ADMINISTRATOR'S GUIDE

Websense Enterprise®
Websense® Web Security Suite™
-including Corporate Edition

v6.3

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

Published January 23, 2007
Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

NP33-0003ADMIN

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 and Websense Enterprise are registered trademarks 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.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Solaris, UltraSPARC, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

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.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

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

Contents

CHAPTER 1 Introduction

Websense software gives network administrators in business, education, government, and other organizations the ability to control, or simply monitor, network traffic to the internet.

This documentation applies to:

- Websense Enterprise®
- Websense Enterprise - Corporate Edition
- Websense Web Security Suite™
- Websense Web Security Suite - Corporate Edition
- Websense Web Security Suite - Lockdown Edition™
- Websense Web Security Suite Lockdown - Corporate Edition

Websense software greatly minimizes employee downtime spent accessing internet data deemed objectionable, inappropriate, or not work-related. The misuse of network resources and the threat of legal action due to inappropriate access are also minimized. Websense software adds a solid layer of security to your network, protecting it from potential spyware, malware, hacking and other intrusions.

The separately-purchased Websense Client Policy Manager enhances regulation of employee desktop software and hardware. For more information, see the *Websense Enterprise Client Policy Manager Administrator's Guide*.

Websense, Inc., strongly recommends that users be informed of your internet access policies.

Websense, Inc., welcomes comments and suggestions regarding the product documentation. Send feedback to **DocFeedback@websense.com**. Include your organization's name in your message.

Overview

Working in conjunction with integration products—proxy servers, firewalls, routers, and caching appliances—Websense software provides the engine and configuration tools to develop and enforce internet access policies.

Note

Delegated Administration and Reporting, available in Corporate Edition only, provide flexibility in managing filtering and reporting across client sets and locations. For more information, see *Chapter 8: Delegated Administration*.

For a quick-start tutorial, go to www.websense.com, and then navigate to the Product Documentation page. Go to the *Getting Started* section.

Each Websense component performs a particular function. For more information, see *Chapter 2: Websense Components*.

Websense Enterprise Reporter, along with its associated Log Server, is a separate program included with Websense software. Log Server records internet activity in your network. Reporter lets you generate reports and charts depicting your network's internet usage trends. Reports can be used to refine internet filtering strategies, helping to maximize network resources and employee productivity.

Note

Websense software sends log information that can only be read by the corresponding version of Reporter. Install or upgrade Reporter as appropriate to generate reports.

Websense Enterprise Explorer also uses the Websense Log Server. Explorer provides a sophisticated, browser-based view of internet usage. For more information, see the Websense Reporting documentation.

Websense Enterprise Real-Time Analyzer™ (RTA) is an optional component. With RTA, view real-time internet activity via a web browser.

RTA lets you view internet usage trends for your network. Use the information from RTA reports to fine-tune your internet usage policies.

Filtering defaults

Immediately following download of the Websense Master Database, the **Global** policy begins monitoring or filtering according to the selection made during installation.

Websense software installs predefined settings for filtering internet protocols and applications, and uses these until configured otherwise. You can customize how protocols are filtered, and configure filtering based on bandwidth usage within your network. For more information, see *Managing protocols*, page 274.

The **Global** policy serves as the default policy. The Websense Filtering Service uses it to monitor or filter every client (user, group, workstation, or network) until the client has been assigned another policy.

> **Note**
>
> If this is an upgrade, Websense software filters according to the settings and policies in your previous version.

Depending on the selection made during installation, the **Global** policy either permits, monitors, and logs all traffic, or blocks categories that are commonly considered unacceptable while granting full or limited access to others. Modify the **Global** policy to suit the largest number of users in your organization (see *The Global policy*, page 300).

A single policy is usually not adequate for an entire organization. For example, one policy could block or limit travel sites to prevent employees from planning personal vacations during work hours. However, if certain employees need to arrange business travel, create another policy that permits travel sites.

Each policy defines which URL categories and protocols are permitted, blocked, or limited at particular times during the week. For category filtering settings, see *Editing a category set*, page 257. For protocol filtering settings, see *Editing a protocol set*, page 290.

A yes list (see *Yes lists*, page 250) can be used to further restrict internet access for users governed during the related time period in a policy. Assigning customized policies to specific clients ensures that each client's internet access fits work requirements.

When a user attempts to access a website, the Websense Network Agent or your integration product receives the request and sends it to the Websense Filtering Service (see *Filtering Service*, page 29). Filtering Service identifies the policy assigned to the requestor and consults the Websense Master Database (see *Websense Master Database*, page 30).

If the site is not found in the Master Database, or is in a permitted category, Filtering Service allows access to the site. If the site is listed in a blocked category, Filtering Service displays a message that the requested site is blocked, and identifies the category under which it is blocked.

Optionally, block by default all sites that are not listed in the Master Database. For more information, see the appropriate installation guide.

Filtering Service follows a specific precedence in determining how to handle requests. For more information, see *Chapter 3: Filtering Basics*.

Internet content transmitted by particular network or application protocols is handled similarly. For more information, see *Managing protocols*, page 274.

The **Limit by Quota** filtering option lets you allocate per-day time to employees for surfing sites in categories you deem appropriate. Quotas give you control over time spent on personal surfing. For more information, see *Quotas*, page 44.

For further flexibility in filtering, define customized lists of URLs to be filtered in particular ways for all users. For more information, see *Custom URLs*, page 259.

Subscriptions

Websense subscriptions are issued on a per-client basis. When you purchase a subscription, a subscription key is provided in the CD package or via email if you download the software. Each key is valid for 1 installation of Websense Policy Server. If you install multiple Policy Servers, you need a separate key for each.

Before you can begin filtering, you must enter a valid subscription key. This lets you download the Master Database, which enables Websense software to filter clients.

After the first successful database download, Websense Manager displays the number of clients your subscription includes. For information on entering your key and downloading the Master Database, see *Database downloads*, page 58.

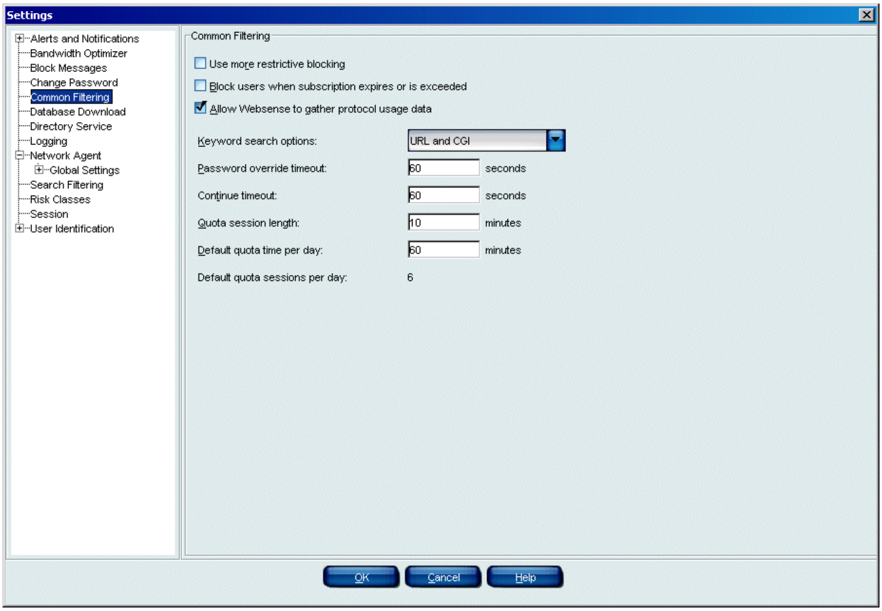
The total number of client machines filtered depends on the subscription level purchased. The subscription level is the number of clients for which Websense software processes internet requests. Websense software maintains a subscription table of clients filtered each day (where a client corresponds to a user or workstation in your network), and processes requests in the subscription table.

The subscription table is cleared each night. The first time a client makes an internet request after the table has been cleared, its IP address is entered in the table.

When the number of clients listed in the table reaches the subscription level, any previously-unlisted client that requests internet access exceeds the subscription. If this occurs, the client exceeding the subscription level is either blocked entirely from the internet or given unfiltered internet access, depending on the **Block users when subscription expires or is exceeded** setting (see the procedure that follows). Likewise, when a subscription expires, all clients are either entirely blocked or unfiltered, depending on this setting.

To determine filtering behavior when a subscription is exceeded:

1. In Websense Manager, select **Server > Settings**. The Settings dialog box appears.
2. Select **Common Filtering** at the left. The Common Filtering settings are displayed.



Common Filtering

□ Use more restrictive blocking

□ Block users when subscription expires or is exceeded

☑ Allow Websense to gather protocol usage data

Keyword search options: URL and CGI

Password override timeout: 60 seconds

Continue timeout: 60 seconds

Quota session length: 10 minutes

Default quota time per day: 60 minutes

Default quota sessions per day: 6

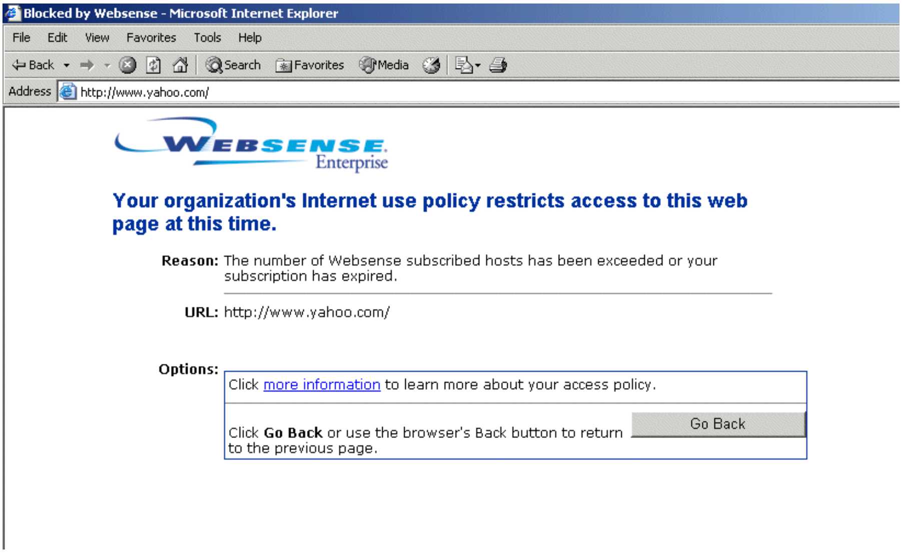
Common Filtering Settings

3. Check or uncheck **Block users when subscription expires or is exceeded**.

   If this option is *checked*, an expired subscription causes Filtering Service to block all users from accessing the internet. An exceeded subscription causes Filtering Service to block the clients exceeding the subscription.

   If this option is *unchecked*, an expired subscription causes Filtering Service to allow all clients unfiltered access to the internet, and an exceeded subscription allows unfiltered access to the clients exceeding the subscription.
4. Click **OK**.

When a subscription is exceeded, a requesting user sees the Websense block page shown below.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.yahoo.com/
WEBSENSE
Enterprise

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The number of Websense subscribed hosts has been exceeded or your subscription has expired.

URL: http://www.yahoo.com/

Options:

Click more information to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page.

Block page resulting from exceeded subscription

If you have more IP addresses in a Dynamic Host Configuration Protocol (DHCP) range than your Websense subscription level allows, you may exceed the subscription. If this occurs, contact Websense, Inc., or an authorized Websense reseller to upgrade your subscription.

To configure Websense software to send email warnings when the subscription approaches or exceeds its limit, see *Setting up alerting*, page 201.

The number of categories filtered depends on your Websense subscription. Websense software filters all sites that are in categories activated by your purchase.

Groups of categories that can be purchased separately are called Premium Groups, and have **[monitor only]** next to their names in Websense Manager until they are purchased. Sites in unpurchased Premium Groups are permitted, and access to them is logged as “Category Not Purchased.” For more information, see *Premium Groups*, page 66.

Websense editions

Websense, Inc., provides multiple editions:

- Websense Enterprise
- Websense Enterprise - Corporate Edition
- Websense Web Security Suite
- Websense Web Security Suite - Corporate Edition
- Websense Web Security Suite - Lockdown Edition
- Websense Web Security Suite Lockdown - Corporate Edition

Each edition provides features tailored to particular filtering and security needs. Certain features are available only in Corporate or Security Suite Editions of Websense Enterprise. Such features are indicated throughout this book.

Any references in this book that mention *Websense Enterprise* refer to all editions.

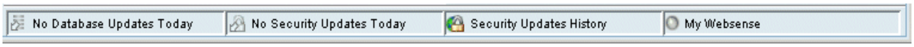
Contact Websense, Inc., for information on upgrading Websense software, or purchasing special features.

Contact information web page

MyWebsense is a website dedicated to maintaining contact information for customers. This web page opens by default when installation is complete.

To access the page manually:

- Select **Help** > **MyWebsense.com**.
- Click the **MyWebsense** link in the status bar at the bottom of the Websense Manager window.



Status bar

View or update your Websense registration information as necessary.

Getting started

To begin filtering internet requests, install Websense software, enter a valid subscription key, and download the Master Database. For more information, see the installation guide.

Get familiar with the Websense components and reporting tools (see *Chapter 2: Websense Components*). Then, begin adding clients, and setting up filtering policies for managing those clients.

Quick start to managing internet access

After you have installed Websense software and optionally set up communication with a directory service (see *Chapter 6: User Identification*), Websense software begins filtering internet requests. If this is an upgrade, Websense software filters according to your policies in the previous version. If this is a new installation, Websense software applies the **Global** policy.

✓ **Note**

Initial, default filtering behavior is determined by your **Initial Filtering** selection during installation.

During installation, you define the initial **Global** policy when you select either to filter internet traffic or monitor it. If you select **Monitor Internet traffic only**, then all requests are permitted and logged. If you select **Filter Internet traffic based on a predefined policy**, then the Global policy enforces the **Default Settings** category set and the **Default Settings** protocol set 24 hours a day, 7 days a week.

Initially, the **Default Settings** category set blocks the following categories:

- Adult Content
- Nudity
- Sex
- Abused Drugs
- MP3
- Gambling
- Games
- Hacking

- Illegal or Questionable
- Job Search
- Militancy and Extremist
- Proxy Avoidance
- URL Translation Sites
- Web Chat
- Uncategorized
- Racism and Hate
- Tasteless
- Violence
- Weapons

All other categories are either permitted or limited by quota time (see *Quotas*, page 44*)*.

Premium Group categories are available only if purchased. For more information, see *Premium Groups*, page 66.

With the **Default Settings** protocol set, the Instant Messaging/Chat, Instant Messaging File Attachments, P2P File Sharing, and Proxy Avoidance protocol groups are blocked by default. All other protocols and internet applications are permitted. To customize filtering settings, see *Customizing protocols and protocol sets*, page 284.

Use Websense Manager to modify the **Global** policy, or to create additional policies to meet the specific filtering needs of your organization. For more information, see *Customizing Websense software*, page 24.

Websense Manager interface

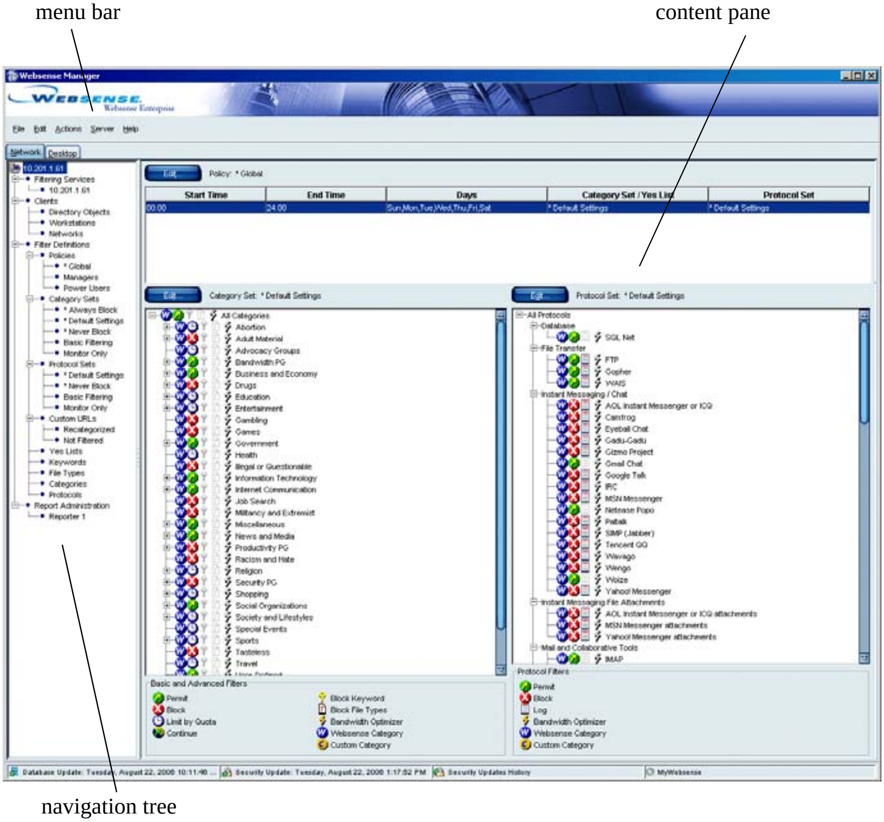
Websense Manager is the filtering configuration interface that lets you customize filtering behavior (see *Customizing Websense software*, page 24).

To start Websense Manager on Windows, select **Start** > **Programs** > **Websense** > **Websense Manager**.

To start Websense Manager on Solaris or Linux, go to the `/Manager` subdirectory in the Websense installation directory and enter:

```
./start_manager
```

The window consists of a menu bar, navigation tree and content pane.



Websense Manager window

Top-level commands are:

- Main menu bar: Provides commonly-used Websense commands. Websense Manager offers shortcut menus for many functions. Right-click to access shortcut menus.
- **Save Changes** button: Sends changes to the Policy Server where you are logged on. Changes to category sets/yes lists, protocol sets, policies, custom categories, file types, or clients are *not* implemented until you click **Save Changes**.

> ✓ **Note**
>
> Changes made in the Settings dialog box are implemented when you click **OK**. Changes made in sub-dialog boxes also do not take effect until you click **OK**.

- **MyWebsense** button: Links to your personalized mywebsense.com page. For more information, see *Contact information web page*, page 16.

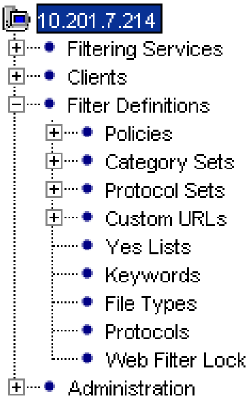
Context-sensitive help

Most dialog boxes have **Help** buttons. If a **Help** button is not available, click in the relevant area of the window and then press **F1**.

Navigation tree

After a Policy Server has been added, the navigation tree lists the Policy Servers available for configuration from this instance of Websense Manager. Once you log on to a Policy Server and enter the password (see *Logging on to a server*, page 187), the navigation tree displays the topics for that server.

Click the plus symbol (+) beside a topic to display its child entries. For example, expand **Policies** to show the policies that have been created. Click an entry to display its details in the content pane.



Navigation tree

Topics in the navigation tree are:

- **Directory Objects**, **Workstations**, **Networks**: Client objects (see *Chapter 5: Clients*) added to Websense Manager. Add individual users and groups as defined in your directory service, specific workstations, or networks identified as IP address ranges.
- **Policies**: The basis of filtering. Each policy identifies which category set or yes list, and which protocol set, are enforced during particular time periods. A policy is assigned to all clients to be filtered according to its restrictions.

  Websense software includes sample policies. Edit these, or create additional policies. By default, clients are filtered by the **Global** policy until another policy is assigned to them (see *About filtering policies*, page 243).

- **Category Sets**: Lists of all Websense categories, with a filtering setting designated for each. Settings include permit, block, limit by quota or file type, bandwidth-based limitations, and continue. Enable keyword blocking in conjunction with any filtering setting.

  Category sets are assigned to time periods within policies (see *Category Sets/Yes Lists*, page 245).
- **Protocol Sets**: Lists of all protocols with a filtering option designated for each. Settings include permit, block, log, and bandwidth-based limitations. Protocol sets are assigned to time periods within policies (see *Managing protocols*, page 274).
- **Custom URLs/Recategorized**: Sites to filter differently than their Master Database categories (including sites classified under Miscellaneous/Uncategorized). Add a URL to any category. Websense software filters the site according to the filtering setting for that category. For more information, see *Custom URLs*, page 259.
- **Custom URLs/Not Filtered**: Master Database sites originally assigned to blocked categories but which you now permit.

  When you add a URL to the Custom URLs/Not Filtered list, Websense software permits that site for all users who have internet access, with these exceptions:

  - When the **Always Block** category set is active
  - When a user is governed by a yes list

  For more information, see *Custom URLs*, page 259.
- **Yes Lists**: Custom-defined lists of sites to permit regardless of other filtering settings. URLs on a yes list are the only sites allowed for the users governed by the associated policy. When multiple policies apply to the same client, yes lists take precedence over any other category set, including the **Always Block** category set. For more information, see *Yes lists*, page 250.
- **Keywords**: Filtering restrictions that block sites whose URLs contain certain words. When keyword blocking is activated for a category, Websense software blocks any site whose URL contains a keyword assigned to the category (see *Keywords*, page 268).

- **File Types**: Groupings of file extensions used for similar purposes. Filter internet content based on file extension. For example, restrict access to particular types of files from sites within an otherwise-permitted category.

  File type filtering is activated via policies. Modify the predefined file types provided, or create new file types (see *About file types*, page 246).

- **Protocols**: Websense objects representing types of internet data transmitted via particular protocols or internet applications. Use the Websense-defined protocols provided, or create new protocol definitions.

  Filtering settings are designated to each protocol within a protocol set. The protocol set is then associated with a time period in a policy. For more information, see *Managing protocols*, page 274.

- **Web Filter Lock** *(Corporate Edition only)*: Key filtering restrictions to be applied to all clients; limits which policy elements can be modified by Delegated Administrators. The Web Filter Lock is only available with the Distributed Administration and Reporting feature, included in Corporate Editions of Websense. For more information, see *Chapter 8: Delegated Administration*.

- **Administration** *(Corporate Edition only)*: Administrative user objects. There is always one Super Administrator. Additional Delegated Administrators can be created by the Super Administrator, and assigned certain permissions. **Administration** is only available with the Distributed Administration and Reporting feature, included in Corporate Editions of Websense. For more information, see *Chapter 8: Delegated Administration*.

  Report Administration *(non-Corporate Edition only)*: Administrative user objects. If you are not running Corporate Edition, you can still define roles and permissions for reporting purposes. For information about using Websense Reporting Tools, see the Reporting documentation.

Customizing Websense software

Follow these steps to configure Websense software to begin filtering. For more information, see the referenced sections.

> **Note**
>
> If you are running a Corporate Edition of Websense, the Distributed Administration and Reporting feature provides increased internet access management functionality. For more information, see *Chapter 8: Delegated Administration*.

1. Start Websense Manager:

   On Windows: **Start** > **Programs** > **Websense** > **Websense Manager**.

   On Solaris or Linux, go to the `/Manager` subdirectory in the Websense installation directory and enter:

   ```
   ./start_manager
   ```

2. Add Policy Server (see *Adding a server*, page 186).
3. Log on to Policy Server: Right-click the server icon and select **Log On to Server**.
4. Enter the password. This is established when first logging on to Policy Server.
5. If not done during installation, download the Master Database (see *Database downloads*, page 58).
6. Configure the Websense Network Agent (see *Initial configuration*, page 83).
7. Select **Server** > **Settings**, and then make appropriate changes (see *Configuring a server*, page 189).
8. Click **OK** to save server configuration changes.
9. Expand **Policies** in the navigation tree, and then select **Global**.

   To change enforcement times, category sets/yes lists, or protocol sets enforced by the **Global** policy, click **Edit**. For more information, see *Editing a policy*, page 302. Click **OK** when finished.

10. Expand **Category Sets** in the navigation tree, and then select **Default Settings**.

11. Click **Edit**, and then select the desired filtering options for each category. Filtering settings are enforced whenever the **Default Settings** category set is active. Click **OK** when finished. For more information, see *Editing a category set*, page 257.
12. Expand **Protocol Sets** in the navigation tree, and then select **Default Settings**.
13. Click **Edit**, and then select the desired filtering settings for each protocol. Filtering settings are enforced whenever the **Default Settings** protocol set is active. Click **OK** when finished. For more information, see *Editing a protocol set*, page 290.
14. To apply filtering policies to particular users or groups, first configure Websense to access your directory service. For more information, see *Directory services*, page 99.
15. Determine how to identify users and groups pulled from your directory service. For more information, see *Chapter 6: User Identification*.
16. Click **Save Changes** above the navigation tree to update Policy Server.

Now you can add category sets, protocol sets, policies, file types, custom URLs, and keywords, and assign policies to individual clients.

Directory services

Websense software can communicate with Windows NTLM-based directories, as well as Windows Active Directory, Sun Java System Directory Server and Novell Directory Services/eDirectory, accessed via Lightweight Directory Access Protocol (LDAP).

Websense, Inc., recommends installing the Websense User Service on a Windows machine (though it can reside on a Linux/Solaris machine). Typically, this is the machine where Policy Server is installed.

If you are running Websense Enterprise Client Policy Manager modules, these must be configured to point to Policy Server and User Service. Alternatively, install separate instances of Policy Server and User Service for use with Client Policy Manager modules only.

Websense software can communicate with a directory service whether it runs on the same operating system as Websense software or on a different operating system. Even if you are using a Windows NTLM-based directory service, you can run the Websense User Service on Windows, Linux, or Solaris.

To configure Websense software to communicate with your directory service, see *Directory services*, page 99.

CHAPTER 2

Websense Components

Understanding fundamental concepts and how they apply to internet filtering helps you use Websense most effectively.

- Primary Websense components:
    - Filtering Service
    - Policy Server
    - User Service
    - Websense Manager
    - Master Database
    - Network Agent
    - Usage Monitor
- Optional transparent identification agents:
    - DC Agent
    - RADIUS Agent
    - eDirectory Agent
    - Logon Agent
- Optional remote filtering components:
    - Remote Filtering Server
    - Remote Filtering Client
- Optional real-time reporting component, Real-Time Analyzer

Filtering

These components work together to filter internet requests.

Policy Server

Websense Policy Server stores server and policy configuration information. Policy Server communicates this data to Filtering Service, which filters internet requests. Configure Policy Server settings via Websense Manager (see page 30).

After installation, Policy Server identifies other Websense components. Policy Server continually tracks the location and status of other Websense services. View or manually modify Websense service status. For more information, see *Stopping or starting Websense services*, page 191.

If your network is large (10,000+ users), you may need multiple Policy Servers. You can replicate configuration settings from 1 Policy Server in your network to another. This functionality varies depending on which edition you are running.

- *Corporate Edition installations*: See *Distributing configuration settings*, page 237.
- *Non-Corporate Edition installations:* See *Distributing policies to multiple servers*, page 306.

The Distributed Administration and Reporting feature, available with Corporate Editions of Websense, offers sophisticated management of multiple-server, multiple-site enterprises. For more information, see *Delegated Administration*, page 215.

Filtering Service

Websense Filtering Service interacts with your integration product to provide internet filtering. When a user requests a site, your integration product sends the request to Filtering Service. The exception is with the Websense Enterprise Stand-Alone Edition (see *Filtering internet content*, page 94).

For each request it receives, Filtering Service determines which policy applies. Once the active policy is determined, Websense software filters the site according to the policy's restrictions.

Configure Filtering Service attributes via Websense Manager (see *Websense Manager*, page 30).

> **Note**
> When Filtering Service is not running, filtering and logging of internet requests cannot occur. For information about Websense logging and reporting, see the Websense Reporting documentation.

Network Agent

The Websense Network Agent enhances filtering and logging capabilities and enables management of internet protocols and applications outside the browser. Network Agent can also evaluate Websense internet filtering capabilities. For more information, see *Chapter 4: Network Agent*.

Websense Master Database

The Websense Master Database is a collection of more than 18 million internet sites. Sites are sorted into more than 90 categories and subcategories. All sites contained in the Master Database have been reviewed by professional web analysts to confirm category accuracy.

