance, you should review the Log Server Configuration utility to verify that the settings meet your needs. Additionally, you must configure the following settings in TRITON - Web Security 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 **All Programs > Websense > 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 TRITON - Web Security Help.

Open TRITON - Web Security

Open TRITON - Web Security 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, and then click **Log On**.
3. Use the pages in TRITON - Web Security to configure key settings to enable reporting, as described in *Configure Settings*, below.

Configure Settings

In TRITON - Web Security, use the **Settings** tab to set key configuration options.

1. In the left navigation pane, click the **Settings** tab.
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 This 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 This Page** for details.

4. On the Settings tab, go to **General > Directory Services**.

   Use the Directory Services page to configure the 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 This 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 TRITON - Web Security with their network logon credentials. Click **Help > Explain This Page** for details.

   Be sure to notify these administrators of the address for accessing TRITON - Web Security 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 TRITON - Web Security to generate reports.

- Configure the Logon Directory, as described in *Configure Settings*, page 20. Then, inform the administrators of the address for accessing TRITON - Web Security 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 TRITON - Web Security. To create these accounts:

  1. In TRITON - Web Security, click the **Main** tab in the left navigation pane.
  2. Go to **Policy Management > Delegated Administration**.
  3. Click the **Manage** 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. The following is the general procedure for configuring roles. For detailed instructions, click **Help > Explain This Page**, as needed.

1. In TRITON - Web Security, go to **Policy Management** > **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

TRITON - Web Security provides 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 TRITON - Web Security.

The **Today** page appears first when you open TRITON - Web Security. 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, 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 **Reporting** > **Presentation Reports** page offers a list of report templates. 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**.

In addition to generating reports from the templates, you can copy a template and apply a customized report filter that identifies specific clients, categories, protocols, or actions to include. Mark both report templates and custom reports 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 basis.

The **Reporting** > **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.

See the TRITON - Web Security Help for instructions on using the many features available in both presentation reports and investigative reports.

Other TRITON - Web Security options

TRITON - Web Security 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 TRITON - Web Security, 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/SupportPortal. Search for topics by keyword or reference number, or browse the most popular articles.

Reports are empty

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 15).

Also, go to the Websense installation machine and verify that 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 14, 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 terms *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
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 if any
- Access to TRITON - Web Security
- Access to the machine running Websense software, 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 the machine running Websense software
- A list of other applications running on the Websense machine

Index