The Master Database houses more than 80 protocol definitions for use in filtering protocols. The updated list of protocols is at:

www.websense.com/global/en/ProductsServices/MasterDatabase/

Another way to get an accurate listing of protocols is to download the database and view the latest protocols via Websense Manager.

Websense, Inc., updates the Master Database daily to maintain accuracy and quality, adding new sites and protocols, and deleting inactive sites.

In addition to the standard categories provided in the Websense Master Database, optionally implement more advanced URL filtering using Websense Enterprise Premium Group categories.

For an up-to-date list of Websense categories, go to:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

Websense Manager

Websense Manager is the configuration interface. It can run on the same machine as Policy Server, or on one or more different machines in your network. Use Websense Manager to define and customize internet access policies, add or remove clients, configure Policy Server, and more. For more information, see *Websense Manager interface*, page 19.

Configure Policy Server to communicate with Websense Manager by adding Policy Server. To get started, see *Chapter 3: Filtering Basics*.

Websense Usage Monitor

This behind-the-scenes service enables alerting based on internet usage. Usage Monitor tracks URL category and protocol visits made by clients, and generates alert messages according to the alerting behavior you have configured. For more information, see *Alerting*, page 199.

Remote Filtering Server

The Websense Remote Filtering Server allows filtering of clients outside a network firewall. The installation guide includes instructions for installing the Websense Remote Filtering Server, which communicates with Filtering Service to provide internet access management of remote machines.

Remote Filtering Client

This client application for remote filtering resides on client machines outside the network firewall. Remote Filtering Client identifies client machines to be filtered, and communicates this information to Remote Filtering Server. For instructions on deploying Remote Filtering Client, see the installation guide.

User identification

The Websense User Service works with any of several optional components to identify users.

User Service

Websense User Service communicates with your directory service to convey user-related information to Policy Server and Filtering Service, for use in applying filtering policies. This includes user-to-group and user-to-domain relationships.

If you have installed a Websense transparent identification agent and activated transparent identification of users (see *Transparent identification*, page 130), User Service helps to interpret user logon session information. User Service uses logon session information from the agent to satisfy Filtering Service requests for user name-to-IP-address associations.

When you add directory objects to Websense (see *Adding directory objects*, page 114), User Service provides the list of objects residing in your directory service to Websense Manager, for use in configuring filtering policies.

There must be 1 instance of User Service for each Policy Server in your network. For information, see *Multiple Policy Server environment*, page 42.

For information about configuring directory service access and customizing directory service search filters, see *Directory services*, page 99.

DC Agent

The Websense DC Agent transparently identifies users in a Windows-based directory service, without prompting users to manually authenticate. DC Agent communicates with User Service to provide up-to-date user logon session information to Websense software for use in filtering. For more information, see *Websense DC Agent*, page 134.

Logon Agent

The Websense Logon Agent provides unsurpassed accuracy in transparent user identification. The associated logon application on client machines ensures that individual user logon sessions are captured and processed directly by Websense software. This enables the Websense Filtering Service to accurately filter based on policies assigned to directory objects (such as users or groups).

Logon Agent does not rely on a directory service or other intermediary component when capturing user logon sessions. It detects user logon sessions as they occur. This maximizes accuracy in identifying users as they log on to the network.

For more information, see *Websense Logon Agent*, page 141.

RADIUS Agent

The Websense RADIUS Agent lets you integrate filtering policies with authentication provided by a RADIUS server. The Websense RADIUS Agent enables Websense software to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection (depending on your configuration). Assign particular filtering policies to users or groups of users who access your network remotely.

For more information, see *Websense RADIUS Agent*, page 148.

eDirectory Agent

The Websense eDirectory Agent works together with Novell eDirectory to transparently identify users so Websense software can filter them according to particular policies assigned to users or groups.

eDirectory Agent uses Lightweight Directory Access Protocol (LDAP) to gather user logon session information from Novell eDirectory, which authenticates users logging on to the network. The Websense eDirectory Agent associates each authenticated user with an IP address. With the help of the Websense User Service, eDirectory Agent supplies this information to the Websense Filtering Service. For more information, see *Websense eDirectory Agent*, page 162.

Reporting

The Websense Log Server stores internet request data, including:

- Source of a request
- Category or protocol associated with a request
- Whether the request was permitted, blocked, or limited by quota, keyword blocking, bandwidth levels, or password protection

Depending on your integration product, Log Server also stores information about number of bytes transferred.

After installing Log Server, configure the Log Server location and port number (see *Logging and Reporting*, page 74).

Websense Enterprise® Reporter

Websense Enterprise Reporter, included with Websense software, generates tabular and graphical internet usage reports. Reports allow you to monitor internet access and fine-tune filtering policies.

For more information, see the Reporting documentation.

Websense Enterprise Explorer

Explorer works with the Websense Log Database, a web server and a web browser to provide flexible, browser-based reporting. Explorer offers sophisticated reporting functionality on both Windows and UNIX.

For more information, see the Reporting documentation.

Websense Enterprise Real-Time Analyzer™

Websense Enterprise Real-Time Analyzer (RTA) is an optional component that graphically displays real-time internet activity via web browser.

RTA lets you view and analyze internet usage trends and verify the effectiveness of filtering policies.

RTA displays internet activity as it flows through Filtering Service, before activity is recorded in the Log Database. To use RTA, you must have Policy Server, Filtering Service, a web server, and a web browser installed.

For information about managing access to and using RTA, see the Reporting documentation.

CHAPTER 3 Filtering Basics

It is simple to implement internet filtering using the default settings Websense software provides, but the level of filtering complexity is also highly customizable.

Filtering order

Websense software uses multiple filters, applied in a specific order, to determine whether to permit, block, or limit requested internet data. Understanding this order helps you create more effective filtering policies.

For each request it receives, Websense software verifies subscription compliance, then determines which policy applies. Once the policy is determined, Websense software filters the site according to the policy's restrictions. This process is described next.

Ensuring subscription compliance

When Websense software receives a site request, it evaluates your subscription. If the subscription is current and the number of subscribed clients has not been exceeded, Websense software searches for the active policy, as described in the next section.

If the subscription has expired or the most recent client's request causes the subscription limit to be exceeded, the Websense Filtering Service either blocks all sites or permits all sites, depending upon the selection under **Common Filtering** in the Settings dialog box (see *Subscriptions*, page 13).

If the subscription is exceeded, you must renew or increase your subscription. Contact Websense, Inc. or your authorized Websense reseller.

Determining the policy

After subscription compliance has been established, Websense software determines which policy applies to the current request, searching in this order:

1. Policy assigned to the *user.*
2. Policy assigned to the IP address (*workstation* or *network*) of the machine being used.
3. Policies assigned to *groups* the user belongs to.
4. The **Global** policy.

If a policy does not have a category set or protocol set scheduled at the time a request is made, Websense software looks further and filters according to the category set or protocol set scheduled at the same time in the next applicable policy.

If there is no other applicable policy, Websense software filters according to the **Global** policy.

Note

If you selected **Filter Internet traffic based on a predefined policy** during installation, then the Global policy enforces the **Default Settings** category set and the **Default Settings** protocol set. If you selected **Monitor Internet traffic only**, the Global policy monitors and logs internet traffic, but permits all requests by default.

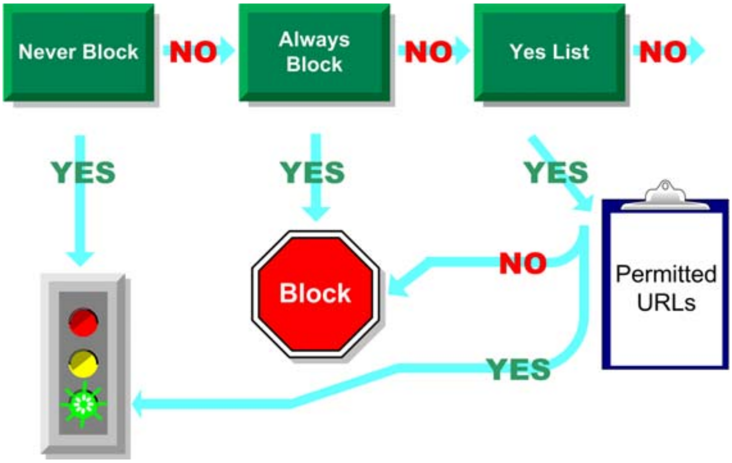
When multiple group policies apply

In some cases, a user belongs to more than 1 group and no user, workstation, or network policy applies. If these cases, Websense software checks the policies assigned to each of the user's groups. If all the groups have the same policy, Websense software filters the request according to that policy.

If one of the groups has a different policy, Websense software filters the request according to the selection made via **Server > Settings > Common Filtering**. If **Use more restrictive blocking** is checked, Websense software blocks the site if it is blocked by *any* of the policies assigned to those groups. If **Use more restrictive blocking** is left unchecked, Websense software permits the site if it is permitted by any of the policies assigned to those groups. For more information, see *Yes lists and multiple groups*, page 251.

After determining which policy applies, Websense software filters the requested site according to the policy's restrictions.

Filtering the site



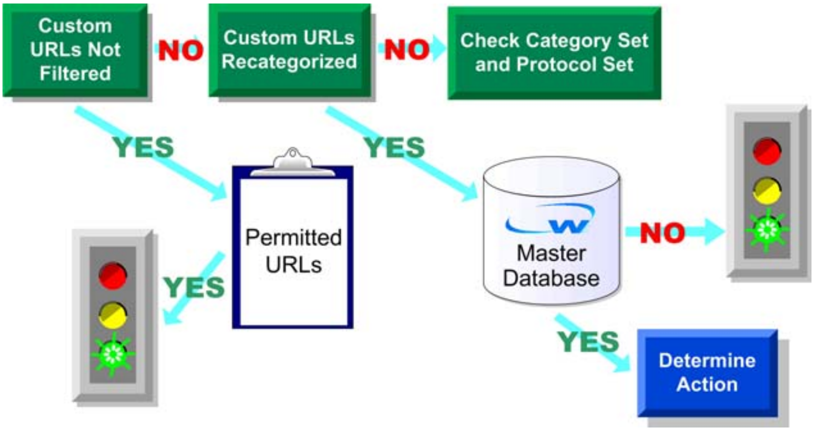
Determining global filtering options

The Websense Filtering Service evaluates the policy's restrictions as follows to determine whether the requested site should be permitted, blocked, or limited by quota.

1. Determines the policy's active category set for the current day and time.
   - If the active category set is **Never Block**, permit the site.
   - If the active category set is **Always Block**, block the site.
   - If the active category set is a yes list, check whether the yes list contains the URL. If so, permit the site. If not, block the site.
   - If any other category set applies, continue to Step 2.

Note

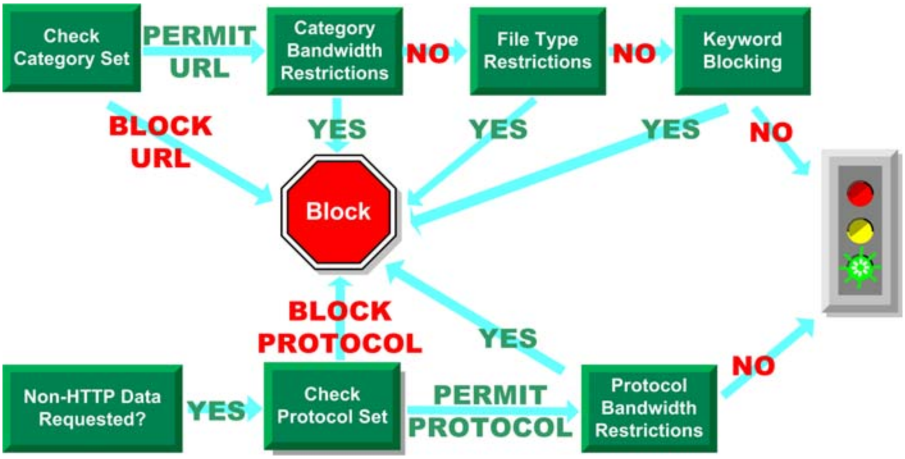
Websense software filters URLs accessed from an internet search engine's cache like any other URLs. URLs stored this way are filtered according to policies active for their URL categories. Log records for cached URLs show the entire cached URL, including any search engine parameters.



Checking for Custom URLs

2. Tries to match the site to a URL in the Custom URLs/Not Filtered list.
   - If the URL appears on the list, permit the site.
   - If the URL does not appear on the list, continue to Step 3.
3. Tries to match the site to a URL in the Custom URLs/Recategorized list.
   - If a match is made, identify the category for the site and go to Step 5.
   - If a match is *not* made, continue to Step 4.
4. Tries to match the site to an entry in the Master Database.
   - If the URL appears in the Master Database, identify the category for the site and continue to Step 5.

- If a match is *not* made, skip to Step 6.

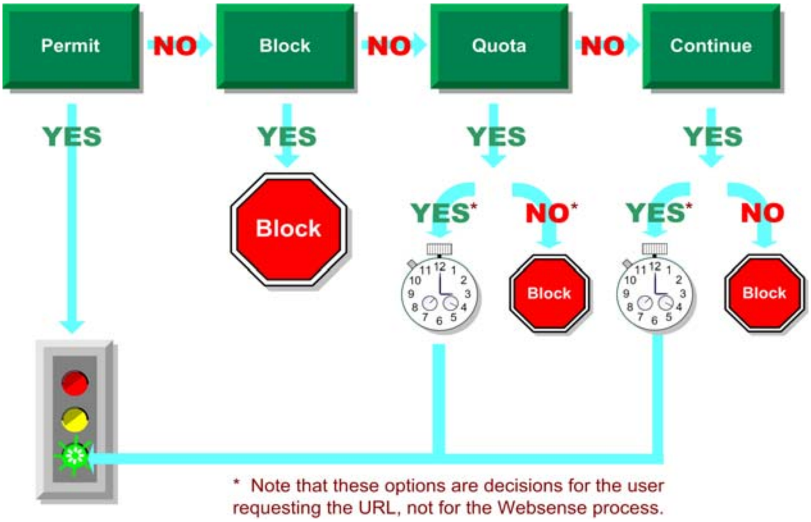


Checking the category set and protocol set

5. Checks the active category set and identifies the filtering option for the category of the requested site.
   - If the filtering option is **Block**, block the site.
   - If any other filtering option is in effect, continue to Step 6.
6. Checks the active protocol set and determines whether any protocols are associated with the request. If so, applies any protocol filtering settings to data that may be transmitted.
7. Checks for bandwidth-based filtering settings in the active category set.
   - If current bandwidth usage exceeds any configured limits, block the site.
   - If current bandwidth usage does not exceed the specified limits, or no bandwidth-based filtering options are active, proceed to Step 8.
8. Checks for file type restrictions applied to the active category.
   - If the site contains files whose extensions are set to **Blocked**, then block access to those files, or to the site if the site itself is comprised of a blocked file type.
   - If the site does not contain files whose extensions are blocked, permit the site and any files associated with it.

   For more information, see *About file types*, page 246.

9. Checks for blocked keywords in the URL and CGI path, according to the **Keyword search options** selection (**Settings** > **Common Filtering**).
   - If a blocked keyword is found, block the site.
   - If a blocked keyword is *not* found, continue to Step 10.
10. Handles the site according to the filtering option set for the category.
    - **Permit**: Permit the site.
    - **Limit by Quota**: Display the Websense block message with an option to view the site using quota time or go back to the previous page.
    - **Continue**: Display the block message with the option to view the site for work purposes.


Permit
NO
Block
NO
Quota
NO
Continue
YES
YES
YES
YES
Block
YES*
NO*
YES*
NO
Block
Block
* Note that these options are decisions for the user requesting the URL, not for the Websense process.

User options for a request

Websense software proceeds until the requested site is either blocked or explicitly permitted. At that point, Websense software does not attempt any further filtering. For example, if a requested site belongs to a blocked category *and* contains a blocked keyword, Websense software blocks the site at the category level without checking the keyword filter. Log Server then logs the request as blocked because of a blocked category, not because of a keyword.

Note

Users with password override privileges can access internet sites regardless of why the site was blocked.

Multiple Policy Server environment

In environments with a large number of workstations, installing multiple Policy Servers for load-balancing purposes may be appropriate. However, some load-balancing configurations permit the same user to be managed by different Policy Servers, depending on the current load. In this configuration, do not implement time-based filtering settings:

- Password Override
- Continue
- Quotas

The timing information associated with these features is not shared among Policy Servers, and users could be granted more or less internet access than you intend.

By default, the **Limit by Quota** filtering option is selected for some categories in the **Default Settings** category set. The **Default Settings** category set is used for any time period when no other category set is assigned.

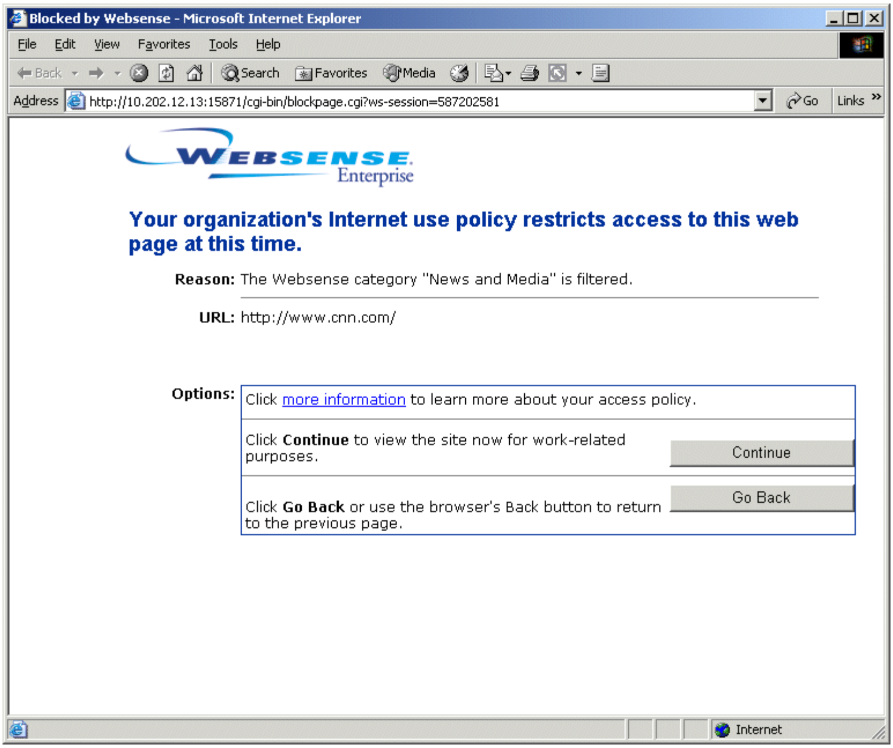
If users can be governed by more than one Policy Server, do one of the following:

- Select a different (non-time-based) filtering setting in all category sets that use quotas, including the **Default Settings** category set.
- Assign 0 minutes of quota time to the clients who may be governed by multiple Policy Servers (see *Allocating quota time to clients*, page 125).
- Change the default quota time to 0 minutes in the Settings dialog box under **Common Filtering**. (This setting affects all users.)

If you are running a *Corporate Edition* of Websense, see *Central Configuration Distribution*, page 235 for information about Policy Servers in a distributed environment.

Continue

With the Continue filtering option, the user can view the site for business purposes, or go back to the previous web page.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
WEBSENSE Enterprise
Continue
Go Back
Internet

http://10.202.12.13:15871/cgi-bin/blockpage.cgi?ws-session=587202581

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "News and Media" is filtered.

URL: http://www.cnn.com/

Options: Click more information to learn more about your access policy.

Click **Continue** to view the site now for work-related purposes.

Click **Go Back** or use the browser's Back button to return to the previous page.

Continue block message

If the user clicks the **Continue** button, Websense software permits the site, and the page is displayed until the browser is closed or another site is requested.

Clicking **Continue** starts a timer. During the configured time period (60 seconds by default), the user visits other sites in Continue categories without encountering another block page. Once the time period ends, browsing to any other Continue site results in another Continue block page.

The default time (60 seconds) can be changed via **Server** > **Settings**, under **Common Filtering**.

The Continue option is activated at the category set level (see *Editing a category set*, page 257).

Note

The Continue option can be used in environments where clients (directory objects, workstations, and networks) are governed by a single Policy Server. It should not be activated for users managed by multiple Policy Servers.

Quotas

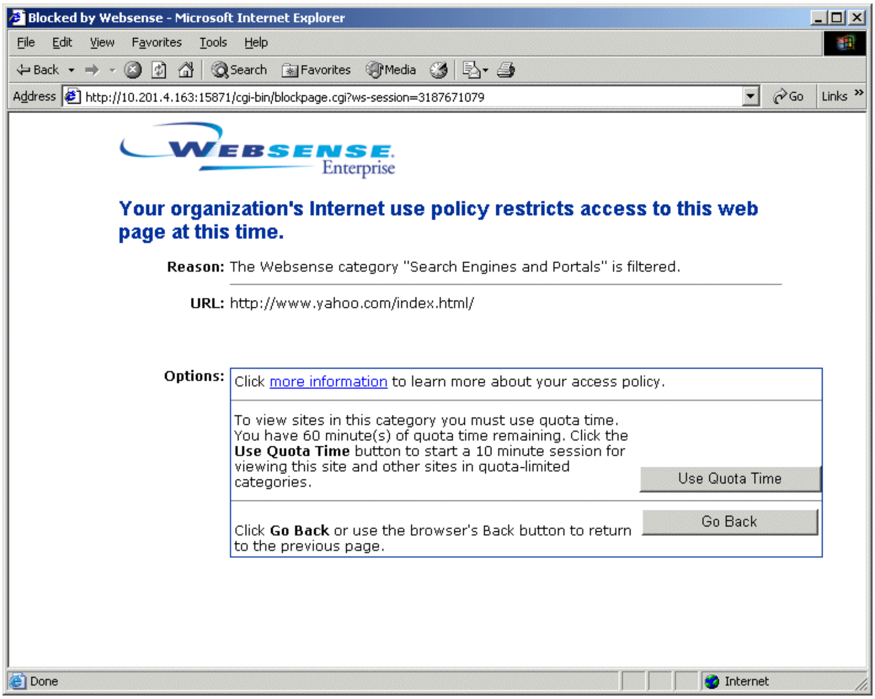
Give employees access to sites in selected categories for a limited amount of time each day. Access is granted in configurable increments of time to sites in categories whose filtering setting is **Limit by Quota**. Quotas give you control over how much time your employees spend on personal surfing and what URL categories they are accessing.

Note

Quotas can be used in environments where clients (directory objects, workstations, and networks) are governed by a single Policy Server. Quota time should not be allocated to users managed by multiple Policy Servers.

If your environment involves multiple Policy Servers, edit the **Default Settings** category set to change the filtering option on applicable categories from **Limit by Quota** to **Block** or **Permit**.

When a user requests a site in a quota-limited category, a block message presents the option to view the site using quota time.



Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=3187671079
Go Links
WEBSENSE Enterprise

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Search Engines and Portals" is filtered.

URL: http://www.yahoo.com/index.html/

Options: Click more information to learn more about your access policy.

To view sites in this category you must use quota time. You have 60 minute(s) of quota time remaining. Click the **Use Quota Time** button to start a 10 minute session for viewing this site and other sites in quota-limited categories.

Click **Go Back** or use the browser's Back button to return to the previous page.

Quota block page

Clicking **Use Quota Time** starts a quota session, during which the user can view sites in any quota category, as well as view permitted sites and sites classified under Miscellaneous/Uncategorized in the Master Database.

After the quota session ends, requesting another site in a quota category results in another quota block message. If quota time remains, the user can start a new quota session. If no time remains, the user can click **Go Back** to return to the previous page.

Quota time is allocated on a daily basis. Once it is used up, clients must wait until the next day to access sites in quota categories. Quota time is independent of policy time restrictions and is granted globally in the **Default Settings** category set (default is 60 minutes). The amount of default quota time can be changed via **Server > Settings** > **Common Filtering**. Quota time can also be granted individually to specific clients (see *Allocating quota time to clients*, page 125).

Once quota time is configured, it activates a priority list for each time a user requests a site in a quota category. Websense software searches for quota time configured for:

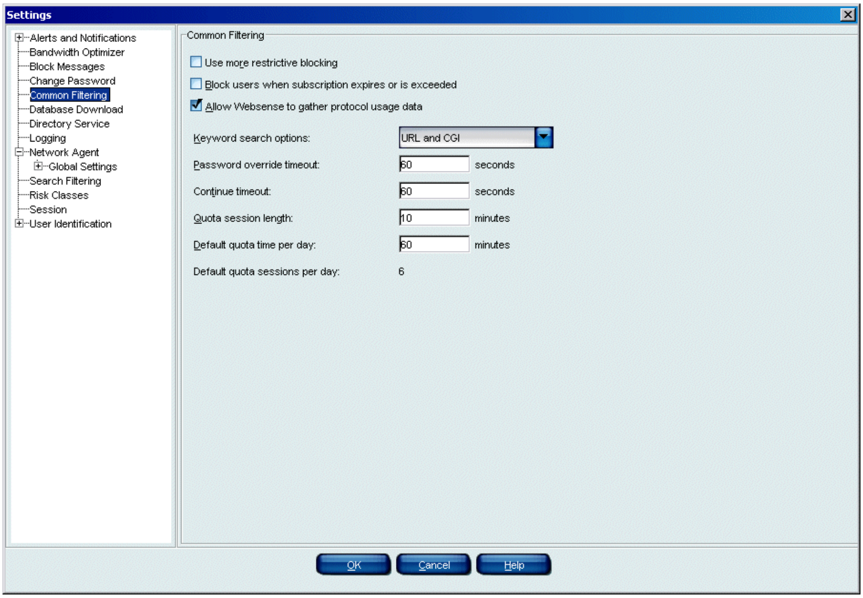
1. The user.
2. The workstation or network (range of IP addresses).
3. Groups of which the user is a member.

   If a user is a member of multiple groups, Websense software grants the quota time according to the **Use more restrictive blocking** setting under **Server > Settings > Common Filtering**.
4. Default quota time.

To take advantage of the quota time feature:

- When adding new category sets or editing existing ones, assign the **Limit by Quota** filtering setting to the appropriate categories (see *Editing a category set*, page 257).
- Add any *new* category sets to policies governing clients who have been granted quota time. To apply pre-existing category sets to additional policies, edit these policies (see *Editing a policy*, page 302).

- Review the quota session length and the default quota time per day via **Server > Settings > Common Filtering**, and then make appropriate changes. Default quota time is applied to all clients equally.



Common Filtering

□ Use more restrictive blocking

□ Block users when subscription expires or is exceeded

☑ Allow Websense to gather protocol usage data

Keyword search options: URL and CGI

Password override timeout: 60 seconds

Continue timeout: 60 seconds

Quota session length: 10 minutes

Default quota time per day: 60 minutes

Default quota sessions per day: 6

Quota time settings

- **Quota session length**: The interval during which users are allowed to view sites in categories whose filtering setting is **Limit by Quota**. A session begins when the user clicks the **Use Quota Time** button. The default is 10 minutes.
- **Default quota time per day**: The amount of quota time each client is allocated each day if no alternative quota time is configured. The default is 60 minutes. If the total quota time remaining is less than the quota session length, the session length is only as long as the time remaining.
- **Default quota sessions per day**: This is a display-only field, calculated as changes are made to the quota session length and default quota time per day values.

- Allocate quota time per day to each client that should be granted more or less time than the default amount (see *Allocating quota time to clients*, page 125).

Quota time and applets

Internet applets, such as Java or Flash applets, may not respond as expected to quota time restrictions you have configured. Even if accessed from a quota-restricted site, any applet that runs within the browser can continue running beyond the configured quota session time.

This is because such applets are downloaded completely to a client machine and run just like applications, without communicating back to the original host server. However, if the user clicks the browser's **Refresh** button, Websense software detects the communication to the host server, and then blocks the request according to applicable quota restrictions.

Password override

Password override lets users with valid passwords access sites blocked by Websense software. Password override can be granted to individual users, groups, workstations, or networks (IP address ranges). For more information, see *Password override*, page 121.

Search Filtering

Search Filtering lets you control how Internet search engine results are displayed in a browser.

Ordinarily, Internet search engine results may include thumbnail images associated with websites matching the search criteria. Websense filters such sites so users cannot view the full-size versions of thumbnail images associated with blocked sites. However, thumbnail images displayed in the search result list may still be inappropriate for viewing.

Websense activates a setting built into search engines so thumbnail images associated with blocked sites are not displayed in search results.

✓ **Note**

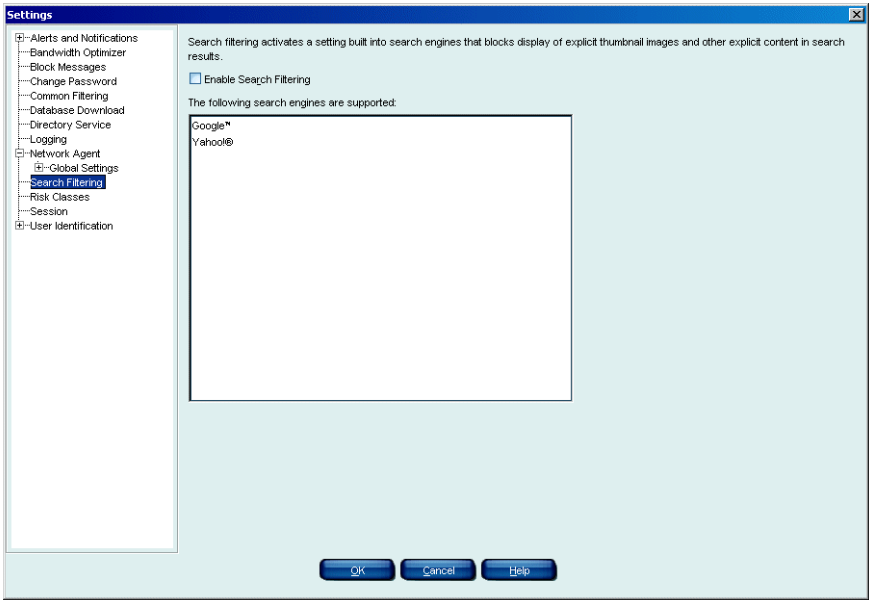
A few thumbnail images may not get blocked as expected, if Network Agent is under a heavy performance load. For Network Agent deployment recommendations, see the *Websense Enterprise Deployment Guide*.

Websense, Inc. maintains a database of search engines for which Search Filtering is supported. When a search engine is added or removed from the database, an alert is generated (if alerting is activated). For more information, see *Alerting*, page 199.

Remote clients are filtered in the same manner as local clients. For more information, see *Remote Filtering*, page 50.

To enable image search filtering:

1. Choose **Server** > **Settings**. The **Settings** dialog box appears.
2. Select **Search Filtering** at the left. The **Search Filtering** settings are displayed.



Search filtering activates a setting built into search engines that blocks display of explicit thumbnail images and other explicit content in search results.

□ Enable Search Filtering

The following search engines are supported:

Google™
Yahoo!®

3. Check **Enable Search Filtering**.
4. Click **OK**.

Remote Filtering

The Remote Filtering feature lets you filter clients outside a network firewall. Implementing Remote Filtering involves:

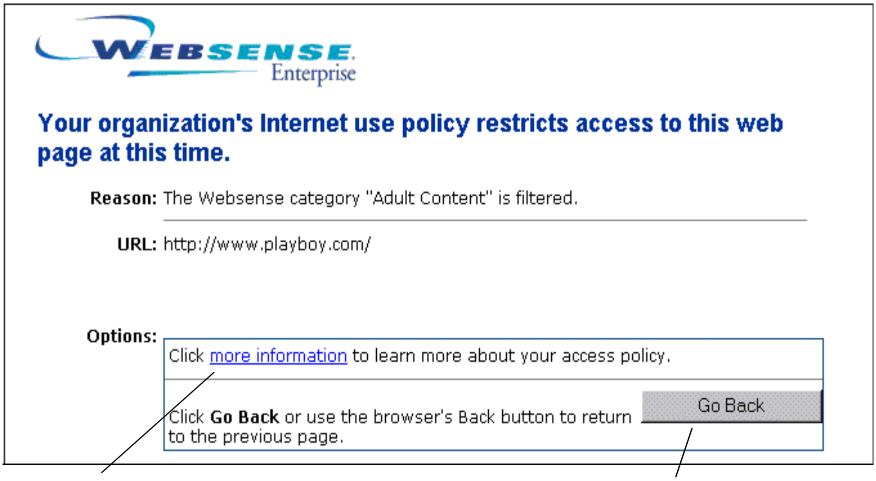
- Installing the Websense Remote Filtering Server and Remote Filtering Client according to the instructions in your installation guide.
- Ensuring that remote users can be successfully identified.

For more information, see *Filtering remote clients*, page 126.

Block messages

When Websense software blocks a website, it displays a block page in the client’s browser. By default, the top frame contains the block message, the requested URL, and the reason it was blocked.

The bottom frame presents any options available to the user. For example, if the user has password override privileges, the bottom frame includes a password field.



Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Adult Content" is filtered.

URL: http://www.playboy.com/

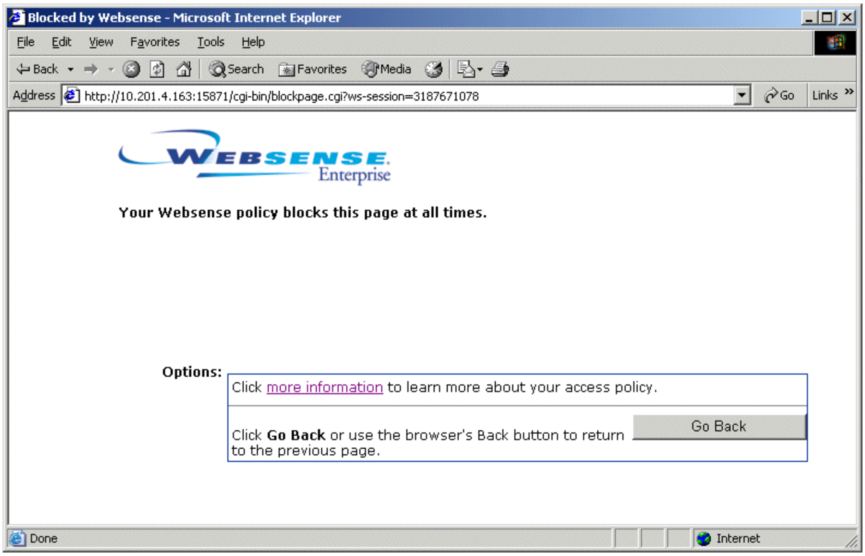
Options: Click more information to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page.

whether and when the site is permitted

return to the previous page

Default block message


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Websense Enterprise
Done
Internet

http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=3187671078

Your Websense policy blocks this page at all times.

Options:

Click more information to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page.

Go Back

more information page

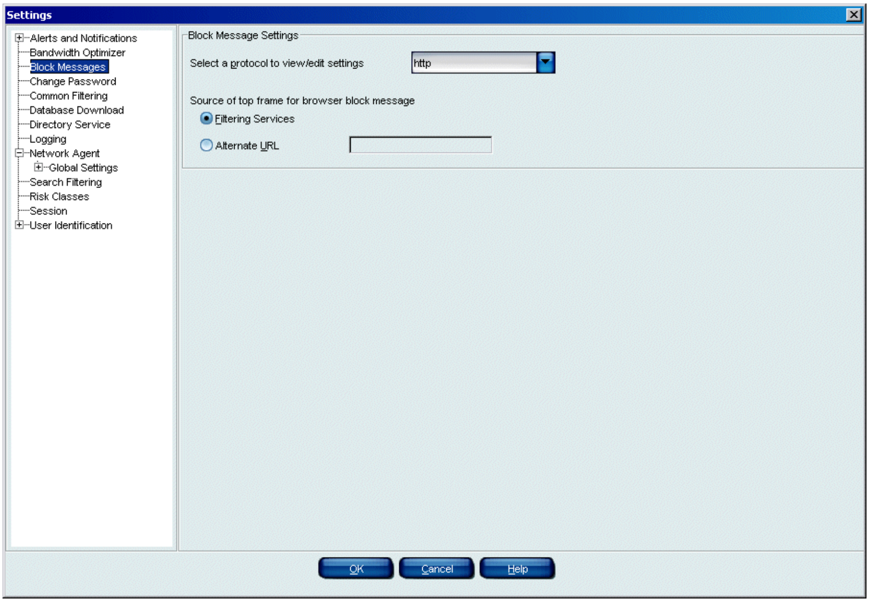
Websense software provides default HTML files for the block pages. You can customize the text of the default Websense messages to better fit your organization’s needs. Additionally, you can use alternate HTML files to completely replace the top frame of all block pages.

If you use the default block messages Websense software provides, no further changes are required. Otherwise, set up the appropriate HTML files, and then configure Websense software to use them. For more information, see *Customizing the default block messages*, page 53.

Customized block messages

Websense software lets you modify portions of the default block messages, using a text editor.

1. Create a new block page by doing one of the following:
   - Customize the default message text (see *Customizing the default block messages*, page 53).
   - Create an alternate HTML file to display (see *Creating an alternate block message*, page 57).
2. In Websense Manager, select **Server** > **Settings**.
3. Select **Block Messages** at the left.



Block Message Settings

Select a protocol to view/edit settings: http

Source of top frame for browser block message

● Filtering Services

○ Alternate URL

Block Message settings

4. Select a protocol for **Select a protocol to view/edit settings**. Your integration product must support the protocol in order for Websense software to use it. In most cases, HTTP is an appropriate protocol.

5. Select a block message setting:

Settings	Description
Filtering Service	Displays the customized default message, if any. Otherwise, Websense software displays the default block message.
Alternate URL	Displays an alternate HTML page as the top portion of the block message. (The bottom frame of the block message displays the customized content or the original default content, which presents password override, quota, and continue options.) Do not use a URL that overwrites frames included with continue or quota options.

6. If you chose **Alternate URL**, enter the path for this custom block message.
7. Click **OK**.

Customizing the default block messages

Websense Setup places these default block message files in the `Websense\BlockPages\en\Default` directory:

- `block.html`: Text for the top frame of the block message. Indicates that access is restricted, the site that was requested and why it is restricted.

> ✓ **Note**
> This message is replaced by a custom message if you enter an alternate URL via **Server** > **Settings** > **Block Messages**.

- `master.html`: Master frame that appears in the continue, quota and password override block messages.

`Master.html` invokes the messages that appear in the bottom frame of block pages:

File Name	Contents
continueFrame.html	Text and buttons for requested sites in categories whose filtering setting is **Continue**.
quotaFrame.html	Text and buttons for requested sites in categories whose filtering setting is **Limit by Quota**.
moreInfo.html	Content for the page that appears when a user clicks the **more information** link on the block page.

Content variables control the information displayed on HTML block pages. The following variables are included with the default block message code.

Variable Name	Content Displayed
ws_date	Current date
ws_username	Current user name (excluding domain name)
ws_userdomain	Domain name for the current user
ws_ipaddr	IP address of the request source machine
ws_workstation	Displays the machine name of the blocked workstation (if no name is available, IP address is displayed)

To use a variable, insert the variable name between the $* *$ symbols in the appropriate HTML tag:

```
<p id=”UserName”>$*ws_username*$</p>
```

where ws_username is the variable.

There are additional variables within the block message code. Websense, Inc., recommends against modifying the variables described in the table below.

These variables are critical to how Filtering Service processes blocked requests, and must remain intact.

Variable Name	Purpose
ws_url	Displays the requested URL
ws_blockreason	Displays why the site was blocked (i.e., which filtering setting is in effect)
ws_pwoverridecgidata	Populates an input field in the block page HTML code with information about use of the **Password Override** button
ws_quota_cgidata	Populates an input field in the block page HTML code with information about use of the **Use Quota Time** button
ws_passwordoverrid_begin, ws_passwordoverrid_end	Plays a role in telling Filtering Service whether to process a request using password override functionality
ws_moreinfo	Displays detailed information (shown after the **more information** link is clicked) about why the requested site was blocked
ws_policyinfo	Indicates which policy governs the requesting client
ws_moreinfocgidata	Sends data to Filtering Service about use of the **more information** link
ws_quotatime	Displays the amount of quota time remaining for the requesting client
ws_quotaintervaltime	Displays quota session length configured for the requesting client
ws_quotabuttonstate	Indicates whether the **Use Quota Time** button is enabled or disabled for a particular request
ws_sessionid	Acts as an internal identifier associated with a request
ws_topframesize	Indicates the size (as a percentage) of the top portion of a block page sent by a custom block server, if one is configured

Variable Name	Purpose
ws_blockmessage_page	Indicates the source to be used for a block page's top frame
ws_category	Displays the category of the blocked URL
ws_categoryid	Associates a unique identifier for the URL category with this request

To customize the default block message:

1. Open the `Websense\BlockPages\en\Default` directory.
2. Copy the file to customize to the `Websense\BlockPages\en\Custom` directory.

   ✓ **Note**

   Do not modify the original block message files in `Websense\BlockPages\en\Default`. Copy them to the `Websense\BlockPages\en\Custom` directory and then modify the copies.

3. Open the file in a text editor.

   ⚠ **Warning**

   Use a plain text editor to edit block message files. Some HTML editors modify HTML code, which could corrupt the files and cause problems displaying the block messages.

4. Modify the text. The files contain comments that guide you in making changes.

   Do not modify the tokens (enclosed by $* and *$ symbols), or the structure of the HTML code. These enable Websense software to display specific information in the block message.

5. Save the file.
6. Restart Filtering Service (see *Stopping or starting Websense services*, page 191 for instructions).

If users experience errors after you implement customized default block messages, you can restore the original default block messages as follows:

1. Delete all the files from the `Websense\BlockPages\en\Custom` directory. Do not delete files from `Websense\BlockPages\en\Default`.
2. Restart Filtering Service (see *Stopping or starting Websense services*, page 191).

Creating an alternate block message

To replace the content of the top frame in the block message, create an appropriate HTML file, or identify one that already exists in your network. Use this approach to display corporate internet use policies, for example.

Alternate block messages are typically stored on an internal web server. If that is not possible, store them on a web server that does not host a site in the Websense Master Database. Otherwise, the alternate block message is blocked whenever Websense software blocks the associated category.

After creating the HTML file and placing it on a suitable web server, configure Websense software to use that file for the appropriate protocols, as described earlier.

Websense software presets the size of the top frame to meet its default block page size requirements. However, your custom message may be of a different size. To change the size parameter of the top frame in the `master.html` file:

1. Copy the `master.html` file from `Websense\BlockPages\en\Default` directory to `Websense\BlockPages\en\Custom`.
2. Open the `master.html` file using a text editor, such as Notepad or vi (not an HTML editor), and edit the parameter

   ```
   <frameset rows=230,* frameborder=0 border=0>
   ```

   where 230 pixels is the default Websense top frame size, and ***** is the remaining number of pixels in the vertical direction. Change only the default value (230) to an appropriate number, leaving the * as is.

Filtering and the Websense Master Database

The Master Database houses the category and protocol definitions that provide the basis for filtering internet content. The database is continually updated.

Database downloads

Download the Master Database by:

- Entering your subscription key during installation, and downloading the database at that time.
- Entering your subscription key via **Server > Settings > Database Download** in Websense Manager. Filtering Service contacts the database server and downloads the Master Database.

After initial download, Websense software downloads changes to the Master Database according to the schedule you establish (see page 60). To download at any other time, select **Server** > **Database Download** in Websense Manager.

If your network involves a proxy server or firewall other than a Websense integration product, you must configure database download to occur via proxy (see *Removing a server*, page 193).

Download status

If your network includes multiple Filtering Services, the Master Database downloads to all Filtering Services (and consequently to Policy Server and Websense Manager) at the same time. However, during download, all message boxes that appear pertain only to the first Filtering Service contacted.

To check download status for subsequent Filtering Services, see the appropriate log:

- *Windows NT:* Check the Windows Application Event log for any listings about the database download, or other error and status messages. To access the Application Event log, select **Start** > **Programs** > **Administrative Tools** > **Event Viewer**. From the **Log** menu, select **Application**.

- *Windows 200x:* Check the Windows Application Event log for any listings about the database download, or other error or status messages. To access the Application Event log, select **Start > Programs > Administrative Tools > Event Viewer**. Click **Application Log** (Windows 2000) or **Application** (Windows 2003).
- *Solaris or Linux:* Websense software creates `Websense.log` in the `Websense/` directory when there are errors to record. This log records error messages and messages pertaining to database download.

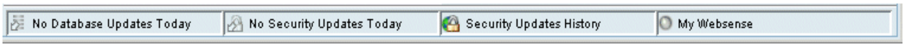
You can be notified whenever a Websense Master Database download fails. For more information, see *Alerting*, page 199.

Real-Time Database Updates

In addition to scheduled downloads, Websense software performs emergency updates to the database as needed. These updates could include recategorizing a site that has been temporarily mis-categorized. This ensures that sites and protocols are filtered appropriately. Websense software checks for database updates every hour.

To view recent database updates, select **Server > Real-Time Updates**.

The status bar at the bottom of the Websense Manager window indicates when the Master Database is updated or when new information is available.



Status bar

Clicking the **MyWebsense** link opens the MyWebsense web page (www.mywebsense.com).

Clicking the Security Updates History link opens the Real-Time Security Updates page on the Websense Security Labs website. This page displays a list of Real-Time Security updates that Websense has issued, starting with the most recent update. If you have a subscription to Real-Time Security Updates, these updates are sent to your database as they are issued. See *Websense Real-Time Security Updates™*, page 71.

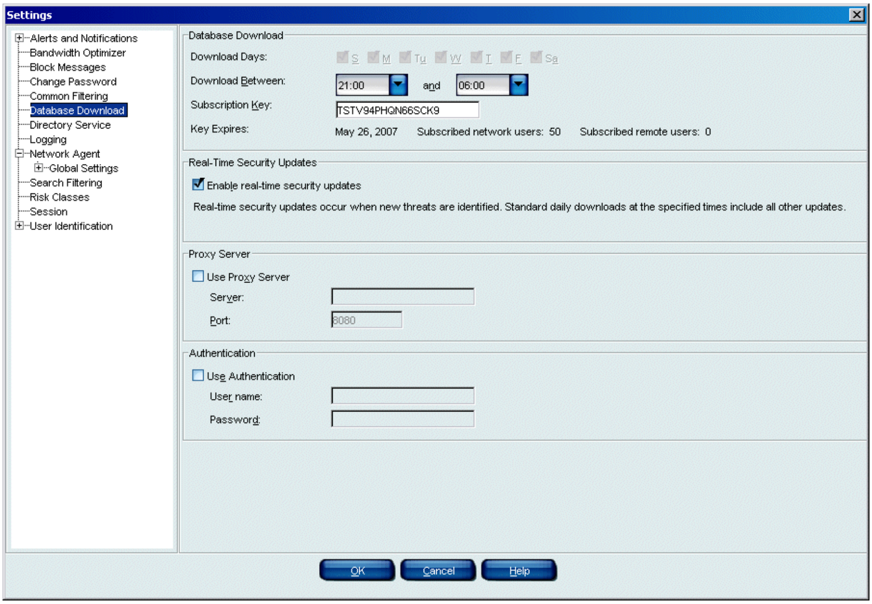
Setting the download schedule

Websense software downloads changes to the Master Database according to the schedule defined in Websense Manager. By default, download is scheduled to occur once a day. Since each subsequent download only transfers changes to the Master Database, downloading daily utilizes the minimum amount of time and bandwidth.

> ✓ **Note**
>
> You must download the Master Database at least every 14 days for Websense software to continue filtering uninterrupted. If no download days are selected, download occurs once a week.

To change the schedule:

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Database Download** at the left. The download settings are displayed.



Database Download

Download Days: ☑ S ☑ M ☑ Tu ☑ W ☑ T ☑ F ☑ Sa

Download Between: 21:00 and 06:00

Subscription Key: TSTV94PHQN66SCK9

Key Expires: May 26, 2007 Subscribed network users: 50 Subscribed remote users: 0

Real-Time Security Updates

☑ Enable real-time security updates

Real-time security updates occur when new threats are identified. Standard daily downloads at the specified times include all other updates.

Proxy Server

□ Use Proxy Server

Server:

Port: 8080

Authentication

□ Use Authentication

User name:

Password:

3. Configure download behavior as desired.

Note

If **Enable real-time security updates** is checked, the default download schedule is used.

Available settings are:

Setting	Purpose
Download days	Days of the week to update your copy of the Master Database. Downloading daily ensures the fastest download time and most up-to-date content.
Download between	Time period for database download. Filtering Service selects a random time during this period to contact the Master Database server. To configure alerts for download failure, see *Alerting*, page 199.
Subscription key	Time period for database download. Filtering Service contacts the Master Database server during this period. To configure alerts for download failure, see *Alerting*, page 199.
Key expires, Subscribed network users, Subscribed remote users	Display-only calculations based on your subscription key. For more information about subscriptions, see *Ensuring subscription compliance*, page 35.

The Master Database is configured to download according to your chosen schedule.

Note

After downloading the Master Database or updates to the Master Database, CPU usage can be 90% or more for 1-3 minutes while the database is loaded into local memory.

Resumable downloads

If download of the Master Database is interrupted, you can resume the process without waiting for the next scheduled download. Download resumes as follows:

- If a download is in progress, click **Cancel All** and then **Download All** to start the download again from the beginning.
- If you schedule or manually start a download and the download is interrupted, Filtering Service attempts to reconnect to the database download server and resumes the download from where it was interrupted.
- If a download fails and the next download is scheduled outside the time frame of the failed download, Filtering Service contacts the database download server to attempt download again.

✓ **Note**

Click **Download All** at any time to resume a database download.

Configuring download via proxy

If Websense software must go through another proxy server or proxying firewall to access the internet and download the Master Database (other than the integration product that Websense software communicates with), you must configure Websense software to use the proxy for database download operations.

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Database Download** at the left. The database settings are displayed.
3. Check **Use proxy server**.
4. For **Server**, enter the IP address or name (*Windows only*) of the machine running the proxy server or firewall through which the database download must pass.
5. For **Port**, enter the port of the proxy server or firewall through which the database download must pass (default is 8080).

6. If your network requires authentication to a firewall or proxy server upstream from your integration product to reach the internet, check **Use authentication**.

   Note

   If **Use authentication** is checked, the upstream proxy server or firewall must be configured to accept clear text or basic authentication in order for Websense software to download the Master Database.

7. Enter the password required by the proxy server or firewall to download the Master Database.

   Note

   By default, Websense software encodes the user name and password based on the character set of the Policy Server machine's locale. To use a character set other than this default, contact Websense Technical Support for assistance.

8. Click **OK**.

Categories and protocols in the Master Database

The Websense Master Database houses the groupings for both URLs and various protocols. URL categories are the basis for internet site filtering, while protocol groups provide internet content filtering by protocol type.

Websense, Inc. does not make value judgments on the categories or sites in the Websense Master Database. Categories have been selected based on feedback from the business and education community about what is unacceptable or inappropriate with regard to employee productivity, student safety or threat of legal action. You choose which categories to block and which to permit.

Categories are broken down to enhance control of internet access levels. In case of uncertainty, a collaborative decision is made as to whether a site is included, and in what category. The Master database is checked regularly for accuracy and quality.

The categories used by Websense, Inc. are designed to create useful groupings of the sites of concern to subscribing customers. They are not intended to characterize any site or group of sites or the persons or interests who publish them, and they should not be construed as such. Likewise, the labels attached to Websense categories are convenient shorthand and are not intended to convey, nor should they be construed as conveying, any opinion or attitude, approving or otherwise, toward the subject matter or the sites so classified.

The up-to-date list of categories is available at:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

In addition to the standard categories provided in the Websense Master Database, you can implement more advanced URL filtering using Premium Group categories. For information about the Websense Enterprise Premium Groups, go to:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php#bandwidth

There is an additional cost for Premium Groups. When purchased, they are delivered through the existing database download process.

To suggest that a site be added to the Master Database, contact Websense, Inc. at:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php

Websense, Inc. groups together similar types of internet protocols and applications to manage internet traffic.

Protocol definitions are verified and updated as frequently as nightly. The up-to-date protocol list is available from this web page:

www.websense.com/global/en/ProductsServices/MasterDatabase.

New categories and protocols

New categories and protocols added to the Websense Master Database are assigned an initial filtering setting (i.e., **Permit** or **Block**). Like the categorizations themselves, these filtering settings are based on feedback regarding appropriateness of the sites or protocols in question. You can change filtering settings for categories or protocols by editing any category set or protocol set.

You can also configure Websense software to generate alerts whenever new categories or protocols are added to the database. For more information, see *Alerting*, page 199.

Special Events

The Websense Master Database contains a Special Events category, created especially to control employee access to sites covering hot topics. Sites in this category are added to the Master Database during scheduled download times. They are kept in Special Events for only a short amount of time, after which they are either deleted from the Master Database or are taken out of the Special Events category and placed in another category.

Websense Security Protocol Groups

If you have *Websense Web Security Suite*, you receive the Security Protocol Groups. These additional Websense protocols offer a built-in layer of protection against spyware and malicious software or content that is transmitted over the internet.

Security Protocol Groups are displayed in Websense Manager. Most of the protocols in these groups are available for filtering, and are blocked by default. A few protocols are monitored and logged only.

For more information, go to:

www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

Premium Groups

Websense Enterprise Premium Groups are Master Database categories with associated subcategories that enhance your ability to manage and report on internet use. The Premium Groups are:

- **Websense Enterprise Productivity PG**™ (also known as **Productivity Categories**): Focuses on preventing cyberslacking
- **Websense Enterprise Bandwidth PG**™ (also known as **Bandwidth Categories**): Focuses on saving bandwidth
- **Websense Security Filtering** (also known as **Websense Security PG**™): Focuses on internet sites containing malicious code, which can bypass virus-detection software programs

✓ **Note**

Websense Security Filtering is included with Websense Web Security Suite.

For information on how Premium Groups can benefit your network, see:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

There is an additional cost for Premium Groups. When purchased, they are delivered via the database download process. Until purchased, Premium Group categories are permitted and logged. They are marked as **[monitor only]** in category lists. You cannot filter internet activity in these categories until Premium Groups are purchased.

Once purchased, the following Premium Group categories are blocked by default:

- **Productivity PG**:
    - Advertisements
    - Freeware and Software Download
    - Instant Messaging
    - Online Brokerage and Trading
    - Pay-to-Surf
- **Bandwidth PG**:
    - Internet Radio and TV
    - Internet Telephony
    - Peer-to-Peer File Sharing
    - Personal Network Storage and Backup
    - Streaming Media
- **Security PG**:
    - Bot Networks
    - Keyloggers
    - Malicious Web Sites
    - Phishing and Other Frauds
    - Potentially Unwanted Software
    - Spyware

To purchase these categories, see your Websense reseller or visit:

www.websense.com/global/en/partners/Channel/FindPartner/

Matching sites in the Master Database

As part of the filtering process, the Websense Filtering Service compares the full address of each requested site to the list of addresses in the Master Database. Filtering Service can match a site address whether it is requested as a text-based URL or a numeric IP address. Filtering Service also recognizes sites that are virtually hosted, as well as those requested by CGI (Common Gateway Interface).

URL matching

Filtering Service analyzes the full URL entered by the user, including the protocol, domain and path to a specific page within the site.

www.websense.com/products/index.cfm

Protocol   DomainPath

This complete analysis prevents Websense software from filtering sites incorrectly when a web server hosts pages that fall into multiple categories.

These URLs share the same domain but fall into different categories:

www.cnn.com/WORLD (News and Media)
www.cnn.com/SHOWBIZ (Entertainment)

If you set Websense software to block only sites in the News and Media category, it blocks the first URL but not the second, even though they share the same domain name.

URL pattern matching

Websense software supports the use of regular expressions (or URL patterns) in matching URLs. When setting up custom URLs, yes lists or keywords, you can use pattern strings in place of absolute character strings. This lets you specify general patterns for Filtering Service to match, as opposed to specific URLs or strings.

For information about creating custom URLs, yes lists or keywords, see *Chapter 9: Setting Up Web Filtering*.

✓ **Note**

Using regular expressions as filtering criteria may increase CPU usage. Tests have shown that with 100 regular expressions, the average CPU usage on the machine running the Websense Filtering Service increased by 20%.

Websense software supports the common sets of Perl, Javascript and Posix regular expression libraries for URL pattern matching.

For further help with regular expressions, see:

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

www.regexbuddy.com

IP address matching

An IP address is the unique numerical identifier for a particular machine. For example, the following IP address and URL request the same website:

63.212.171.196
www.websense.com

When comparing sites to the Master Database, Websense software uses exclusive technology to recognize sites requested with text-based URLs or with the numerical IP addresses of the servers hosting the sites. This ensures accurate filtering regardless of how a site is requested.

IP addresses assigned to domain names are subject to change. This can occur if the host server for the site represented by the domain name changes (as the new server has a different IP address), or if the original server is reassigned a new IP address.

Virtual host recognition

Web servers configured to host more than 1 website or unique domain are called virtual hosts. Although most virtual hosts resolve all websites and domains to the same IP address, some virtual hosts assign separate IP addresses to each website and domain they host. For example, a web server may host a shopping site, a religion site, and an adult material site, and resolve all 3 sites to the same IP address. Websense software identifies individual virtually hosted sites to ensure that they are properly categorized.

CGI requests

CGI (Common Gateway Interface) scripts are common in interactive websites. When a user enters a search engine request or clicks on an image map, the CGI script generates a new URL request.

This example shows a URL generated by a search engine when the term "Websense" was entered as the search request.

CGI request: http://search.yahoo.com/bin/search?p=Websense

CGI-generated site requests contain a question mark in the URL indicating to the web server where the search parameters begin. Following the question mark is the search query making the results unique. This query typically includes the text of the user's search request, the URL of a linked site, or a combination of templates, names and values.

Because the result of each search engine request may be unique, Websense software disregards the "?" and everything beyond it when comparing a CGI-requested site to the Master Database. When filtering the example given, Websense software matches the requested URL to the Master Database listing even though the requested site has a CGI string ("?p=Websense") appended to it.

CGI request: http://search.yahoo.com/bin/search?p=Websense
Master Database match: http://search.yahoo.com/bin/search

For tighter filtering of sites requested via CGI, block keywords in CGI strings appended to URLs (see *Keywords*, page 268).

Adding your own sites

Since the list of accessible internet sites changes daily, Websense, Inc. cannot guarantee that all sites for a given category have been identified in the Master Database. You can filter sites not in the database by defining them as custom URLs (see *Custom URLs*, page 259). Websense software then filters these according to the filtering settings you specify.

You also can suggest that the site be added to the Master Database. Suggestions can be made at the Websense website:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php

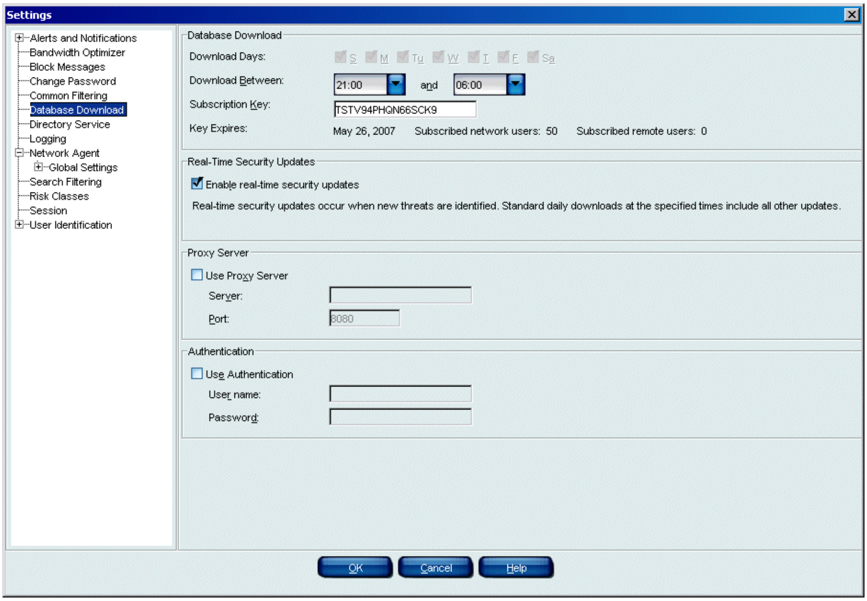
Or, email suggestions to: **suggest@websense.com**.

Websense Real-Time Security Updates™

The Websense Real-time Security Updates feature is the capability to get database security updates as soon as they are published by Websense, Inc. This feature is purchased separately, and is activated via your subscription key.

Real-time security updates provide a layer of protection against security threats that can enter your network over the internet. Installing security updates as soon as they are created eliminates vulnerability to threats such as new phishing (identity fraud) scams, rogue applications, or malicious code infecting a mainstream website or application. These affect the Websense Enterprise Security PG (see *Premium Groups*, page 66) and Websense Enterprise Client Policy Manager (see the Client Policy Manager documentation).

The Websense Filtering Service queries the database download server every 5 minutes for security updates. Updates include changes to the database only when security threats occur. Typically, actual changes are occasional, and do not disrupt normal network activity. Meanwhile, standard database downloads must occur at least every 14 days. Otherwise, you configure how often standard downloads occur.



Database Download

Download Days: ☑ S ☑ M ☑ Tu ☑ W ☑ T ☑ F ☑ Sa

Download Between: 21:00 and 06:00

Subscription Key: TSTV94PHQN66SCK9

Key Expires: May 26, 2007 Subscribed network users: 50 Subscribed remote users: 0

Real-Time Security Updates

☑ Enable real-time security updates

Real-time security updates occur when new threats are identified. Standard daily downloads at the specified times include all other updates.

Proxy Server

☐ Use Proxy Server

Server:

Port: 8080

Authentication

☐ Use Authentication

User name:

Password:

Real-Time Security Updates activated

When Real-time Security Updates are active, Websense software downloads security updates in a real-time manner. By default, Websense Manager is configured to perform standard database downloads every day of the week. All download days are checked by default. However, you can customize the time frame for standard database downloads.

If you do not want standard database downloads to occur every day, disable the real-time security update feature. Once you uncheck **Enable real-time security updates**, you can modify the standard download schedule.

Standard downloads include all other updates to the Master Database. You can still download the database at any time via the **Server** > **Database Download** command in Websense Manager.

Websense Web Protection Services

The Websense Web Protection Services include ThreatWatcher, SiteWatcher™ and BrandWatcher™. These services help protect websites, brands, and web servers. All three are included with Websense® Web Security Suite™. SiteWatcher is available together with the Websense Enterprise Security PG (see *Premium Groups*, page 66).

ThreatWatcher, the newest addition, provides a “hacker's-eye” view of your web server, regularly scanning for vulnerabilities and threats, and reporting on risk levels and recommended actions through a web-based portal.

Benefits:

- Helps prevent malicious attacks to web servers and websites before they happen
- Lets you monitor and report on web server activity
- Alerts you to known vulnerabilities, open ports, or policy compliance issues

SiteWatcher alerts you when your website has been infected with mobile malicious code (MMC), letting you take immediate measures to prevent its spread to website visitors.

BrandWatcher alerts you when your website or brand has been targeted in phishing or malicious keylogging attacks. BrandWatcher provides security intelligence, including attack details and other security-related information, letting you proactively notify customers of threats.

Activating Websense Web Protection Services

1. Go to www.mywebsense.com, log on, and enter your Web Security Suite subscription key.
2. On the MyWebsense main page, go to the **Websense Security Labs** box. This box displays the security services—ThreatWatcher, SiteWatcher, BrandWatcher, and Security Alerts—included with Web Security Suite.
3. Click **Sign Up** beside each of the services in turn, and follow the on-screen instructions.

Logging and Reporting

The Websense Log Server is installed with the Websense Reporting Tools. With Log Server running, Websense software can save detailed log entries for filtered internet requests. Use the Websense Reporting Tools to analyze the log entries and create reports of internet activity.

Note

Websense software sends log information that can only be read by the corresponding version of Websense Reporting Tools. Install or upgrade Reporting as appropriate to generate reports. For more information, see the Reporting documentation.

Log entries contain:

- Date and time a site was requested
- Category/yes list or keyword, and protocol, under which it was filtered
- User or workstation requesting the site
- Full URL and IP address of the requested site
- How the requested site was filtered
- Number of bytes contained in the requested site (called bytes transferred)

Note

Websense software logs bytes transferred only if Network Agent or an integrated proxy or cache machine is in use.

Although Log Server must be installed in the same network as other Websense components, running it on a separate machine optimizes performance.

Note

No logging can occur until Log Server is installed and logging settings are specified via **Server** > **Settings** > **Logging**.

Selective logging

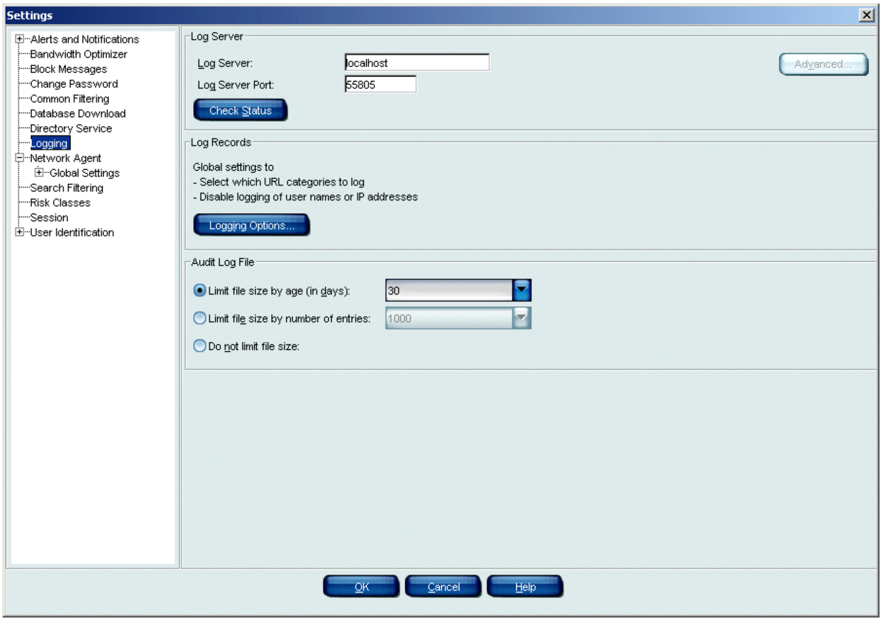
Websense software lets you limit which URL categories are logged. Use selective logging to report only on requests in certain URL categories. For example, to report only on usage in the Sports and Adult Material categories, configure logging to exclude all categories except for those. For more information, see *Configuring logging*, page 75.

Your selective logging settings apply to all category sets in all active policies. Categories excluded from reports are always excluded.

Limiting which categories are logged also reduces the size of the Websense Log Database, which can grow large over time. For information on the Log Database and its role in reporting, see the Reporting documentation. For disk space recommendations, see the *Websense Enterprise Deployment Guide*.

Configuring logging

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Logging** at the left. The **Logging** settings are displayed.
3. Specify Log Server settings.



Log Server

Log Server: localhost

Log Server Port: 55805

Log Records

Global settings to
- Select which URL categories to log
- Disable logging of user names or IP addresses

Audit Log File

● Limit file size by age (in days): 30

○ Limit file size by number of entries: 1000

○ Do not limit file size:

- **Log Server**: Enter the name or IP address of the machine on which Log Server is installed. You must enter a machine name or IP address. If the **Log Server** field is blank, logging is disabled.

✓ **Note**

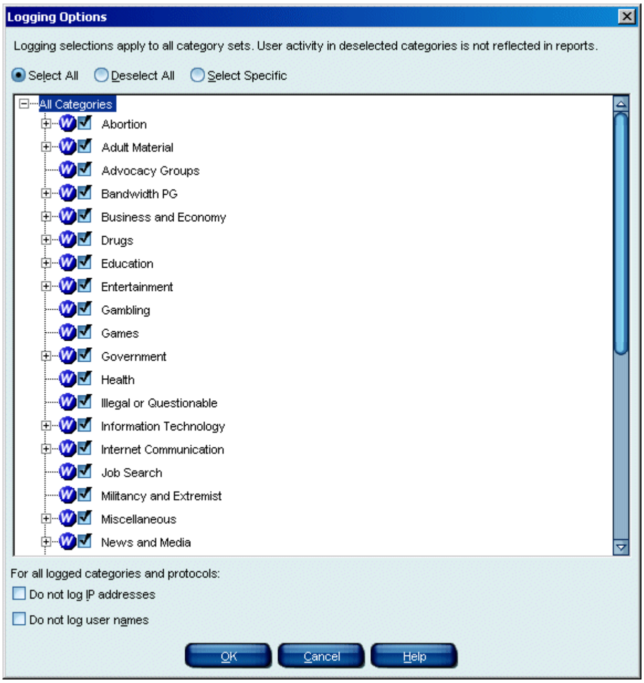
Machine names containing extended ASCII characters may not resolve properly. If you are using a non-English version of Websense, enter an IP address instead of a machine name.

To determine the IP address:

- ***Windows NT/2000:*** On the machine where Log Server is installed, select **Start** > **Programs** > **Accessories** > **Command Prompt**. Type `ipconfig` and then press **Enter.** The IP address is displayed.
- ***Solaris or Linux****:* Go to the command line, and type the command `ifconfig -a`.

- **Log Server Port**: Enter the port Websense software uses to communicate with Log Server. The default port is 55805.
- **Check Status**: Shows whether the Websense Filtering Service can successfully connect to the IP address and port specified for Log Server.

4. Click **Logging Options**. The Logging Options dialog box appears.



Logging selections apply to all category sets. User activity in deselected categories is not reflected in reports.

● Select All ○ Deselect All ○ Select Specific

All Categories
- ☑ Abortion
- ☑ Adult Material
- ☑ Advocacy Groups
- ☑ Bandwidth PG
- ☑ Business and Economy
- ☑ Drugs
- ☑ Education
- ☑ Entertainment
- ☑ Gambling
- ☑ Games
- ☑ Government
- ☑ Health
- ☑ Illegal or Questionable
- ☑ Information Technology
- ☑ Internet Communication
- ☑ Job Search
- ☑ Militancy and Extremist
- ☑ Miscellaneous
- ☑ News and Media

For all logged categories and protocols:

□ Do not log IP addresses

□ Do not log user names

5. Select which categories to log. Only requests for sites in selected categories are included in reports.

   This provides flexibility in reporting. Change selections to broaden or narrow report output. For example, select only **Adult Material** and **Sports** to report only on usage in those categories.

Important

Disabling logging for a category also disables any usage alerts configured for that category. For more information, see *Alerting*, page 199.

6. Specify anonymity options for reports.
   - **Do not log user names**: Omits user names from report output, and preserves anonymity in internet usage reporting.
   - **Do not log IP addresses**: Omits IP addresses from report output.
7. Click **OK**.

Risk classes

URL categories in the Websense Master Database are classified into groups known as risk classes. Risk classes identify URL categories according to areas of risk to your network. Risk classes help you measure internet usage by risk area.

Risk classes include:

- **Network Bandwidth Loss**
- **Legal Liability**
- **Security Risk**
- **Productivity loss**
- **Business Usage**
- **Miscellaneous**

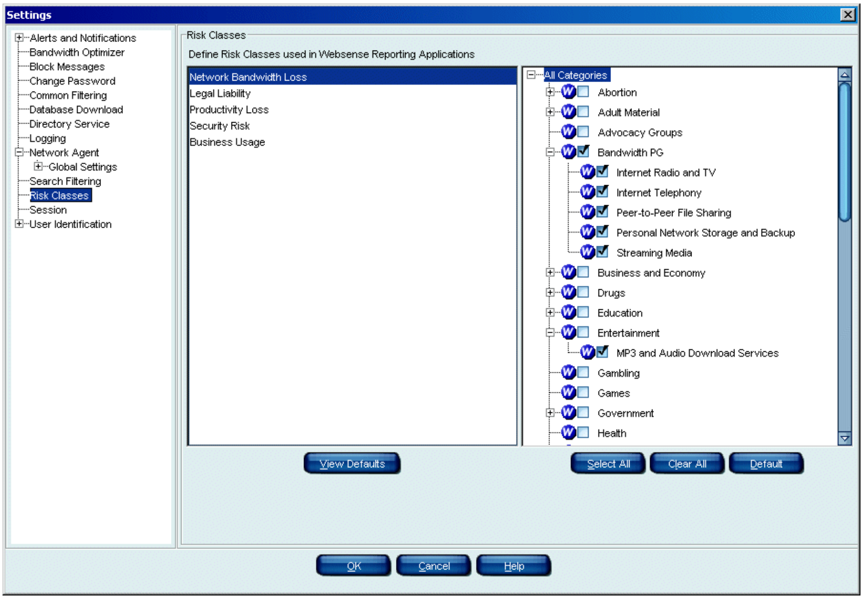
For examples of internet usage reporting based on risk class, see the Reporting documentation.

Websense software provides risk class definitions for your convenience. However, you can customize report output by modifying risk classes.

To modify the predefined risk classes:

1. Select **Server > Settings**. The Settings dialog box appears.

2. Select **Risk Classes** at the left. The risk class settings are displayed.



Risk Classes

Define Risk Classes used in Websense Reporting Applications

- Network Bandwidth Loss
- Legal Liability
- Productivity Loss
- Security Risk
- Business Usage

All Categories
- ☐ Abortion
- ☐ Adult Material
- ☐ Advocacy Groups
- ☑ Bandwidth PG
  - ☑ Internet Radio and TV
  - ☑ Internet Telephony
  - ☑ Peer-to-Peer File Sharing
  - ☑ Personal Network Storage and Backup
  - ☑ Streaming Media
- ☐ Business and Economy
- ☐ Drugs
- ☐ Education
- ☐ Entertainment
  - ☑ MP3 and Audio Download Services
- ☐ Gambling
- ☐ Games
- ☐ Government
- ☐ Health

3. Select a risk class to add or remove URL categories from its definition. Use the buttons to add or remove categories.

   - **Select All**: Selects all categories for the chosen risk class.
   - **Clear All**: Deselects all categories for the chosen risk class.
   - **Reset to Defaults**: Resets category choices to those provided by the Websense software.

4. Click **OK**.

CHAPTER 4 Network Agent

Network Agent enables several Websense functions. In most cases, Network Agent operates behind-the-scenes to provide a complete internet filtering solution, according to configuration settings in Websense Manager.

Network Agent is involved in:

- Internet content filtering
- Protocol and internet application management
- Bandwidth management
- Logging of bytes transferred

For more information, see *Filtering internet content*, page 94.

Network Agent continually monitors overall network usage, including bytes transferred over the network. The Agent sends usage summaries to Websense software at predefined intervals. Each summary includes start time and end time, overall bytes used, and bytes used per protocol.

By default, Network Agent also provides bandwidth usage data to Policy Server, and filtering log data to Filtering Service.

Network Agent sees all traffic in your network. The Agent distinguishes:

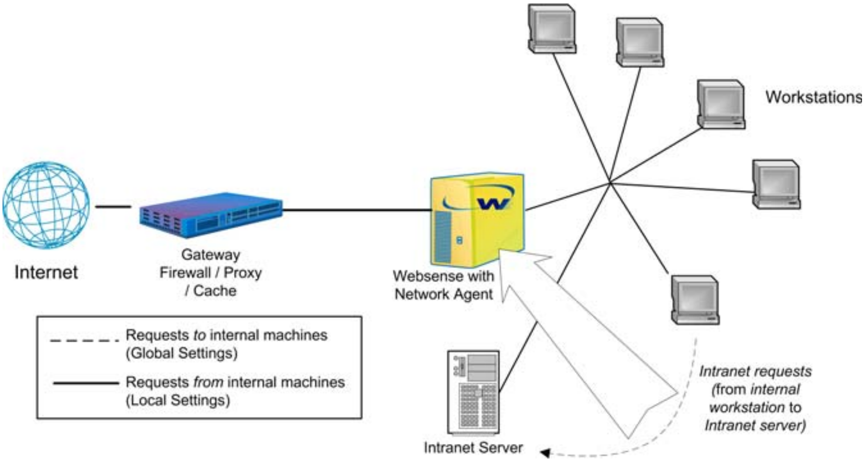
- Requests sent from internal machines to internal machines (hits to an intranet server, for example)
- Requests sent from internal machines to external machines such as web servers (user internet requests, for example)

The latter is the primary concern in monitoring employee internet usage.

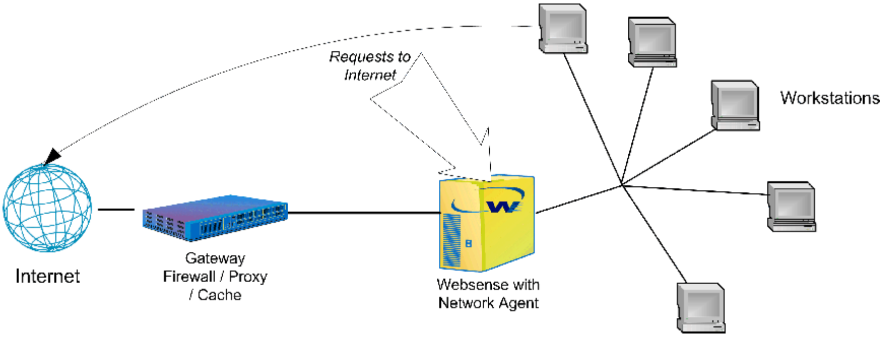
✓ **Note**

For a quick-start guide, go to www.websense.com/global/en/SupportAndKB/ProductDocumentation/, and go to the *Getting Started* section.

All Network Agent instances monitor traffic *to* internal machines according to a unified configuration. Monitoring traffic *from* internal machines is a local function that can be customized for each Network Agent, or even each NIC on a Network Agent machine. This configuration tells Network Agent which machines to watch as request sources or destinations.



Monitoring requests to internal machines



Monitoring requests from internal machines

Configure global and local settings for Network Agent via Websense Manager (see page 83).

Installation

Network Agent is included in a typical Websense installation. Network Agent is configurable via the Websense Manager interface.

For system requirements and installation instructions, see the installation guide. For more detailed installation scenarios, see the *Websense Enterprise Deployment Guide*:

> www.websense.com/global/en/SupportAndKB ProductDocumentation/?Section=All

Initial configuration

After you have installed Network Agent, you must configure its network monitoring behavior. This includes the network segments where Network Agent should monitor traffic, which network interface card (NIC) it uses, and how it handles HTTP and protocol traffic.

NICs on the Network Agent machine

One or more instances of Network Agent can monitor traffic. Each Network Agent instance must use at least 1 designated network interface card (NIC). You can also have Network Agent on a machine with multiple NICs.

For information on placement of Network Agent and requirements for the NICs it uses, see Chapter 2 of the *Websense Enterprise Deployment Guide.*

If you add a new NIC on the Network Agent machine, restart the Network Agent service, and then configure the new NIC (see *Network Interface Card (NIC) settings*, page 91).

> ✓ **Note**
>
> To determine whether the NIC used by Network Agent can see traffic in a network segment, use the Traffic Visibility Tool provided. Select **Start > Programs** > **Websense** > **Utilities > Traffic Visibility Tool**. For more information, see the *Initial Setup* chapter of the installation guide.

Configuring the Agent

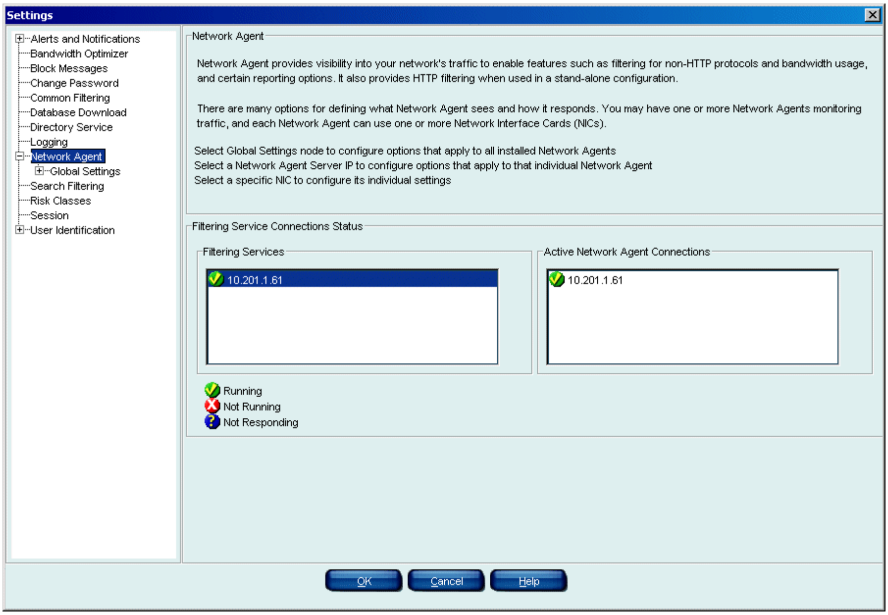
Specify global settings (for all Network Agents installed), and local settings for each particular Network Agent. After initial configuration, you can go back and change settings at any time.

Filtering Service Connections Status shows which Network Agent communicates with each instance of Filtering Service in your network. For each Filtering Service, at least 1 instance of Network Agent is connected.

Modify Filtering Service connections via the Network Agent local settings (see *Local Settings*, page 89).

✓ **Note**

Typically, Network Agent is installed on the Filtering Service machine, so the IP addresses shown for Filtering Service and the related Agent are the same.



Network Agent

Network Agent provides visibility into your network's traffic to enable features such as filtering for non-HTTP protocols and bandwidth usage, and certain reporting options. It also provides HTTP filtering when used in a stand-alone configuration.

There are many options for defining what Network Agent sees and how it responds. You may have one or more Network Agents monitoring traffic, and each Network Agent can use one or more Network Interface Cards (NICs).

Select Global Settings node to configure options that apply to all installed Network Agents
Select a Network Agent Server IP to configure options that apply to that individual Network Agent
Select a specific NIC to configure its individual settings

Filtering Service Connections Status

Filtering Services: ✓ 10.201.1.61

Active Network Agent Connections: ✓ 10.201.1.61

✓ Running
✗ Not Running
? Not Responding

Main Network Agent settings panel

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Network Agent** at the left. The Network Agent main settings panel is displayed.
3. Define network activity, following the guidelines given.
4. When finished with configuration, click **Save Changes** above the navigation tree.

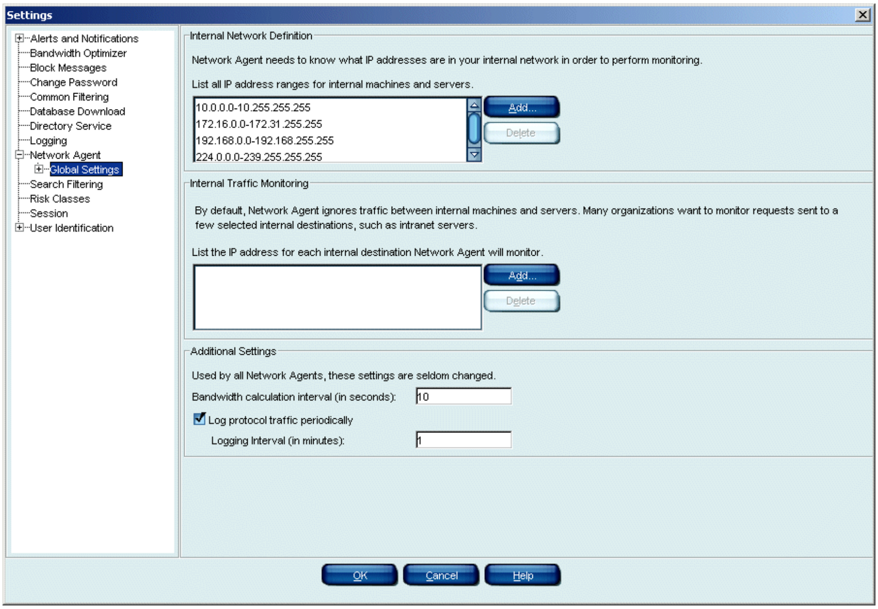
Note

If at any time you change the IP address of a machine running Network Agent or any Websense component, be sure to follow the guidelines in *Changing an IP address*, page 195 to ensure uninterrupted filtering.

Global Settings

Global Settings determine the functions performed by all installed Network Agents. If your network includes multiple Network Agents, these settings apply to all instances.

> **Note**
>
> To monitor/filter file attachments exchanged internally via peer-to-peer messaging, tell Network Agent to monitor the internal machines involved. For more information, see *Instant Messaging Attachment Manager*, page 282.



Internal Network Definition

Network Agent needs to know what IP addresses are in your internal network in order to perform monitoring.

List all IP address ranges for internal machines and servers.

10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0-192.168.255.255
224.0.0.0-239.255.255.255

Internal Traffic Monitoring

By default, Network Agent ignores traffic between internal machines and servers. Many organizations want to monitor requests sent to a few selected internal destinations, such as intranet servers.

List the IP address for each internal destination Network Agent will monitor.

Additional Settings

Used by all Network Agents, these settings are seldom changed.

Bandwidth calculation interval (in seconds): 10

☑ Log protocol traffic periodically

Logging Interval (in minutes): 1

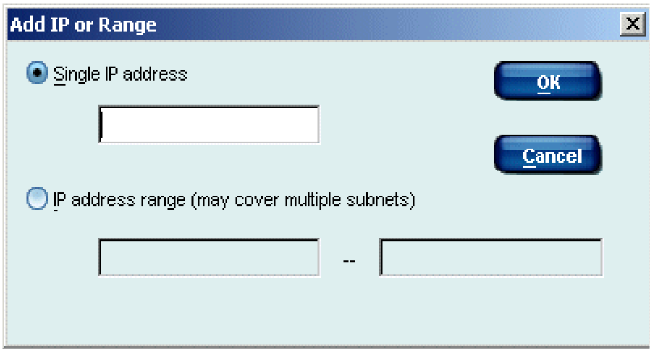
Network Agent global settings panel

- **Internal Network Definition**: Identify the machines in your network. By default, Network Agent does not monitor requests sent to internal machines, so Websense software does not filter or log these requests.

  (Identify machines Network Agent should monitor, under **Internal Traffic Monitoring**.)

To add machines other than the network segments recognized by default:

1. Click **Add**.



Add IP or Range dialog box

2. Enter an IP address or range, and then click OK.
3. To enter additional IP addresses or ranges, click Add again, and then repeat the process.

- **Internal Traffic Monitoring**: Identify any machines Network Agent should always monitor. Network Agent monitors requests sent to the IP addresses you specify.

  For example, keep track of requests made to an internal web server hosting your intranet site. In this case, enter the IP address of the internal web server machine.

  Note

  To monitor/filter file attachments exchanged internally via peer-to-peer messaging, you must specify the IP addresses of the internal machines involved. For more information, see *Instant Messaging Attachment Manager*, page 282.

  To identify a machine, click **Add**, and then enter its IP address. Repeat the process to identify additional machines.

- **Additional Settings**: Specify general monitoring behavior for Network Agent.

- **Bandwidth calculation interval (in seconds)**: Accept the default interval (**10** seconds), or specify a different interval. A lower value (more frequent interval) ensures higher accuracy in bandwidth measurements, but also increases overall network traffic. The default value balances these factors.

  Network Agent monitors bandwidth for filtering and load-balancing purposes. Filtering policies can restrict internet site access based on overall network bandwidth usage, or access to protocols based on usage per protocol. For more information, see *Managing bandwidth*, page 295.

- **Log requests and traffic volume by protocol**: Accept the default interval (**1** minute), or specify a different interval (at least 1 minute). *Un*check this box to prevent Network Agent from periodically logging protocol traffic, except for when TCP connections are closed.

When this option is selected, Network Agent periodically sends UDP and TCP connection status to Log Server. Network Agent always logs when TCP connections are closed.

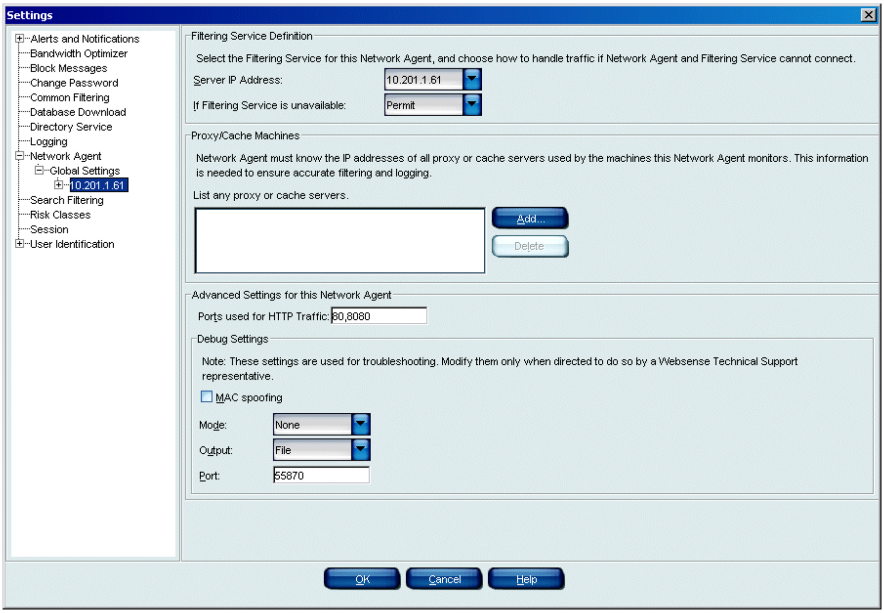
Local Settings

These determine the functions performed by each particular Network Agent. By default, Network Agent monitors requests from all internal machines it sees. Websense software filters internet content requested from these machines. Machine names are tracked in log data and Real-Time Analyzer output.

Configure how much of the internal network each Agent sees. Then, specify any desired exceptions to the default monitoring behavior.

Note

If you have multiple Network Agents installed, configure one at a time.



Filtering Service Definition

Select the Filtering Service for this Network Agent, and choose how to handle traffic if Network Agent and Filtering Service cannot connect.

Server IP Address: 10.201.1.61

If Filtering Service is unavailable: Permit

Proxy/Cache Machines

Network Agent must know the IP addresses of all proxy or cache servers used by the machines this Network Agent monitors. This information is needed to ensure accurate filtering and logging.

List any proxy or cache servers.

Advanced Settings for this Network Agent

Ports used for HTTP Traffic: 80,8080

Debug Settings

Note: These settings are used for troubleshooting. Modify them only when directed to do so by a Websense Technical Support representative.

☐ MAC spoofing

Mode: None

Output: File

Port: 55870

Network Agent local settings panel

- **Filtering Service Definition**: Define the Filtering Service for the selected Network Agent.
  - **Server IP Address**: The Filtering Service connected to this Network Agent.

  - **If Filtering Service is unavailable**: How to handle internet and protocol requests if the Filtering Service connected to this Network Agent is down.

- **Proxy/Cache Machines**: Identify any proxy or cache server machines situated between this Network Agent and client machines. Network Agent ignores traffic from the proxy to external web servers.

  Note

  You must identify any proxy or cache server with which Network Agent communicates. This includes any device (such as a cache engine product) used in proxy mode.

  If the proxy or cache server is not specified, Network Agent may only filter and log traffic from the server, and not user requests.

  To identify a machine, click **Add**, and then enter its IP address. Repeat the process to identify additional machines.

- **Advanced Settings for this Network Agent**:

  - **Ports used for HTTP traffic**: Accept the default ports (**80**, **8080**) on which Network Agent should monitor HTTP traffic, or specify different port numbers if necessary.

  Note

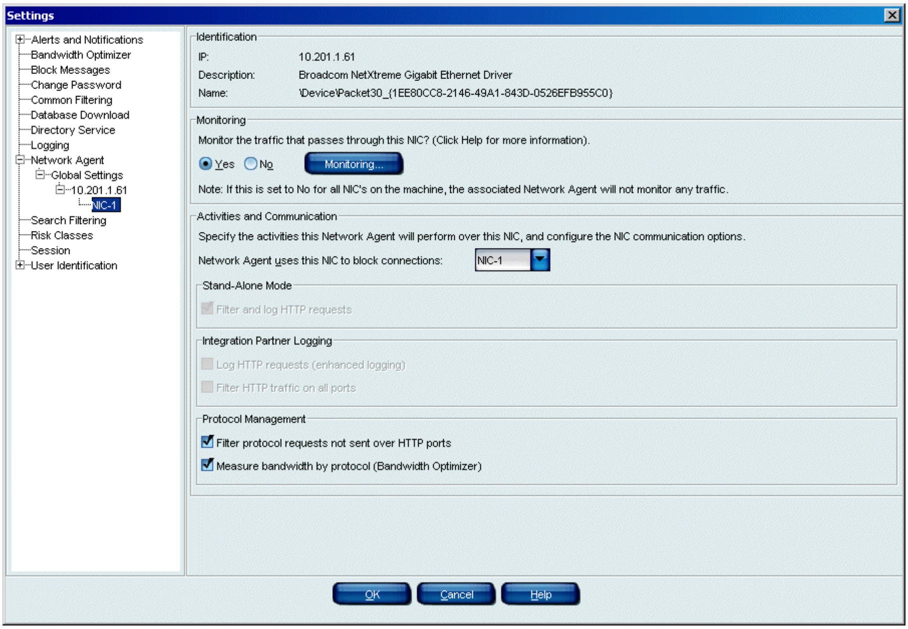
  Network Agent scans all ports for HTTP traffic. This protects against HTTP servers set up for spyware or phishing that use non-standard HTTP ports to avoid detection.

- **Debug Settings**: Do not modify the defaults unless instructed to by a Websense Technical Support representative.

Network Interface Card (NIC) settings

Network Interface Card (NIC) settings customize Network Agent behavior for a particular NIC on a Network Agent machine using multiple NICs.

Configure one NIC at a time.



Identification

IP: 10.201.1.61
Description: Broadcom NetXtreme Gigabit Ethernet Driver
Name: \Device\Packet30_{1EE80CC8-2146-49A1-843D-0526EFB955C0}

Monitoring

Monitor the traffic that passes through this NIC? (Click Help for more information).

● Yes ○ No Monitoring...

Note: If this is set to No for all NIC's on the machine, the associated Network Agent will not monitor any traffic.

Activities and Communication

Specify the activities this Network Agent will perform over this NIC, and configure the NIC communication options.

Network Agent uses this NIC to block connections: NIC-1

Stand-Alone Mode

☑ Filter and log HTTP requests

Integration Partner Logging

□ Log HTTP requests (enhanced logging)
□ Filter HTTP traffic on all ports

Protocol Management

☑ Filter protocol requests not sent over HTTP ports
☑ Measure bandwidth by protocol (Bandwidth Optimizer)

Network Agent NIC settings panel

- **Identification**: Displays identifying information for the selected NIC.
- **Monitoring**: Select whether to use this NIC to monitor traffic. (If the Network Agent machine has multiple NICs, you can configure more than 1 NIC to monitor traffic.)

  If you select **Yes**, click **Monitoring**.

  - **Monitor List**: Specify how much of the internal network should be monitored for internet and protocol requests.
    - **All**: Network Agent monitors requests from all machines it sees using the selected NIC. Typically, this includes all machines in the same network segment as the current Network Agent machine or NIC.

        - **None**: Network Agent does not monitor any machines in the selected NIC’s network segment.
        - **Specific**: Network Agent monitors only a portion of the selected NIC’s network segment.

        If you selected **Specific**, click **Add**, and then specify the IP addresses of the machines Network Agent should monitor.

        Note

        You cannot enter overlapping IP address ranges. If ranges overlap, network bandwidth measurements may not be accurate, and bandwidth-based filtering may not be applied correctly.

    - **Monitor List Exceptions**: Identify any internal machines Network Agent should exclude from monitoring.

        For example, Network Agent could ignore requests made by CPM Server. This way, CPM Server requests will not clutter Websense log data or Real-Time Analyzer output.

        To identify a machine, click **Add**, and then enter its IP address. Repeat the process to identify additional machines.

- **Activities and Communication**: Verify which NIC is used to activate Websense blocking in response to requests. Typically, the same NIC is used for monitoring and blocking. By default, the NIC you are editing is used.

    Note

    If Network Agent runs on a Linux or Solaris machine with multiple NICs, the operating system determines real-time which NIC to use for blocking. Network Agent may sometimes use a blocking NIC other than the one specified here.

If the Network Agent machine has multiple NICs performing monitoring, the monitoring NICs can use the same blocking NIC. The monitoring NIC can also use itself as a blocking NIC.

Note

Multiple NICs for a single Network Agent must be in the same network segment if only 1 is used for monitoring. Use the Websense Traffic Visibility tool to determine which network segment a NIC sees. Start the tool via **Start** > **Programs** > **Websense** > **Utilities** > **Traffic Visibility Tool**. For usage instructions, see the *Initial Setup* chapter of your installation guide.

Select the level of HTTP monitoring Network Agent should perform via the selected NIC.

- **Filter and log HTTP requests**: *(Active by default in Stand-alone mode)* Network Agent performs full HTTP monitoring and logging using the selected NIC.

Note

Which ports Network Agent scans for HTTP traffic is determined by the Websense version you are running. For more information, see *Managing HTTP traffic*, page 95.

- **Log HTTP requests (enhanced logging)**: Network Agent logs requests, but does not send HTTP usage data to Filtering Service. This is useful if your integration product filters HTTP traffic, but you still want to use Websense reporting features.
- **Protocol Management**: Select whether this Network Agent should handle non-HTTP protocol and application requests via the selected NIC.
    - **Filter protocol requests not sent over HTTP ports (Protocol Management)** activates the Protocol Management feature (see *Managing protocols*, page 274).

- **Measure bandwidth by protocol (Bandwidth Optimizer™)** activates the Bandwidth Optimizer feature. Network Agent uses this NIC to track network bandwidth usage by each protocol or application (see *Managing bandwidth*, page 295).

> **Note**
>
> Click **Save Changes** above the navigation tree to save the Network Agent configuration.

Filtering internet content

The Websense Network Agent lets you block internet content:

- Transmitted by protocols or applications, based on port number or IP address
- Transmitted over particular ports or IP addresses, regardless of how data is transferred
- Of an application type, regardless of the port or IP address used for data transmission
- Transmitted from a source with identifiable IP address

Network Agent can be used in conjunction with a proxy server, firewall, or cache product that is integrated with Websense software. Typically, the integration product manages all HTTP, HTTPS and FTP internet content, while Network Agent manages all other network-based protocols.

Network Agent can also be used without an integrated proxy, cache or firewall. In this case, select **Stand-alone** during installation to activate HTTP, HTTPS and FTP internet filtering. Network Agent provides full filtering capabilities for all HTTP internet content, plus **Permit** and **Block** filtering options for HTTPS and FTP content.

> **Note**
>
> When Network Agent is in stand-alone mode, keyword blocking and custom URL filtering do not apply to FTP requests. This is because Network Agent identifies FTP requests by IP address and not by URL.

✓ **Note**

When Filtering Service is down, users can access to all internet sites, protocols and applications by default. You can change this default behavior using the **If Filtering Service is unavailable** option (see *Local Settings*, page 89).

Managing HTTP traffic

By default, Network Agent scans ports 80 and 8080 for HTTP traffic. However, HTTP servers used for spyware or phishing have begun using non-standard HTTP ports to avoid detection, sometimes even changing the ports they use. You can specify additional ports to scan, if you know which ports to monitor.

To specify ports, select **Server > Settings > Network Agent**, select the Network Agent machine in the tree at the left, and add ports under **Advanced Settings for this Network Agent**.

✓ **Note**

Network Agent scans all ports for HTTP traffic. Scanning all ports adds a layer of protection against potentially intrusive HTTP content.

Managing protocols and internet applications

Websense software can filter internet requests based on protocols or internet applications other than HTTP, HTTPS or FTP–for example, those used for instant messaging, streaming media, file sharing, file transfer, internet mail, and various other network or database operations.

Websense software manages protocols and internet applications in conjunction with an integration product. When users make internet requests, the integrated firewall, proxy or cache product distinguishes HTTP content from content provided by other network or application protocols. The integration product then passes the HTTP content to Filtering Service for filtering, and leaves traffic from other protocols to be monitored by the Websense Network Agent.

Websense software can block internet content transmitted over particular ports or IP addresses, or marked by particular signatures, regardless of the nature of data. For more information, see *How protocols are filtered*, page 277.

For more information, including instructions on configuring protocol definitions and protocol-based filtering, see *Managing protocols*, page 274.

Protocol usage

To continue enhancing how Network Agent handles protocols, Websense, Inc. can gather actual protocol usage data. Websense, Inc. only gathers usage data for Websense-defined protocols, and not for any custom protocols you have defined.

Websense, Inc. does not collect usage data from your network unless you allow it. You are given the option to disable usage data gathering during installation (it is enabled by default). However, you can disable it later:

1. Select **Server** > **Settings**.
2. Select **Common Filtering** at the left.
3. Uncheck **Allow Websense to gather protocol usage data**.

Measuring network bandwidth

Websense Enterprise® Bandwidth Optimizer is an optional feature available for purchase with Websense software. This feature lets you limit internet access based on bandwidth availability. Network Agent enables this *threshold* filtering, or filtering of particular types of internet content based on available network bandwidth. For more information, see *Managing bandwidth*, page 295.

CHAPTER 5

Clients

Initially, Websense software either filters or monitors all clients in the same manner, depending on the **Initial Filtering** setting established during installation (see the installation guide). If you selected **Filter Internet traffic based on a predefined policy**, the **Global** policy enforces the Default Settings category set and the Default Settings protocol set for all clients. If you selected **Monitor Internet traffic only**, the Global policy causes Filtering Service to permit clients' requests and log them.

Customize how Websense software filters requests from specific users or machines by adding them as *clients* via Websense Manager. Clients can be:

- **Directory objects**:
  - **Users**: Specific users having accounts in a directory service that Websense software can communicate with.
  - **Groups**: Specific groups established in a directory service that Websense software can communicate with.
  - **Domains**: Group of networked computers that share a common communications address.
  - **Organizational Units**: Custom, high-level definitions in a directory service that associate related sub-groups.
- **Workstations**: Individual computers in your network, defined by IP address.
- **Networks**: Groups of computers, each defined collectively as a range of IP addresses.

After a client is added via Websense Manager, you can assign it a specific policy (see *Assigning policies to clients*, page 304). The Websense Policy Server enforces only 1 policy per internet request.

When multiple policies apply, such as when separate policies are assigned to the user and the machine, Policy Server determines which policy to enforce as follows:

1. Apply the policy assigned to the user making the request. If that policy has no category set scheduled at the time of the request, use the next applicable policy.
2. If there is no user-specific policy, or the policy has no active category set at the time of the request, look for a policy assigned to the workstation or network from which the request was made.
3. If there is no workstation or network-specific policy, or the policy has no active category set at the time of the request, look for a policy assigned to any group to which the user belongs. If the user belongs to multiple groups, Websense software considers all group policies that apply. For more information, see page 37.
4. If no group-specific policy is found, or the policy has no category set assigned at the time of the request, enforce the **Global** policy.
5. If no category set or protocol set is scheduled in the **Global** policy at the time of the request, apply the **Default Settings** category set or protocol set.

Directory services

When Websense software is installed for the first time, all users are filtered by the **Global** policy. However, you can filter based on individual directory object (user, group, or domain/organizational unit) policies.

This requires that Websense software be configured to access your directory service to get directory object information. For instructions, see:

- *Windows NTLM-based directory*, page 100
- *LDAP-based directory*, page 101

Note

You can only configure settings for 1 type of directory service per Policy Server. Settings for additional directory services are not saved.

Websense software can communicate with Windows NTLM-based directories, as well as Windows Active Directory, Sun™ Java System Directory Server and Novell Directory Services/eDirectory, accessed via Lightweight Directory Access Protocol (LDAP).

Websense, Inc. recommends installing the Websense User Service on a Windows machine (though it can reside on a Linux/Solaris machine). Typically, this is the machine where Policy Server is installed.

If you are running Websense Enterprise Client Policy Manager, it must be configured to point to Policy Server and User Service. Alternatively, install separate instances of Policy Server and User Service for use with Client Policy Manager modules only.

Your directory service can run on the same operating system as Websense software, or on a different operating system. Even if you are using a Windows NTLM-based directory service, you can run the Websense User Service on Windows, Linux, or Solaris.

Windows NTLM-based directory

Websense software accesses your directory service when you add directory objects to Websense Manager to assign filtering policies, and when Websense software analyzes internet requests. To filter based on specific user, group, and domain/organizational unit policies, add the directory objects to filter to Websense Manager, and then assign policies to them.

Directory objects that have not been added to Websense Manager and assigned specific policies are filtered by the policy assigned to the workstation, if any, or by the **Global** policy. For more information, see *Adding directory objects*, page 114.

The Websense User Service is specially designed to be compatible with Windows- or UNIX-based operating systems. Even if you are using a Windows NTLM-based directory service, you can run the Websense User Service on Windows, Linux, or Solaris.

Windows NT Directory or Active Directory in mixed mode

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Directory Service** at the left. The directory service settings are displayed.
3. Select **Windows NT Directory / Active Directory (Mixed Mode)**.
4. Click **OK**.

Windows 2000/2003 environment

If you are running Windows 2000/2003, but are still using a Windows NTLM-based directory service, configure the Websense User Service to run using an account with local security attributes.

Log on to the User Service machine as a user with local administrative rights, and then configure a Local Security Policy for User Service. Configuring the account User Service uses to communicate with the directory service to run as part of the operating system enables Websense software to identify users correctly.

For more information, see the Microsoft Management Console online Help. Select **Start** > **Programs** > **Administrative Tools** > **Local Security Policy**, and then open the **Help** menu.

LDAP-based directory

Websense software supports Sun Java System Directory Server, Novell eDirectory and Windows Active Directory accessed via Lightweight Directory Access Protocol (LDAP).

If user, group, and domain/organizational unit information resides in Active Directory, a Sun Java System directory, or a Novell directory, configure Websense software to retrieve this information. Follow the instructions in the appropriate section.

Note

Websense software does not accept LDAP user names with blank passwords. If you are using an LDAP-based directory service, ensure that all user names are assigned passwords.

When configuring any of these directory services to communicate with Websense software, you can secure communications between Websense software and the directory server.

Websense software can use LDAP expressions to classify users for filtering purposes. Create named groups of users based on any LDAP attribute in your directory service, and add these groups to Websense Manager. For more information, see page 111.

Active Directory

Follow these instructions to configure Websense software to communicate with the Global Catalog Server.

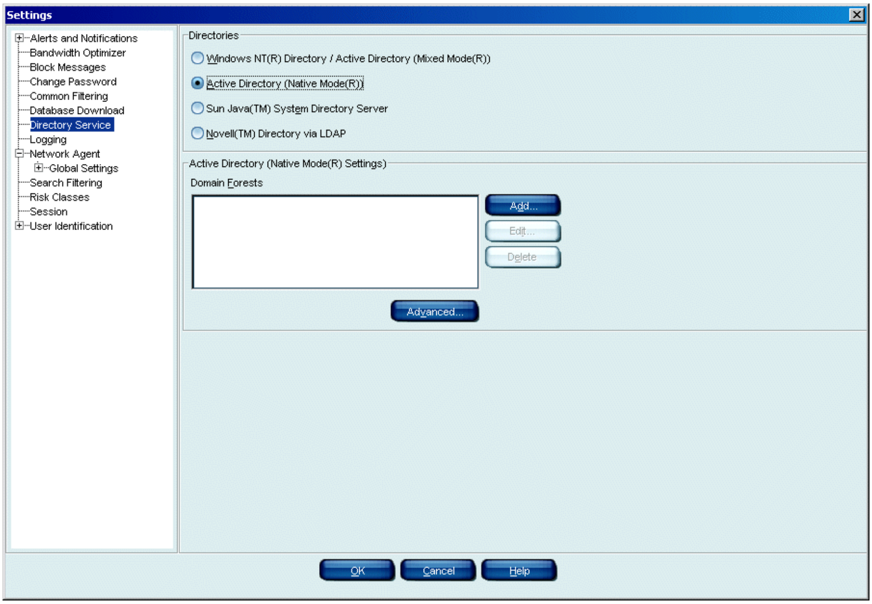
Note

If you have more than 2000 users in a single Active Directory container, you must increase the user limit in Global Catalog Server in order for all users in your directory service to be added to Websense Manager (see Websense Knowledge Base item #741). Go to www.websense.com, and then navigate to the Support & Knowledge Base page.

1. Ensure that User Service can connect to domain controllers in your network. Otherwise, local groups are not displayed when you add directory objects to Websense Manager.

   Connections to domain controllers are enabled during Active Directory setup. To verify this from the User Service machine, use `ping` or a similar utility.

2. Select **Server** > **Settings**. The Settings dialog box appears.
3. Select **Directory Service** at the left. The directory service settings are displayed.
4. Select **Active Directory**.



Directories

○ Windows NT(R) Directory / Active Directory (Mixed Mode(R))

● Active Directory (Native Mode(R))

○ Sun Java(TM) System Directory Server

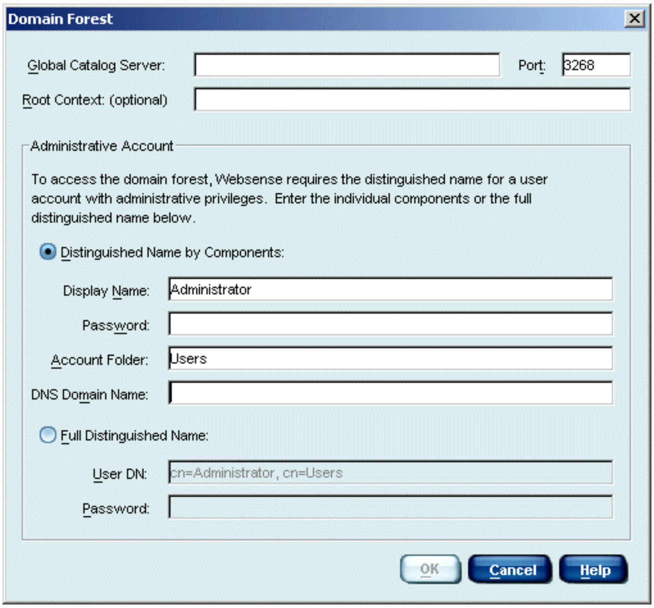
○ Novell(TM) Directory via LDAP

Active Directory (Native Mode(R) Settings)

Domain Forests

5. Add Global Catalog Server as a domain forest.

   a. Click **Add**. The Domain Forest dialog box appears.



Global Catalog Server:

Port: 3268

Root Context: (optional)

Administrative Account

To access the domain forest, Websense requires the distinguished name for a user account with administrative privileges. Enter the individual components or the full distinguished name below.

● Distinguished Name by Components:

Display Name: Administrator

Password:

Account Folder: Users

DNS Domain Name:

○ Full Distinguished Name:

User DN: cn=Administrator, cn=Users

Password:

   b. Enter the machine name or IP address of the **Global Catalog Server**.

   c. Enter the **Port** over which Global Catalog Server communicates with Policy Server (default is 3268).

   d. Enter the top-level **Root Context** for the organization (or start further down the path if appropriate). It must be a valid context in your domain. As an example, *dc=mycompany,dc=com*.

      If this field is left blank, Websense software begins searching at the top level of the directory service.

Note

For best results, do not have the same user name in multiple domains. If your network includes multiple domains and you need duplicate user names, configure Websense software to search only 1 domain at a time.

If Global Catalog Server is associated with more than 1 domain, and Websense software finds duplicate account names for the user logging on, Websense cannot transparently identify that user.

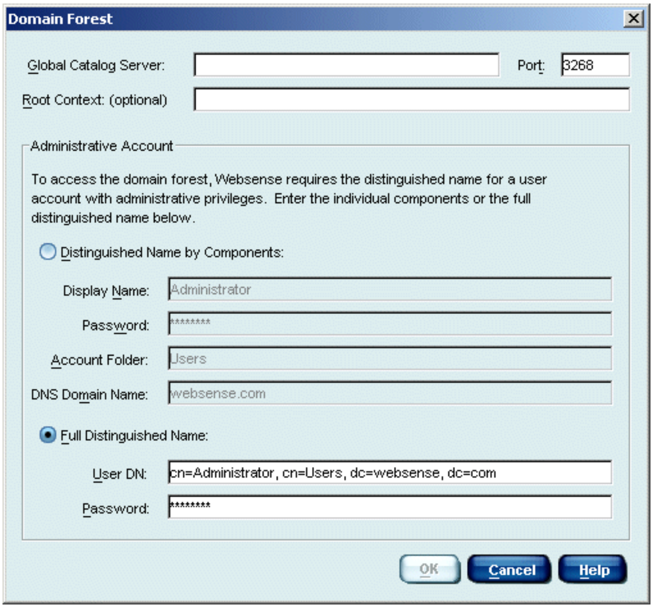
e. Under **Administrative Account**, select **Distinguished Name by Components** to enter the distinguished name (DN) for the administrative account Websense software will use to access the domain forest. Use the common name (cn) form of the administrative user name, and *not* the user ID (uid) form.

Enter the DN components separately in the **User Name**, **Account Folder** and **Domain Name** fields.

Note

The **Account Folder** field does not support values with the organizational unit (*ou*) tag (for example, *ou=Finance*). If your administrative account name contains an *ou* tag, enter the **Full Distinguished Name** for the administrative account, as described below. For example: *cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net*.

Alternatively, select **Full Distinguished Name** to enter the distinguished name as 1 string in the **User DN** field, as in this example.


Domain Forest

Global Catalog Server: Port: 3268

Root Context: (optional)

Administrative Account

To access the domain forest, Websense requires the distinguished name for a user account with administrative privileges. Enter the individual components or the full distinguished name below.

○ Distinguished Name by Components:

Display Name: Administrator

Password: ********

Account Folder: Users

DNS Domain Name: websense.com

● Full Distinguished Name:

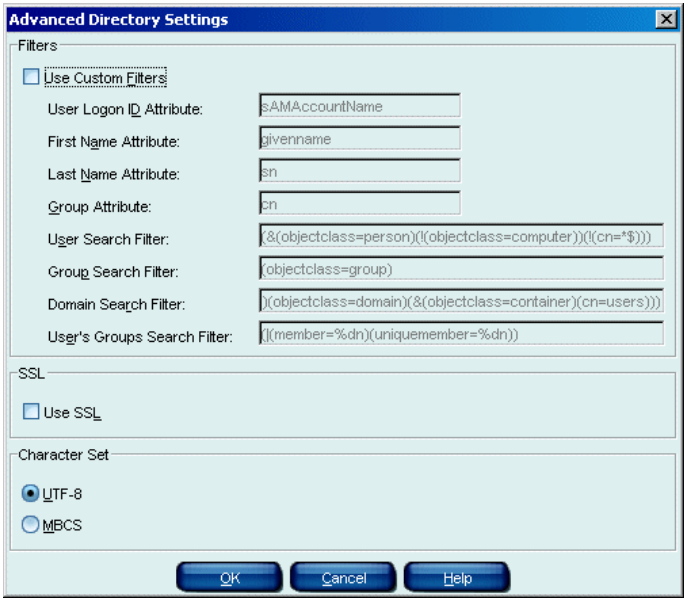
User DN: cn=Administrator, cn=Users, dc=websense, dc=com

Password: ********

Full Distinguished Name entered

f. Repeat steps a-e for each Global Catalog Server machine. Click **OK** when finished.

6. Click **Advanced Settings**. The Advanced Directory Settings dialog box appears.



Advanced Directory Settings

Filters

□ Use Custom Filters

User Logon ID Attribute: sAMAccountName

First Name Attribute: givenname

Last Name Attribute: sn

Group Attribute: cn

User Search Filter: (&(objectclass=person)(!(objectclass=computer))(!(cn=*$)))

Group Search Filter: (objectclass=group)

Domain Search Filter:)(objectclass=domain)(&(objectclass=container)(cn=users)))

User's Groups Search Filter: (|(member=%dn)(uniquemember=%dn))

SSL

□ Use SSL

Character Set

● UTF-8

○ MBCS

7. Verify the default settings Active Directory provides. Typically, the default settings are adequate.

8. To secure communications between Websense software and Active Directory Server, check **Use SSL**.

   Selecting the **Use SSL** option tells Websense software to use Secure Sockets Layer (SSL) technology to secure communications between the Websense User Service and the directory service. When unchecked, SSL is not used.

   ✓ **Note**

   By default, Websense software encodes LDAP directory server configuration information based on the character set specified under **Character Set** in the Advanced Directory Settings dialog box. If you need to use a character set other than the options available, contact Websense Technical Support.

9. Click **OK** to close the Settings dialog box and update Policy Server with your changes.
10. Add the objects in Active Directory to Websense Manager (see *Chapter 5: Clients*).

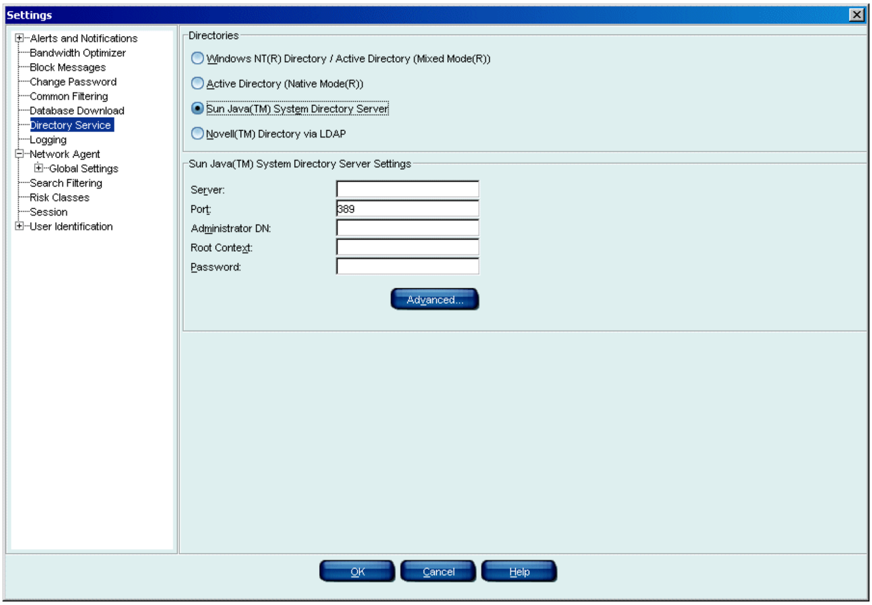
Additionally, you may need to configure Websense software to recognize custom object class types (see *Custom object class types*, page 111).

Sun Java System directory server

Follow these instructions to configure Websense software to access a Sun Java System (formerly iPlanet) directory service.

This configuration is saved to the Websense Policy Server, which then applies the settings to User Service.

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Directory Service** at the left.
3. Select **Sun Java System Directory Server**.



Directories

○ Windows NT(R) Directory / Active Directory (Mixed Mode(R))

○ Active Directory (Native Mode(R))

● Sun Java(TM) System Directory Server

○ Novell(TM) Directory via LDAP

Sun Java(TM) System Directory Server Settings

Server:

Port: 389

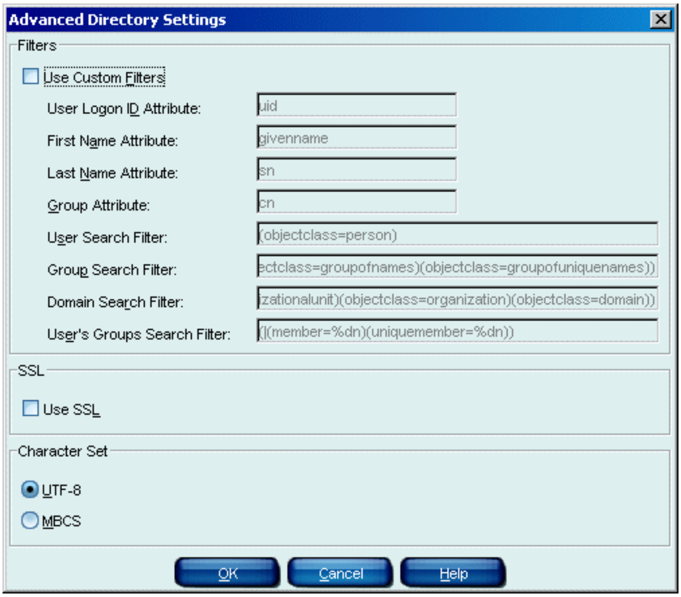
Administrator DN:

Root Context:

Password:

4. Specify the machine name or IP address of the machine running the Sun Java System directory in the **Server** field, and the corresponding **Port** number (default is 389).

5. If your Sun Java System server requires an administrator user name and password for read-only access, enter them in the **Administrator DN** and **Password** fields.
6. Enter the **Root Context**. This is required by Sun Java System to narrow the search for user or group information. For example, *o=domain.com*.
7. Click **Advanced Settings**. The Advanced Directory Settings dialog box appears.



Advanced Directory Settings

Filters

□ Use Custom Filters

User Logon ID Attribute: uid

First Name Attribute: givenname

Last Name Attribute: sn

Group Attribute: cn

User Search Filter: (objectclass=person)

Group Search Filter: ectclass=groupofnames)(objectclass=groupofuniquenames))

Domain Search Filter: zationalunit)(objectclass=organization)(objectclass=domain))

User's Groups Search Filter: (|(member=%dn)(uniquemember=%dn))

SSL

□ Use SSL

Character Set

● UTF-8

○ MBCS

8. To secure communications between User Service and the Sun Java System Directory Server, check **Use SSL**.

   Activating the **Use SSL** option tells Websense software to use Secure Sockets Layer (SSL) technology to secure communications between User Service and the directory service.

   ✓ **Note**

   By default, Websense software encodes LDAP directory server configuration information based on the character set specified under **Character Set** in the Advanced Directory Settings dialog box. If you need to use a character set other than the options available, contact Websense Technical Support.

9. Click **OK** to close the Advanced Directory Settings dialog box.
10. Click **OK** to close the Settings dialog box.
11. Close Netscape Certificate Management System, and stop User Service (see *Stopping or starting Websense services*, page 191).
12. Move both database files to the **Policy Server** directory. If prompted, overwrite any existing files. Add the objects in your Sun Java System directory to Websense Manager (see *Adding directory objects*, page 114).
13. Verify that User Service successfully connected to the directory service using SSL. Look for a connection from **Websense User Service** in Sun Java System Directory Server's Access Log.
14. Enable Websense manual authentication so that if Websense software is not able to identify users transparently, it can prompt users for directory authentication (see *Manual authentication*, page 180).

    Additionally, you may need to configure Websense software to recognize custom object class types (see *Custom object class types*, page 111).

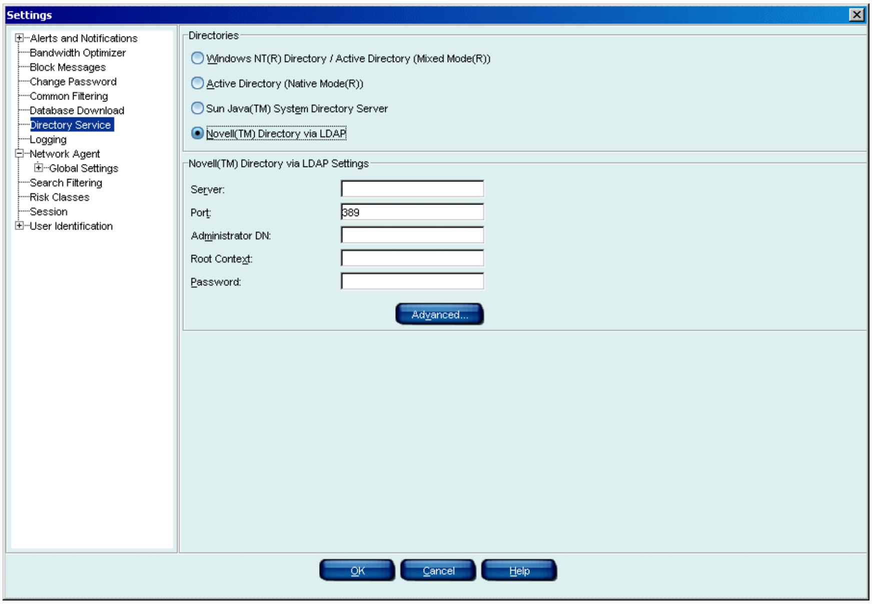
Novell eDirectory

This configuration is saved to the Websense Policy Server, and User Service inherits the settings.

To configure Websense software to access the Novell directory service:

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Directory Service** at the left. The directory service options are displayed.

3. Select **Novell Directory via LDAP**.



Directories

○ Windows NT(R) Directory / Active Directory (Mixed Mode(R))

○ Active Directory (Native Mode(R))

○ Sun Java(TM) System Directory Server

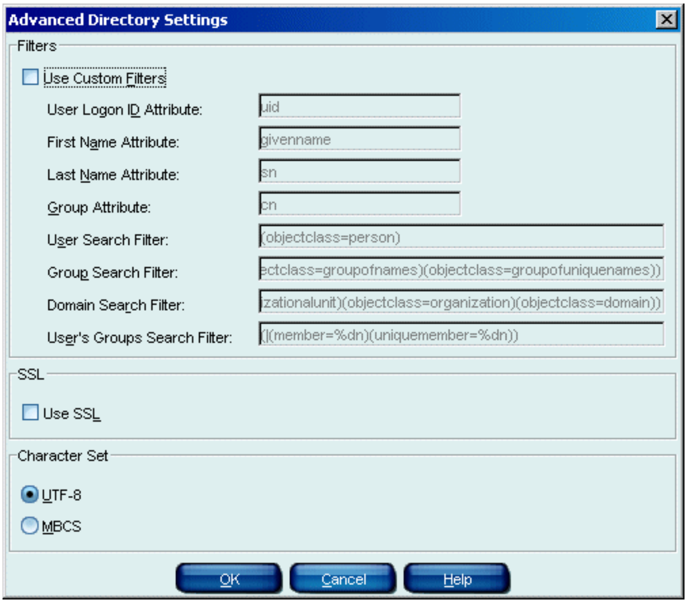
● Novell(TM) Directory via LDAP

Novell(TM) Directory via LDAP Settings

Server:	
Port:	389
Administrator DN:	
Root Context:	
Password:	

4. Specify the machine name or IP address of the machine running Novell eDirectory in the **Server** field, and the **Port** number (default is 389).
5. If your Novell directory requires an administrator user name and password for read-only access, enter them in the **Administrator DN** and **Password** fields.
6. Enter the **Root Context**, required by the Novell eDirectory to narrow the search for user or group information. For example, *o=domain.com*.

7. Click **Advanced Settings**. The Advanced Directory Settings dialog box appears.



Advanced Directory Settings

Filters

□ Use Custom Filters

User Logon ID Attribute: uid

First Name Attribute: givenname

Last Name Attribute: sn

Group Attribute: cn

User Search Filter: (objectclass=person)

Group Search Filter: ectclass=groupofnames)(objectclass=groupofuniquenames))

Domain Search Filter: zationalunit)(objectclass=organization)(objectclass=domain))

User's Groups Search Filter: (|(member=%dn)(uniquemember=%dn))

SSL

□ Use SSL

Character Set

● UTF-8

○ MBCS

8. Verify the default settings the Novell eDirectory provides. Make changes if necessary.

Note

By default, Websense software encodes LDAP directory server configuration information based on the character set specified under **Character Set** in the Advanced Directory Settings dialog box. If you need Websense software to use a character set other than the options available, contact Websense Technical Support for assistance.

9. To secure communications between User Service and Novell eDirectory, check **Use SSL**.

Selecting the **Use SSL** option tells Websense software to use Secure Sockets Layer (SSL) technology to secure communications between User Service and the directory service.

> **Note**
>
> Using SSL to secure communications between Websense software and Novell eDirectory in environments using Sun Java System Web Proxy Server is currently *not* supported.

10. Click **OK** to close the Advanced Directory Settings dialog box.
11. Click **OK** to close the Settings dialog box.
12. Add the objects in your Novell eDirectory to Websense software by following the instructions in *Chapter 5: Clients*.
13. Enable Websense manual authentication so Websense software prompts users for directory authentication (see *Manual authentication*, page 180).

You may need to configure Websense software to recognize custom object class types (see *Custom object class types*, page 111).

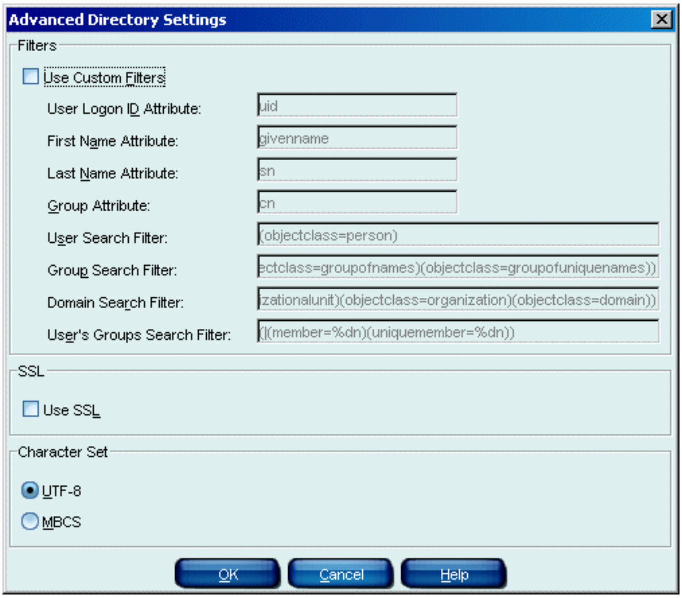
Custom object class types

Adding directory objects to Websense Manager to assign specific filtering policies requires a search of the directory service that houses user, group and domain information. When Websense software requests directory object information from a directory service, it searches the entries with the attribute names of *organization* and *organizationalunit* by default.

If you have customized these object class types within the directory, you must configure Websense software to recognize the new object class types:

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Directory Service** at the left. The directory service options are displayed.

3. Click **Advanced Settings**. The Advanced Directory Settings dialog box appears.



Advanced Directory Settings

Filters

□ Use Custom Filters

User Logon ID Attribute: uid

First Name Attribute: givenname

Last Name Attribute: sn

Group Attribute: cn

User Search Filter: (objectclass=person)

Group Search Filter: ectclass=groupofnames)(objectclass=groupofuniquenames))

Domain Search Filter: zationalunit)(objectclass=organization)(objectclass=domain))

User's Groups Search Filter: (|(member=%dn)(uniquemember=%dn))

SSL

□ Use SSL

Character Set

● UTF-8

○ MBCS

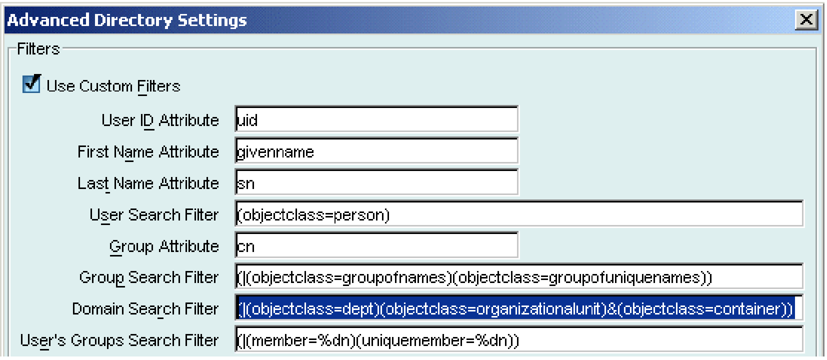
4. Check **Use Custom Filters**. The default filter strings appear in the various **Filter** fields.

5. Edit the existing filter strings, substituting object class types specific to your directory. For example, if your directory uses an object class type such as *dept* instead of *organizationalunit*, insert a new argument in the **Domain Search Filter** field. (The example shown applies to Sun Java System Directory Server or Novell eDirectory.)

   Attributes are always strings used in searching the directory service contents. Custom filters provide the functionality described here.

   - **User Search Filter**: Filters user information that is displayed in the Add Directory Objects dialog box.
   - **Group Search Filter**: Defines how group information is displayed in Websense Manager
   - **Domain Search Filter**: Defines how domain information is displayed in Websense Manager

- **User’s Groups Search Filter**: Filters user group information that is displayed in the Add Directory Objects dialog box. *%dn* represents user name.



Advanced Directory Settings

Filters

☑ Use Custom Filters

User ID Attribute: uid

First Name Attribute: givenname

Last Name Attribute: sn

User Search Filter: (objectclass=person)

Group Attribute: cn

Group Search Filter: (|(objectclass=groupofnames)(objectclass=groupofuniquenames))

Domain Search Filter: (|(objectclass=dept)(objectclass=organizationalunit)&(objectclass=container))

User's Groups Search Filter: (|(member=%dn)(uniquemember=%dn))

Domain Search Filter string with a custom object class type added

The **Domain Search Filter** string shown indicates that instead of only searching for objects of type *organizationalunit* in the directory, Websense software would also search for object of type *dept*. Alternatively, you could replace the argument *(objectclass=organizationalunit)* with *(objectclass=dept)*, to have Websense software search for objects of type *dept* instead of *organizationalunit*.

6. Click **OK** to close the Advanced Directory Settings dialog box.
7. Click **OK** to close the Settings dialog box.

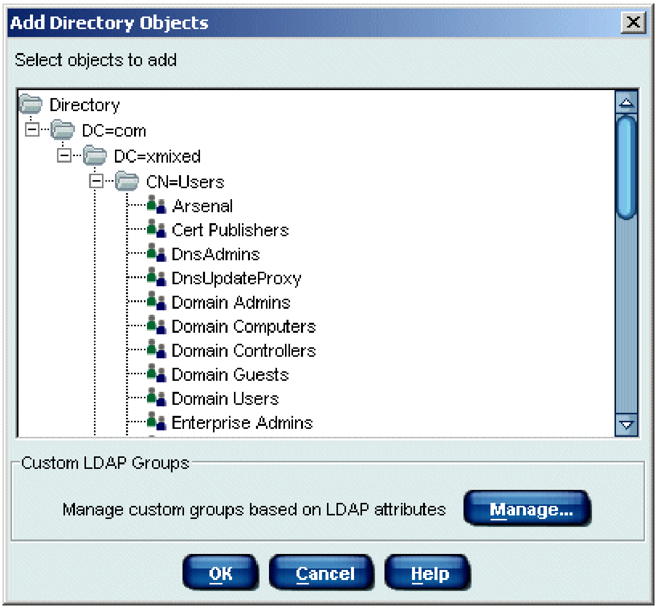
Adding directory objects

Add directory objects to Websense Manager to assign them distinct filtering policies. Any user *not* added is filtered by the policy for the group he or she belongs to, a workstation or network policy (if applicable), or the **Global** policy. To be added to Websense Manager, a user must have an account in a directory service that Websense software can communicate with, in the network where Websense software is installed.

✓ **Note**

If you are changing directory services, implement that change before adding directory objects. Otherwise, directory objects must be re-added after the change.

1. Right-click in the navigation tree, and then select **Add Directory Objects**.
2. The Add Directory Objects dialog box appears.
3. Double-click the **Directory** folder to display its domain/context list.
4. Double-click a domain/context folder to display a list of its objects.



Add Directory Objects

Select objects to add

- Directory
  - DC=com
    - DC=xmixed
      - CN=Users
        - Arsenal
        - Cert Publishers
        - DnsAdmins
        - DnsUpdateProxy
        - Domain Admins
        - Domain Computers
        - Domain Controllers
        - Domain Guests
        - Domain Users
        - Enterprise Admins

Custom LDAP Groups

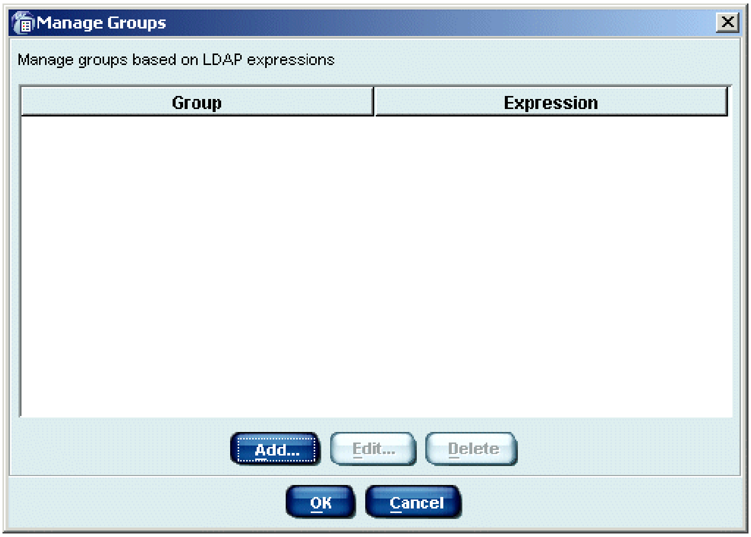
Manage custom groups based on LDAP attributes

5. Select the object to add to Websense Manager.

   To select multiple objects, press the **Ctrl** key while clicking each group name. To select a range of objects, hold down the **Shift** key while clicking the first and last users in the range.

6. *LDAP-based directory service only:* To add or edit a group based on an LDAP attribute, click **Manage**. The Manage Custom LDAP Groups dialog box appears.

   Windows-based directory service: Skip to Step 11.



7. To define a group in Websense Manager based on any attribute you have defined in your directory service, click **Add**. The Add Group dialog box appears.

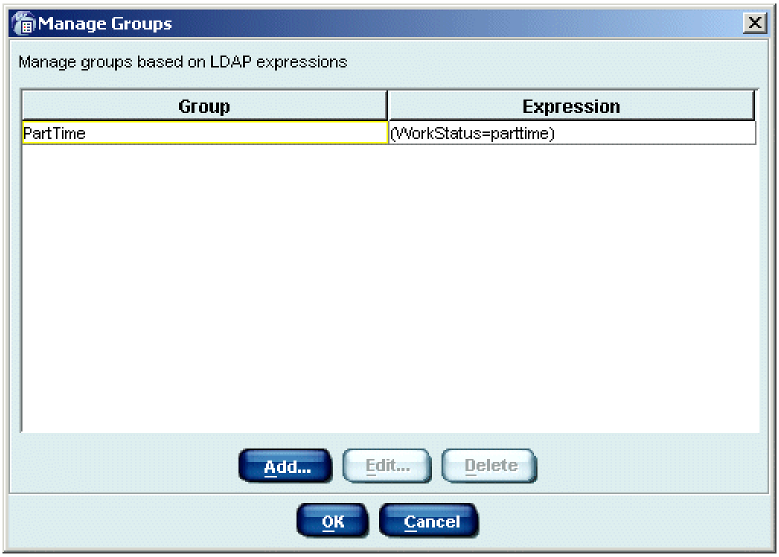
8. Enter a name for the group. Group names are case-sensitive.

9. Enter the expression that defines this group in your directory service. For example:

   ```
   (WorkStatus=parttime)
   ```

   where `WorkStatus` is a user attribute that indicates employment status, and `parttime` is a value indicating that the user is a part-time employee.

10. Click **OK**. The new group appears in the Manage Custom LDAP Groups dialog box, next to its defining expression.

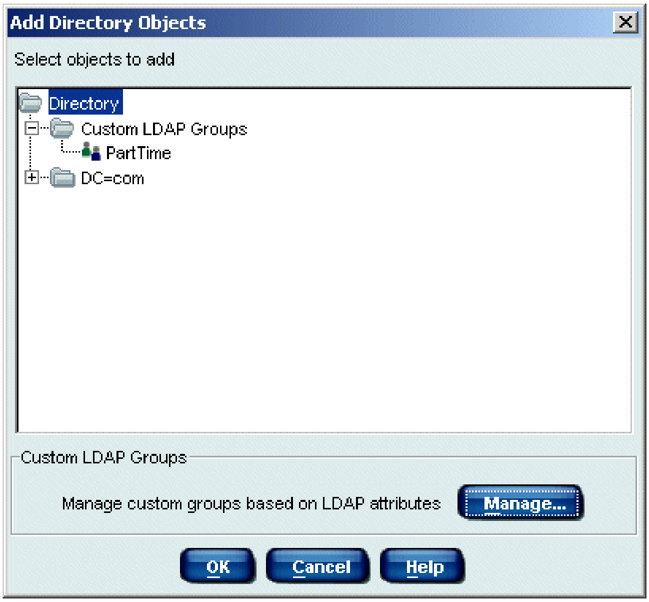


Manage groups based on LDAP expressions

Group	Expression
PartTime	(WorkStatus=parttime)

New group specified

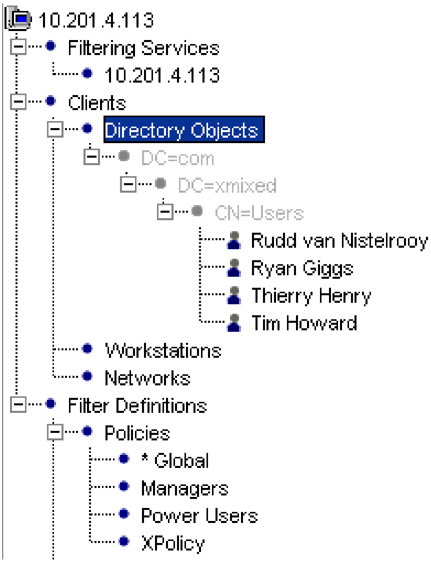
11. When you are done defining groups, click **OK** to return to the Add Directory Objects dialog box. The group you just created appears in the **Custom LDAP Groups** folder.



Directory objects with a group based on an LDAP attribute

12. *All directory services:* When finished adding user and group objects to Websense Manager, click **OK**.

13. To view users in the navigation tree, expand **Directory Objects**, then the user’s domain/context.



14. Click **Save Changes** above the navigation tree.

Note

For Websense software to filter internet requests from specific users, you may need to enable Websense manual authentication. Then, if Websense software is not able to identify users transparently, it prompts users for directory authentication. For more information, see *Manual authentication*, page 180.

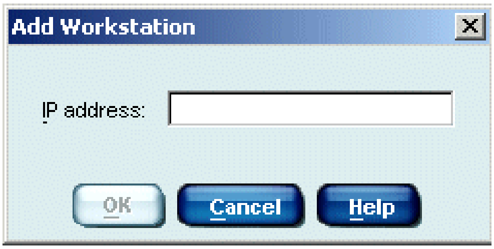
Requests continue to be filtered by the **Global** policy until another policy is assigned. For more information, see *Assigning policies to clients*, page 304.

Adding workstations

Adding a workstation enables you to assign a filtering policy specifically to it. This can be useful, for example, when a workstation is used by multiple people during the day.

Workstations are identified by IP address.

1. Right-click in the navigation tree, and then select **Add Workstation**.
2. The Add Workstation dialog box appears.
3. Enter the **IP address** of the workstation to add. (To add multiple workstations at once, see *Adding networks*, page 120).



4. Click **OK**. The IP address of the workstation appears in the navigation tree under **Workstations**.
5. Click **Save Changes** above the navigation tree.

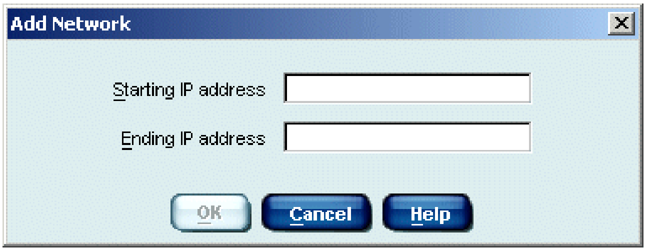
The workstation is filtered by the **Global** policy until another policy is assigned to it (see page 304).

Once a workstation is added, you can assign password override privileges to it, and give the password to the appropriate users. This enables users to access sites that would otherwise be blocked on that machine. For more information, see page 121.

Adding networks

Networks let you manage filtering collectively for several workstations. Define a range of IP addresses as a Websense network, and then assign a policy to that network. For each new network, the IP address range must be sequential and cannot overlap another IP address range already defined in Websense Manager.

1. Right-click in the navigation tree, and then select **Add Network**.
2. The Add Network dialog box appears.



3. Enter the **Starting IP address** and **Ending IP address** of the workstations to add as a network.
4. Click **OK**. The network appears in the navigation tree under **Clients** > **Networks**.
5. Click **Save Changes** above the navigation tree.

The network is filtered by the **Global** policy until another policy is assigned to it (see *Assigning policies to clients*, page 304).

Password override

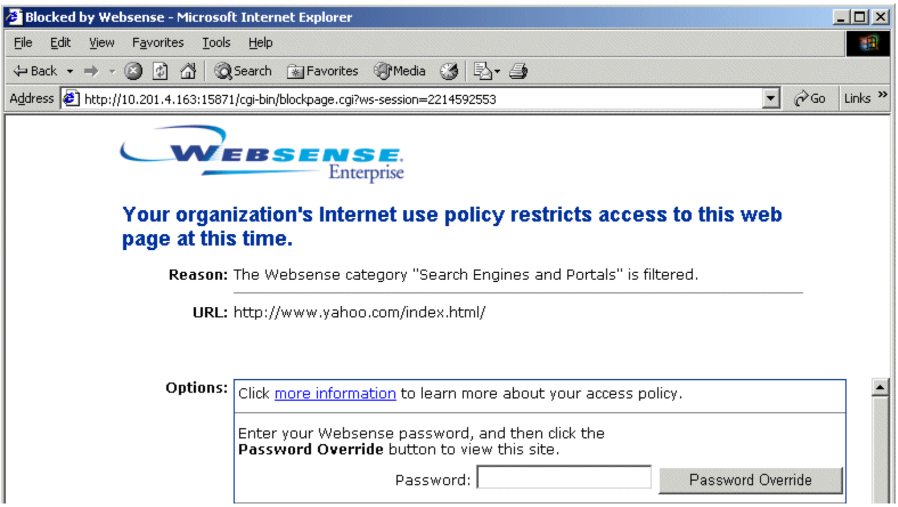
Password override lets users with valid passwords access sites that are otherwise blocked. Override privileges can be granted to individual users, groups, workstations or networks (IP address ranges).

When password override is activated, the Websense block message includes a password field. If a valid password is entered, Websense software permits free access to any blocked site for a limited amount of time.

Note

Password override can be used when clients are filtered by a single Policy Server. It should not be assigned to users or groups who may be filtered through multiple Policy Servers in a load-balancing configuration.

A user with password override privileges is presented with the Websense block page shown.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
WEBSENSE Enterprise
Password Override

http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=2214592553

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Search Engines and Portals" is filtered.

URL: http://www.yahoo.com/index.html/

Options: Click more information to learn more about your access policy.

Enter your Websense password, and then click the **Password Override** button to view this site.

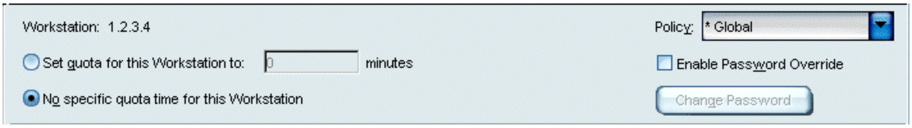
Password:

Block page allowing password override

Enabling password override

1. Select **Server** > **Settings** > **Common Filtering**.
2. For **Password Override timeout**, specify the time interval for access to blocked sites after a password has been entered.

   When the override period expires, the password must be entered again for access to additional blocked sites.
3. Expand **Directory Objects, Workstations, or Networks** in the navigation tree, and then select the client to which to grant password override privileges. The settings for the selected client appear in the content pane.



Workstation: 1.2.3.4

Policy: * Global

○ Set quota for this Workstation to: 0 minutes

□ Enable Password Override

● No specific quota time for this Workstation

4. Check **Enable Password Override**. The Enter Password dialog box appears.
5. Enter a password for this client or group of clients. Confirm the spelling by entering it again in the **Confirm new password** field.
6. Click **OK**.
7. Click **Save Changes** above the navigation tree.

Changing the password

1. Select the appropriate directory object, workstation, or network in the navigation tree.
2. Click **Change Password** in the content pane. The Enter Password dialog box appears.
3. Type a new password for this directory object, workstation, or network. Type it again to confirm it.
4. Click **OK**.
5. Click **Save Changes** above the navigation tree.
6. Inform the appropriate personnel of the new password.

Disabling password override

1. In the navigation tree, select the directory object, workstation, or network whose password override privilege is being disabled.
2. Uncheck **Enable Password Override** in the content pane.
3. Click **Save Changes** above the navigation tree.

Quota time

Quota time can be allocated to employees as:

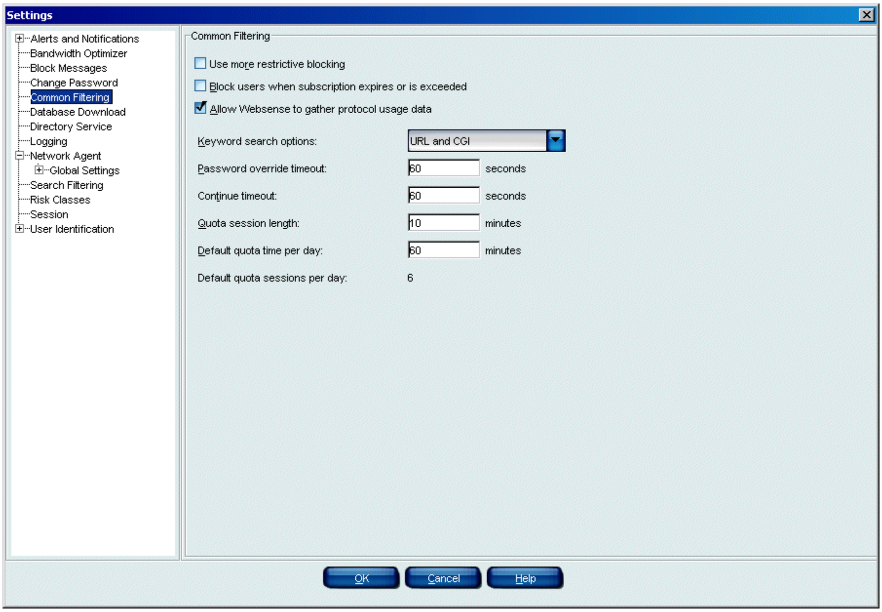
- Default quota time – allocated to all clients equally.
- Quota time – allocated specifically to clients that have been added to Websense Manager.

Default quota time

Default quota time is allocated to all clients equally. The default setting is 60 minutes, and can be changed as follows.

1. Select **Server** > **Settings**. The Settings dialog box appears.

2. Select **Common Filtering** at the left.



Common Filtering

☐ Use more restrictive blocking

☐ Block users when subscription expires or is exceeded

☑ Allow Websense to gather protocol usage data

Keyword search options: URL and CGI

Password override timeout: 60 seconds

Continue timeout: 60 seconds

Quota session length: 10 minutes

Default quota time per day: 60 minutes

Default quota sessions per day: 6

3. For **Quota session length**, enter the number of minutes for a quota session. (Ten minutes is the default time period.)
4. For **Default quota time per day**, enter the number of minutes a client can spend daily (default is 60 minutes). If quota time is specifically allocated to a client (see the next section), that time interval overrides the default time period.
5. Click **OK**.

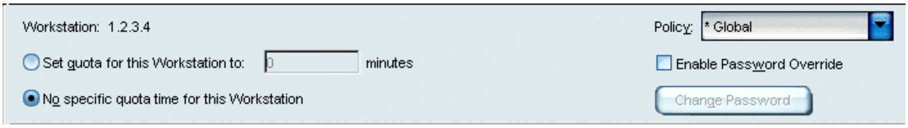
Allocating quota time to clients

1. Add to Websense Manager the user, group, workstation, or network to which to allocate quota time (see *Allocating quota time to clients*, page 125).

   ✓ **Note**

   Do not assign quota time to clients that are filtered by the **Always Block** category set.

2. Expand **Directory Objects**, **Workstations**, or **Networks** in the navigation tree, and then select the client to which to allocate quota time. The settings for the selected client appear in the content pane.



Workstation: 1.2.3.4

○ Set quota for this Workstation to: 0 minutes

● No specific quota time for this Workstation

Policy: * Global

□ Enable Password Override

3. Select **Set quota time for this user to...minutes**.
4. Enter the desired number of minutes (0-240) of quota time.
5. Click **Save Changes** above the navigation tree.

Change the filtering option on selected categories to **Limit by Quota** (see *Editing a category set*, page 257).

Filtering remote clients

Use the Remote Filtering feature to apply internet filtering to clients outside a network firewall. Remote Filtering is purchased separately, though it only works with a full Websense installation.

Follow the recommendations in the *Websense Enterprise Deployment Guide* carefully to deploy the Websense Remote Filtering Server and Remote Filtering Client. The installation guide provides instructions for installing these components.

> **Note**
>
> Install only 1 primary Remote Filtering Server instance per Filtering Service. For more information, see the *Websense Enterprise Deployment Guide*.

For remote clients, Websense software filters HTTP traffic only. The Websense Remote Filtering Server detects whether clients are inside or outside of the network firewall. If it determines that a client is inside the firewall, Remote Filtering is deactivated and the user is filtered just like other internal clients. Remote Filtering is only activated if the client is outside the firewall.

> **Note**
>
> If you are using Network Agent in Stand-Alone mode (without an integration product), configure Network Agent *not* to monitor the Remote Filtering Server machine (see *Initial configuration*, page 83).

How remote filtering works

Filtering of remote clients works similarly to internal filtering. Once a user is identified, the filtering policy assigned to that user is applied. If a policy includes use of quota time for limited viewing of sites, the configured quota time applies as long as users are successfully identified.

Bandwidth-based filtering is currently not supported for remote clients. Bandwidth generated by remote traffic is not included in bandwidth measurements (see *Managing bandwidth*, page 295).

For information on customizing block pages, see *Customized block messages*, page 52.

Virtual Private Network (VPN) connections

If users are connected via a network-based Virtual Private Network (VPN) and access the internet via the default network gateway or firewall, these remote clients are filtered in the same manner as internal clients.

How Websense identifies remote users

For Websense software to transparently identify remote users, users must log on to their cached domains. Users are then identified just as internal users are. If a user logs on using only a local account, the user is not recognized according to his network user account. In this case, Websense software applies the **Global** policy, and user activity is logged under the local user name.

Note

Remote clients must log on to cached domains for their internet activity to be logged to the Log Database. For more information about Delegated Reporting, see the Reporting documentation.

Corporate Edition users: Remote users also must log on to cached domains in order for users to be identified and Distributed Administration roles to take effect.

For remote clients, Websense software uses the last portion of the Media Access Control (MAC) address to recognize users, rather than the standard IP address. This means that policies assigned to specific IP addresses do not take effect. If no other policy is found for a particular remote user, Filtering Service applies the **Global** policy.

It is also possible that the last quadrant of a MAC address overlaps with another IP address. In this case, any policy assigned to that particular IP address is applied to the remote user.

For more information about transparent identification of users, see *Transparent identification*, page 130.

Manual authentication and remote clients

Manual authentication (see *Manual authentication*, page 180) is supported for remote clients. If **Prompt user for directory authentication** (Settings dialog box, **User Identification** panel) is active, and a situation arises where Websense software defaults to prompting users to log on, remote users are prompted by the browser to log on just as local users are.

CHAPTER 6

User Identification

Policy-based filtering lets you define individual filtering plans for different members of your organization. In any environment, assign policies to workstations (identified by IP address), or a single policy to a collection of workstations with contiguous IP addresses, defined as a network.

If your environment includes a directory service, Websense software lets you filter internet requests based on policies assigned to directory objects. Identify objects in a directory service, add them to Websense Manager, and assign specific policies to them. For more information, see *Directory services*, page 99.

To apply policies assigned to directory objects, Websense software must be able to identify the user making a request, given the originating IP address. There are various methods for this:

- Websense software receives user identification from your integration product, if it provides authentication. For more information, see the installation guide.
- Websense software identifies the user transparently, if your network uses a directory service and you implement Websense transparent identification. For more information, see *Transparent identification*, page 130.
- Websense software prompts the user for identification, if the information cannot be obtained otherwise. For more information, see *Manual authentication*, page 180.

Transparent identification

Transparent identification allows Websense software to filter internet requests from users in your directory service without prompting users to log on to the browser.

Several optional components enable Websense software to filter based on policies assigned to users or groups housed in a directory service. In all cases, Websense software must be configured appropriately.

These can be used alone or combined, with some exceptions noted later in this section.

- **Websense DC Agent**: Can be used with a Windows-based directory service. Periodically queries domain controllers and workstations for user logon sessions. Websense DC Agent can run on a Windows or Linux server. DC Agent should *not* need to reside in any particular domain.
- **Websense Logon Agent**: For use with Windows client machines. Identifies users as they log on to Windows domains. Logon Agent can run on Windows, Linux, or Solaris. The associated logon application runs only on Windows client machines.
- **Websense RADIUS Agent**: Can be used in conjunction with either Windows- or LDAP-based directory services. Works together with a RADIUS client and RADIUS server to identify users logging on from remote locations.
- **Websense eDirectory Agent**: For use with Novell eDirectory. Authenticates users against user accounts in Novell eDirectory.

For instructions on installing each agent, see the installation guide. For instructions on configuring a transparent identification agent to identify users, see the appropriate section in this chapter.

✓ **Note**

If you integrate a NetCache appliance with Websense software, for transparent identification to work, NetCache must send user names to Websense software in WinNT, LDAP, or RADIUS format.

Note

If you have a proxy server, Websense, Inc., recommends using Anonymous authentication in your proxy server with Websense transparent identification. In rare cases, enabling Basic or Integrated Windows Authentication in your proxy server may adversely affect access to internet applications.

Websense software can prompt users to manually authenticate if it cannot obtain user information from a transparent identification agent. This can occur if more than one user is assigned to the same machine, or if a user is an anonymous user/guest, or for other reasons. You can configure Websense software to prompt users for identification so they still can be filtered by object-specific policies. For more information, see *Manual authentication*, page 180.

If a user cannot be identified transparently, *and* manual authentication is not enabled, Websense software filters based on workstation or network policies, or the **Global** policy, depending on your configuration.

Combining transparent identification agents

Websense, Inc., supports some combinations of transparent identification agents within the same network. If your network configuration requires multiple agents, it is best to install them on separate machines. However, in some cases you can configure Websense software to work with multiple agents on a single machine. See the next table for details.

Supported combinations:

Combination	Same machine?	Same network?	Configuration required
Multiple DC Agents	No	Yes	Ensure that all instances of DC Agent can communicate with Filtering Service.
Multiple RADIUS Agents	No	Yes	Configure each instance to communicate with Filtering Service.
Multiple eDirectory Agents	No	Yes	Configure each instance to communicate with Filtering Service.
Multiple Logon Agents	No	Yes	Configure each instance to communicate with Filtering Service.
DC Agent + RADIUS Agent	Yes	Yes	See Websense Knowledge Base article #1115.
DC Agent + eDirectory Agent	No	No	Websense software does not support communication with both Windows and Novell directory services in the same deployment. However, you can have both agents installed, with only 1 active agent.
DC Agent + Logon Agent	Yes	Yes	Configure both agents to communicate with Filtering Service. By default, each agent uses a unique port, so port conflicts are not an issue unless these ports are changed.

Combination	Same machine?	Same network?	Configuration required
eDirectory Agent + Logon Agent	No	No	Websense software does not support communication with both Windows and Novell directory services in the same deployment. However, you can have both agents installed, with only 1 active agent.
RADIUS Agent + eDirectory Agent	Yes	Yes	Configure both agents to communicate with Filtering Service. When adding agents to Websense Manager, use an IP address to identify one, and a machine name to identify the other.

Transparent identification and remote connections

Websense software can transparently identify users logging on to your network from remote locations. If you have deployed the Websense Remote Filtering Server and Remote Filtering Client, Websense software can identify any remote user logging on to a cached domain using a domain account. For more information, see *Filtering remote clients*, page 126.

If remote filtering is not implemented, Websense software can still identify remote users, as described next.

Remote transparent identification with DC Agent

The same requirements apply as with local users: Websense DC Agent can reside on a Windows or Linux server. Users should log on to named Windows domains in your network. If remote users do not log on directly to domains in your network, DC Agent may not be able to identify these users. In this case, use Websense manual authentication (see *Manual authentication*, page 180).

Remote transparent identification with RADIUS Agent

If you are using a RADIUS server to authenticate users logging on from remote locations, Websense RADIUS Agent can transparently identify these users so you can apply filtering policies based on users or groups. For information about installing and configuring RADIUS Agent, see *Websense RADIUS Agent*, page 148.

Websense DC Agent

Websense DC Agent detects users in a Windows network running NetBIOS, WINS or DNS networking services. DC Agent itself can run on Windows or Linux.

Note

If you are running DC Agent on Linux and are using Windows Active Directory, NTLM authentication must be enabled in Active Directory. DC Agent on Linux is *not* currently supported with LDAP-based directory services.

DC Agent obtains user logon session information from domain controllers and workstations in your network, and sends user name/IP address pairings to the Websense User Service. User Service regularly stores the latest user information, and sends user-name-to-IP-address correspondences to appropriate Websense components. This allows users to be identified transparently whenever they make internet requests.

Note

If DC Agent does not update User Service, User Service caches user-name-to-IP-address mappings for 3 hours. You can refresh the cache by clicking the **Save Changes** button in Websense Manager. If a user is not filtered as expected, the User Service cache may need to be refreshed.

To enable transparent identification with DC Agent:

1. Install DC Agent. For more information, see *Installing Websense Components Separately* in the installation guide.

2. Configure Policy Server to allow User Service to communicate with DC Agent (see *Configuring User Service to communicate with DC Agent*, page 136).
3. Add the directory objects to filter individually via Websense Manager (see *Adding directory objects*, page 114).

Websense software can prompt users for identification if User Service is not able to obtain information from a DC Agent. For more information, see *Manual authentication*, page 180.

Installing DC Agent

DC Agent resides on a Windows or Linux server in the network. DC Agent can be installed with other Websense components or separately. For more information, see *Installing Websense Components Separately* in the installation guide.

✓ **Note**

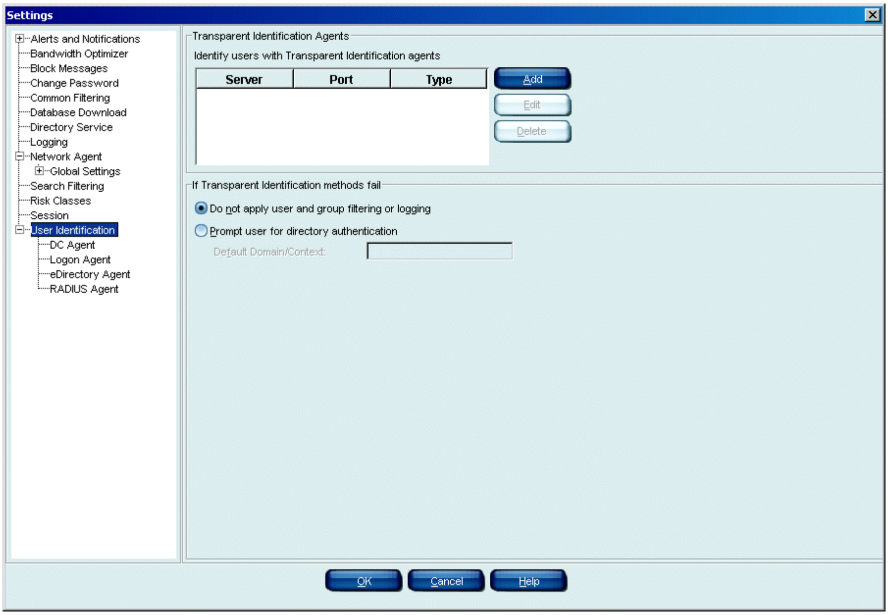
Run DC Agent using domain administrator privileges. On Windows, the domain administrators group used must be a member of the **Administrators** group on the current machine.

This is required for DC Agent to retrieve user logon information from the domain controller. If you cannot install DC Agent with such privileges, configure administrator privileges for these services after installation. For more information, see *Websense is not filtering based on a directory object policy*, page 321.

When you installed the Websense DC Agent, Websense software was configured to communicate with DC Agent. Verify your configuration as follows.

Configuring User Service to communicate with DC Agent

1. Right-click the Policy Server icon in Websense Manager, and then select **Log On to Server**.
2. Enter the password for this Policy Server, and then click **OK**.
3. Select **Server** > **Settings**. The Settings dialog box appears.
4. Select **User Identification** at the left. Installed agents appear in a list under **Identify users with these transparent identification agents**.



Transparent Identification Agents

Identify users with Transparent Identification agents

Server	Port	Type

If Transparent Identification methods fail

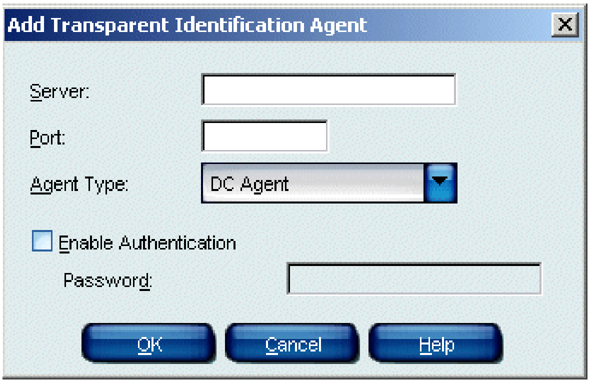
● Do not apply user and group filtering or logging

○ Prompt user for directory authentication

Default Domain/Context:

5. For a new agent instance that does not appear in the list, add the agent as follows.

a. Click **Add**. The Add Transparent Identification Agent dialog box appears.



Add Transparent Identification Agent

Agent Type: DC Agent

☐ Enable Authentication

b. Enter the following:

- **Server**: IP address or machine name of the machine where DC Agent is installed.

Note

Machine names must start with an alphabetical character (a-z), not a numeric or special character.

Machine names containing certain extended ASCII characters may not resolve properly. If you are using a non-English version of Websense software, enter an IP address instead of a machine name.

- **Port**: Number of the port over which User Service and DC Agent communicate. The default is 30600.

c. For **Agent Type**, select **DC Agent**.

d. To establish an authenticated connection between User Service and DC Agent, check **Enable Authentication**.

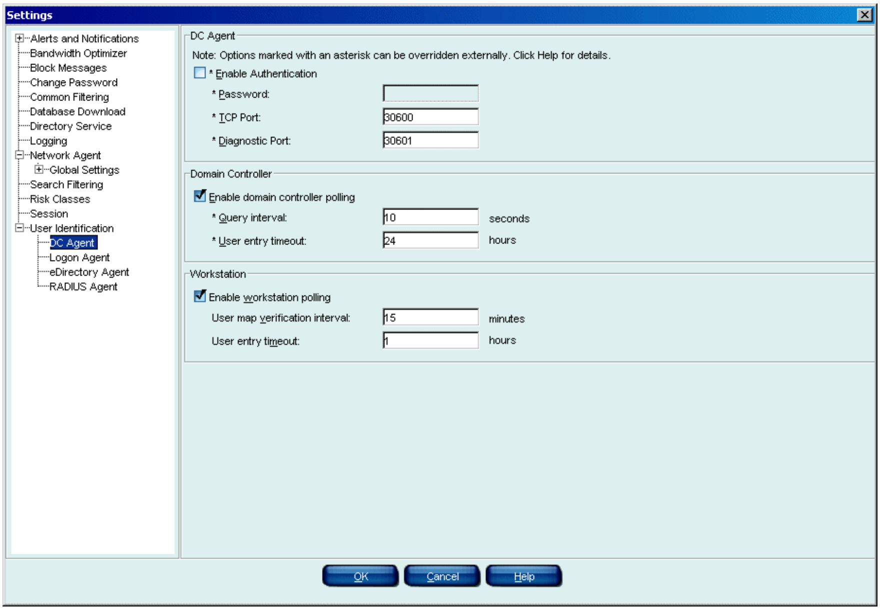
e. If you checked **Enable Authentication**, enter a password for the authenticated connection to DC Agent.

f. Click **OK**.

6. Expand **User Identification** > **DC Agent** at the left. The DC Agent settings are displayed.

✓ **Note**

These settings are global and apply to all instances of DC Agent. Fields marked with an asterisk (*) can be configured independently for a particular instance. For more information, see *Configuring different settings for an agent instance*, page 176.



DC Agent

Note: Options marked with an asterisk can be overridden externally. Click Help for details.

□ * Enable Authentication

* Password:

* TCP Port: 30600

* Diagnostic Port: 30601

Domain Controller

☑ Enable domain controller polling

* Query interval: 10 seconds

* User entry timeout: 24 hours

Workstation

☑ Enable workstation polling

User map verification interval: 15 minutes

User entry timeout: 1 hours

7. Under **DC Agent**, specify the following.

- To establish an authenticated connection between User Service and DC Agent, check **Enable Authentication**.
- If you checked **Enable Authentication**, enter a password for the authenticated connection to User Service.

✓ **Note**

This password must match the one specified earlier in the Add Transparent Identification Agent dialog box.

- **TCP Port**: Specify the port over which DC Agent connects to the Websense User Service. Normally, it is best to accept the default port (30600).
- **Diagnostic Port**: Accept the default port for DC Agent diagnostic activities (30601). This is the port over which the Websense troubleshooting tool listens for data from DC Agent.

8. Under **Domain Controller**, check **Enable domain controller polling** to enable DC Agent to query domain controllers specified in its `dc_config.txt` file for user logon sessions.

    - **Query interval**: Specify how often DC Agent queries domain controllers.

      Decreasing the query interval may provide greater accuracy in capturing logon sessions, but also increases overall network traffic. Increasing the query interval decreases network traffic, but may also delay or prevent the capture of some logon sessions. The ideal interval is typically 10 seconds (default).

    - **User Entry Timeout**: Specify how frequently DC Agent refreshes the user entries in its map resulting from domain controller polling.

> **Note**
>
> If you are using multiple DC Agents, you can configure a unique timeout for a particular Agent instance (see *Configuring different settings for an agent instance*, page 176).

9. Under **Workstation**, check **Enable workstation polling** for DC Agent to query workstations for user logon sessions. This may include particular workstations that are outside the domains already queried by DC Agent.

    - **User Map Verification Interval**: Specify how often DC Agent contacts workstations to verify which users are logged on. The ideal interval is typically 15 minutes (default).

      DC Agent compares the query results with the user name/IP address pairs in the user map it sends to Filtering Service. Decreasing this interval may provide greater user map accuracy, but increases network traffic. Increasing the interval decreases network traffic, but also may decrease accuracy.

    - **User Entry Timeout**: Specify how often DC Agent refreshes its user map. The ideal interval is typically 1 hour (default).

DC Agent removes from its map any user name/IP address entries that are older than this timeout period, and that DC Agent cannot verify against currently logged-on users. Increasing this interval may lessen user map accuracy, because the map would potentially retain old user names for a longer time. Decreasing this interval to less than the **User Map Verification Interval** value may cause problems with the expiration process. User names may be removed from the user map before they can be verified.

10. Click **OK**.

> ✓ **Note**
>
> If Websense software is not able to connect to one of the configured DC Agents, it logs a message in the Application Event Log (Windows), or in the `Websense.log` file in /`Websense/bin`/ (Solaris or Linux).

11. Click **OK** to save the changes and close the Settings dialog box.
12. To configure DC Agent to ignore logon names that are not associated with actual users, see *Configuring an Agent to ignore user names*, page 175.
13. Add the directory objects to filter individually (see *Adding directory objects*, page 114).

Websense Logon Agent

Websense Logon Agent detects users as they log on to Windows domains in your network via client machines. The Agent runs on Windows, Linux, or Solaris, and works together with the Websense User Service and Websense Filtering Service.

Logon Agent can be used with a Windows NT-based directory service or with Active Directory, which is LDAP-based. However, the associated logon application runs only on Windows-based client machines.

Using Logon Agent maximizes accuracy in identifying users as they log on to the network. While DC Agent identifies users by periodically querying domain controllers and workstations, Logon Agent identifies users in a real-time manner, as they log on to domains. This enables the Websense Filtering Service to accurately filter internet access based on policies assigned to particular users, groups, workstations or networks.

In most cases, using either DC Agent or Logon Agent is sufficient, but you can use Logon Agent in conjunction with the Websense DC Agent. In this case, Logon Agent takes precedence over DC Agent. DC Agent only communicates a logon session to Filtering Service in the unlikely event that Logon Agent has missed one.

Install Logon Agent with a typical Websense installation, and deploy the associated logon application to client machines from a central location, such as the domain controller running Logon Agent. For more information, see the installation guide.

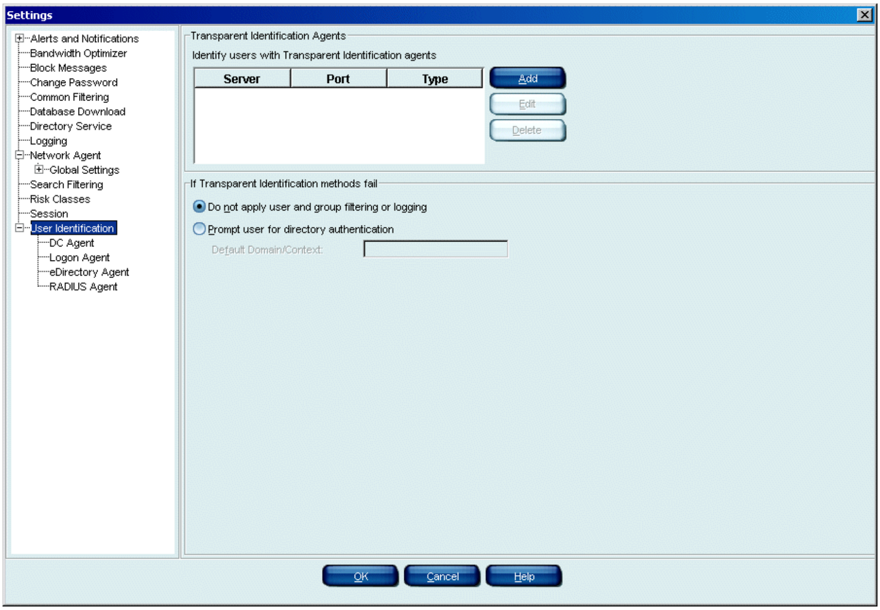
After installation, configure the Agent to communicate with client machines and with the Websense Filtering Service.

Configuring Filtering Service to communicate with Logon Agent

Logon Agent (the Websense XID Authentication Service) passes logon session information to the Websense User Service and the Websense Filtering Service, for internet request processing.

Websense software is configured to communicate with Logon Agent during installation. Verify your configuration as follows.

1. Right-click the Policy Server icon, and then select **Log On to Server**.
2. Enter the password, and then click **OK**.
3. Select **Server** > **Settings**. The Settings dialog box appears.
4. Select **User Identification** at the left. Installed agents appear in a list under **Identify users with these transparent identification agents**.



Transparent Identification Agents

Identify users with Transparent Identification agents

Server	Port	Type

If Transparent Identification methods fail

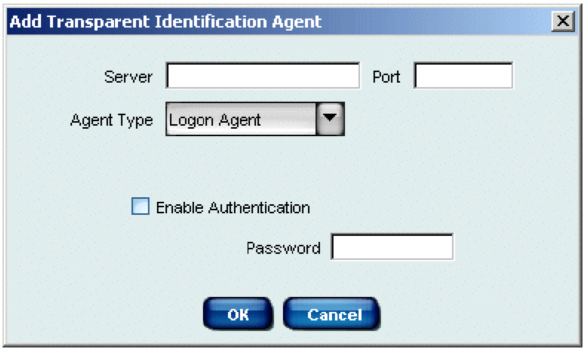
● Do not apply user and group filtering or logging

○ Prompt user for directory authentication

Default Domain/Context:

5. *If* this is a new agent instance that does not appear in the list, add the agent.

a. Click **Add**. The Add Transparent Identification Agent dialog box appears.



Agent Type: Logon Agent

□ Enable Authentication

b. Enter the following:

- **Server**: IP address or machine name of the machine where Logon Agent is installed.

Note

Machine names must start with an alphabetical character (a-z), not a numeric or special character.

Machine names containing certain extended ASCII characters may not resolve properly. If you are using a non-English version of Websense software, enter an IP address instead of a machine name.

- **Port**: Number of the port over which Filtering Service and Logon Agent communicate. The default is 30602.

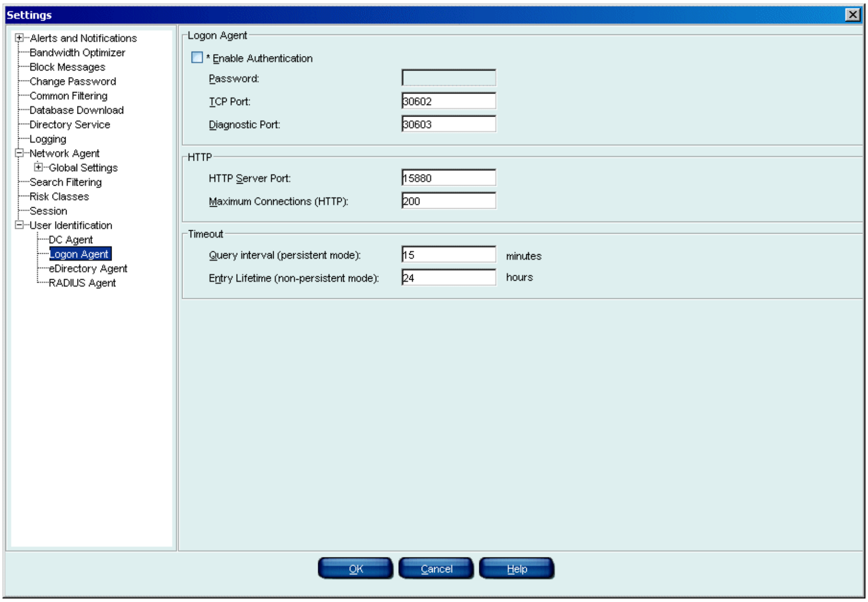
c. For **Agent Type**, select **Logon Agent**.

d. To establish an authenticated connection between Filtering Service and Logon Agent, check **Enable Authentication**.

e. If you checked **Enable Authentication**, enter a password for the authenticated connection to Logon Agent.

f. Click **OK**.

6. Expand **User Identification > Logon Agent** at the left. The Logon Agent settings are displayed.



Settings

Logon Agent

☐ * Enable Authentication

Password:

TCP Port: 30602

Diagnostic Port: 30603

HTTP

HTTP Server Port: 15880

Maximum Connections (HTTP): 200

Timeout

Query interval (persistent mode): 15 minutes

Entry Lifetime (non-persistent mode): 24 hours

7. Under **Logon Agent**, specify the following.

   - To establish an authenticated connection between Filtering Service and Logon Agent, check **Enable Authentication**.
   - If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
   - **TCP Port**: Specify the port over which Logon Agent connects to the Websense Filtering Service. Normally, Websense, Inc. recommends accepting the default port (30602).
   - **Diagnostic Port**: Accept the default port for Logon Agent diagnostic activities (30603). This is the port over which the Websense ConsoleClient troubleshooting tool listens for data from Logon Agent.

8. **Under HTTP**, specify:

   - **HTTP Server Port**: The port over which the logon application connects to Logon Agent.
   - **Maximum HTTP Connections**: The maximum number of logon application connections to Logon Agent at any one time.

If your network is large, you may need to increase this number. Note that increasing the number can increase network traffic.

9. Under **Logon Application Settings**, specify:
   - **Query Interval (persistent mode)**: The frequency at which the logon application sends logon information to the Agent. In persistent mode, the logon application communicates logon information periodically.

> **Note**
>
> If you change this value, the change does not take effect until the previous interval period has elapsed. For example, if you change the interval from 15 minutes to 5 minutes, the current 15-minute interval must end before the query starts occurring every 5 minutes.

   - **Entry Lifetime (non-persistent mode)**: How long a user entry (user name/IP address pair) remains in Logon Agent's user map before expiring. This applies only when the application is running in non-persistent mode. In this mode, logon information is sent to the Agent only once for each logon.

10. Click **OK**.

> **Note**
>
> If Websense software cannot connect to Logon Agent, it logs a message in the Application Event Log (Windows), or in the `Websense.log` file in `/Websense/bin/` (Solaris or Linux).

11. Click **OK** to close the Settings dialog box.

Next, add the directory objects to filter individually (see *Chapter 5: Clients*).

Troubleshooting DC Agent or Logon Agent

While DC Agent and Logon Agent do not have built-in troubleshooting capabilities, there are other tools available for transparent identification troubleshooting.

First, check for possible solutions (see *Chapter 10: Troubleshooting*). If user identification problems occur, check all network connections, and then check the Windows Event Viewer and the Websense Log for related error messages. If you cannot identify the cause, contact Websense Technical Support.

Note

For best results in troubleshooting RADIUS Agent or eDirectory Agent, use their built-in diagnostic capabilities. For more information, see *Troubleshooting RADIUS Agent*, page 161 or *Troubleshooting eDirectory Agent*, page 174.

Windows Services (or Service Control Manager)

Transparent identification agents, User Service, and Filtering Service run as Windows services, and are accessible from the Windows Services manager. From the Windows Control Panel, select **Administrative Tools** (Windows 2000/2003 only), and then select **Services** to open the Services manager.

Windows Event Viewer

Because it records error messages pertaining to Windows events such as service activities, the Event Viewer can help you identify network or service errors that may be causing user identification problems. To access the Event Viewer:

Windows NT: Select **Start** > **Programs** > **Administrative Tools** > **Event Viewer**. From the **Log** menu, select **Application**.

Windows 2000/2003: Select **Start** > **Programs** > **Administrative Tools** > **Event Viewer**. In the Event Viewer, click **Application Log**.

Websense log

In Windows, Solaris and Linux environments, Websense software writes errors to the `Websense.log` file in the `\Websense\bin\` directory. This error record is comparable to the Windows Event Log.

Websense Technical Support and ConsoleClient

Websense Technical Support can use the Websense ConsoleClient tool to determine the source of any problems with the transparent identification process, if other troubleshooting methods have not revealed a cause. For example, if a user is not being filtered properly, but the user name and IP address have been recorded by DC Agent and User Service, ConsoleClient can reveal data pertaining to the cause.

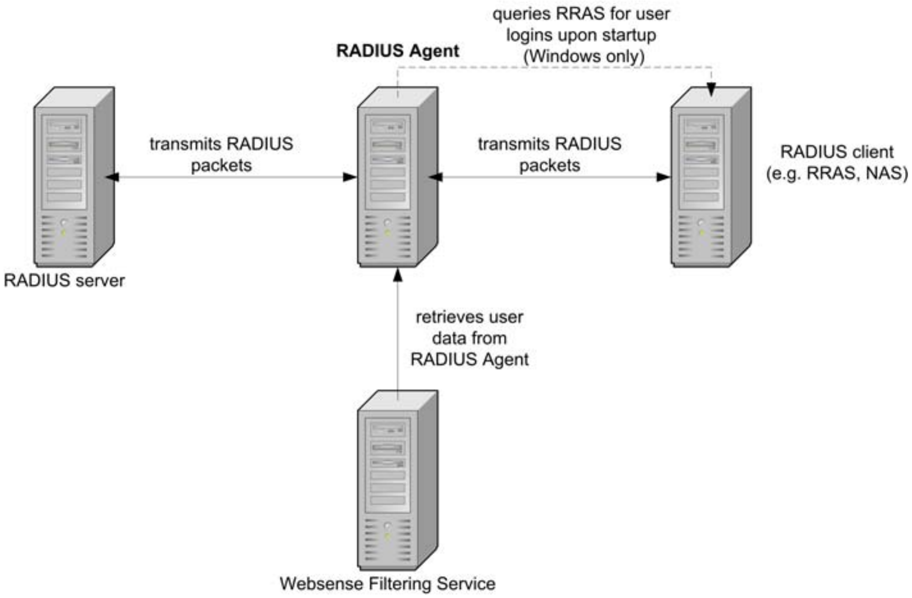
The transparent identification agents store user name-to-IP address correspondences to a user map in local memory. Analyzing the user name associations an agent has recorded helps determine whether users and workstations are being identified correctly.

For Websense Technical Support contact information, see *Websense Technical Services Support Center*, page 337.

Websense RADIUS Agent

Websense RADIUS Agent lets you integrate Websense filtering policies with authentication provided by a RADIUS server. Websense RADIUS Agent enables transparent identification of users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection (depending on your configuration).

Websense RADIUS Agent works together with the RADIUS server and RADIUS client in your network to process and track Remote Access Dial-In User Service (RADIUS) protocol traffic. This enables you to assign particular filtering policies to users or groups of users who access your network remotely, as well as to local users.



Role of RADIUS Agent in user identification

When you install RADIUS Agent, the Agent integrates with existing Websense components. However, RADIUS Agent, your RADIUS server, and your RADIUS client must be configured appropriately (see *Configuring the RADIUS environment*, page 150).

Processing RADIUS traffic

The Websense RADIUS Agent acts as a proxy that forwards RADIUS messages between a RADIUS client and a RADIUS server (or multiple clients and servers, depending on network configuration).

RADIUS Agent does not authenticate users directly. Instead, the Agent identifies remote users and associates them with IP addresses so a RADIUS server can authenticate those users. Ideally, the RADIUS server passes authentication requests to an LDAP-based directory service.

RADIUS Agent stores user name-to-IP-address pairings in a user map. If your RADIUS client supports accounting (or user logon tracking), and accounting is enabled on the client, RADIUS Agent gleans more detail about user logon sessions from the RADIUS messages it receives.

✓ **Note**

If RADIUS Agent receives a new request having an IP address already included in a user name/IP entry in its map, it *replaces* the existing pairing in its map with the new one.

When properly configured, Websense RADIUS Agent captures and processes all RADIUS protocol packets of these types:

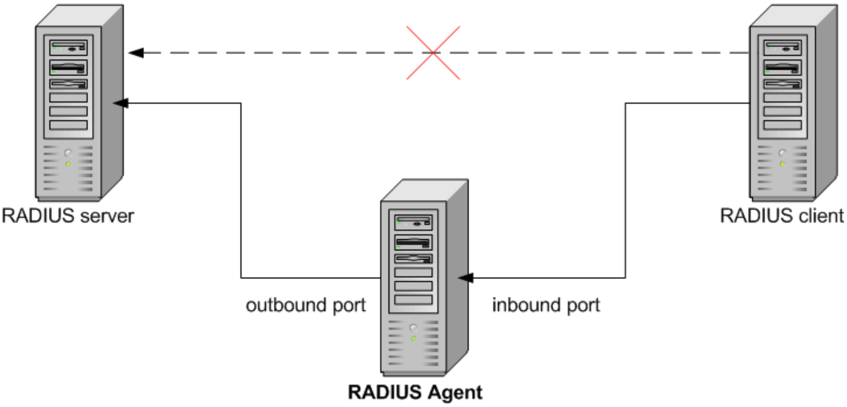
- **Access-Request**: Sent by a RADIUS client to request authorization for a network access connection attempt.
- **Access-Accept**: Sent by a RADIUS server in response to an Access-Request message; tells the RADIUS client that the attempted connection is authorized and authenticated.
- **Access-Reject**: Sent by a RADIUS server in response to an Access-Request message; tells the RADIUS client that the attempted connection is rejected.
- **Accounting-Stop-Request**: Sent by a RADIUS client to tell the RADIUS server to stop tracking user activity.

Installing RADIUS Agent

Using RADIUS Agent to identify remote users requires both a RADIUS server and a RADIUS client in your network. The RADIUS client can be a server such as a Network Attached Storage (NAS) server, or a remote access server. For more information, see the installation guide.

Configuring the RADIUS environment

Websense RADIUS Agent serves as a proxy between a RADIUS client and a RADIUS server. This diagram shows a simplified view of how using RADIUS Agent differs from a standard RADIUS setup.



RADIUS Agent as a proxy

After installing RADIUS Agent:

- Configure Websense Filtering Service to communicate with RADIUS Agent over a specified IP address and port.
- Configure RADIUS Agent to transmit authentication requests from clients to the RADIUS server. Websense, Inc. recommends that the RADIUS server pass authentication requests to an LDAP-based directory service.

- Configure your RADIUS client (typically an NAS) to communicate with RADIUS Agent instead of directly with your RADIUS server. Normally, the NAS communicates directly with a RADIUS server. Now, the NAS uses RADIUS Agent as the source of authentication and accounting requests.

  ✓ **Note**

  Websense, Inc. recommends installing and running RADIUS Agent and the RADIUS server on separate machines. (The Agent and server cannot have the same IP address, and must use different ports.)

- Configure your RADIUS server to use the Websense RADIUS Agent as a proxy (see the RADIUS server documentation). If you have multiple RADIUS servers, configure each server separately.

  ✓ **Note**

  You must configure Lucent RADIUS Server to use Password Authentication Protocol (PAP), and the RRAS server to accept only PAP requests. For more information, see the related product documentation.

Use these procedures to set up your RADIUS environment.

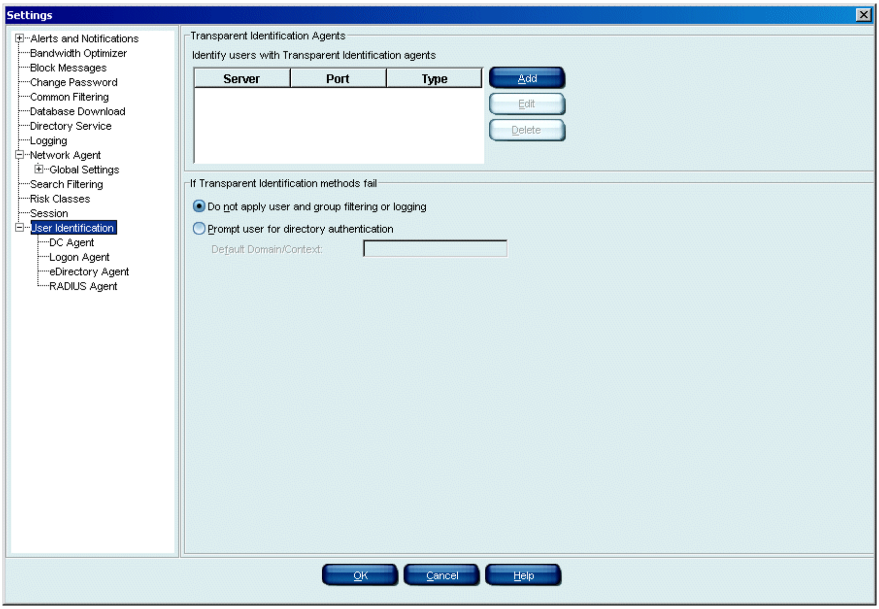
Configure RADIUS Agent and Filtering Service

Websense Filtering Service must be able to communicate with RADIUS Agent. Websense software is configured to communicate with RADIUS Agent during installation. However, Websense, Inc. recommends verifying your RADIUS Agent configuration.

> **Note**
>
> If you are using Microsoft RRAS as a RADIUS client, you must specify the RRAS machine for RADIUS Agent to query for user logon sessions. Use the procedure below.

1. Right-click the Policy Server icon, and then select **Log On to Server**.
2. Enter the password for this Policy Server, and then click **OK**.
3. Select **Server > Settings**. The Settings dialog box appears.
4. Select **User Identification** at the left.

   Installed agents appear in a list under **Identify users with these transparent identification agents**.



Transparent Identification Agents

Identify users with Transparent Identification agents

Server	Port	Type

If Transparent Identification methods fail

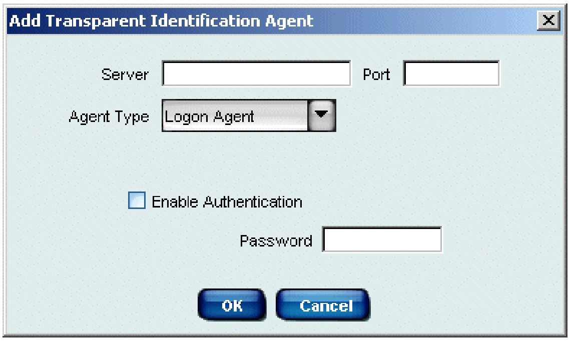
● Do not apply user and group filtering or logging

○ Prompt user for directory authentication

Default Domain/Context:

5. *If* this is a new agent instance that does not appear in the list, add the agent.

   a. Click **Add**. The Add Transparent Identification Agent dialog box appears.



Agent Type: Logon Agent

   b. For **Server**: Enter the IP address or machine name of the RADIUS Agent machine.

> **Note**
>
> Machine names containing certain extended ASCII characters may not resolve properly. If you are using a non-English version of Websense software, enter an IP address instead of a machine name.

   c. For **Port**: Enter the port number Filtering Service should use to connect to RADIUS Agent (port 30800).

> **Note**
>
> Websense, Inc. recommends using port 30800 for communication with Filtering Service. 30800 is specified for this purpose during installation.
>
> If you need to use a different port number, contact Technical Support for assistance.

   d. For **Agent Type**, select **RADIUS Agent**.

   e. To establish an authenticated connection between Filtering Service and RADIUS Agent, check **Enable Authentication**.

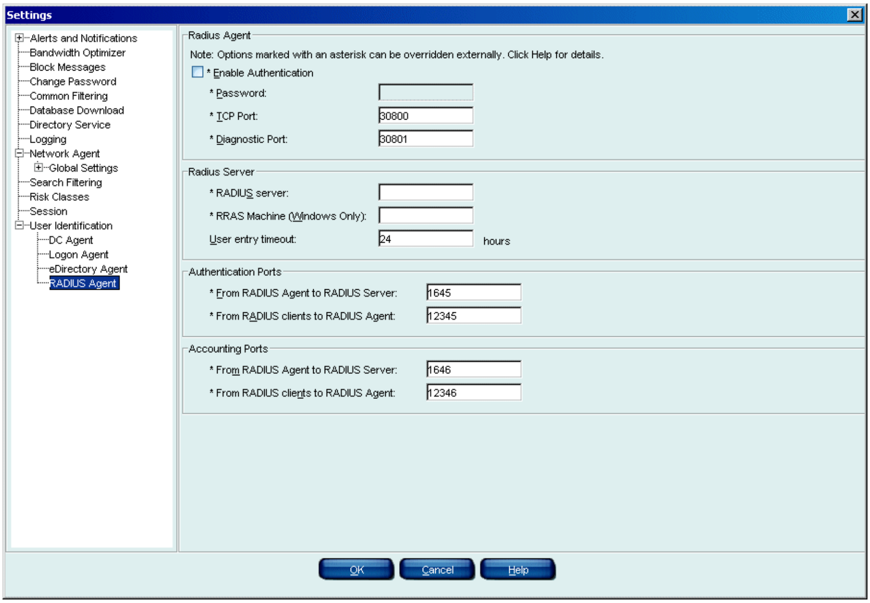
f. If you checked **Enable Authentication**, enter a password for the authenticated connection to RADIUS Agent.

g. Click **OK**.

6. Expand **User Identification** > **RADIUS Agent** at the left. The RADIUS Agent settings are displayed.

Important

These settings are global, and apply to all instances of RADIUS Agent. Fields marked with an asterisk (*) can be configured independently for a particular instance. For more information, see *Configuring different settings for an agent instance*, page 176.



Radius Agent

Note: Options marked with an asterisk can be overridden externally. Click Help for details.

□ * Enable Authentication

* Password:

* TCP Port: 30800

* Diagnostic Port: 30801

Radius Server

* RADIUS server:

* RRAS Machine (Windows Only):

User entry timeout: 24 hours

Authentication Ports

* From RADIUS Agent to RADIUS Server: 1645

* From RADIUS clients to RADIUS Agent: 12345

Accounting Ports

* From RADIUS Agent to RADIUS Server: 1646

* From RADIUS clients to RADIUS Agent: 12346

7. Specify the ports RADIUS Agent uses.
   - **TCP Port**: The port over which RADIUS Agent connects to the Websense User Service. Normally, Websense, Inc. recommends accepting the default port (30800).
   - **Diagnostic Port**: The port over which the RADIUS Agent troubleshooting tool listens for data from RADIUS Agent. Accept the default port (30801).
8. To establish an authenticated connection between User Service and RADIUS Agent, check **Enable Authentication**.
9. If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
10. Specify the following.
    - **RADIUS Server**: The IP address or name of your RADIUS server machine. RADIUS Agent forwards authentication requests to the RADIUS server, and must know the identity of this machine.
    - **RRAS Machine (Windows Only)**: If Microsoft RRAS is in use – the IP address of the machine running RRAS. Websense software queries this machine for user logon sessions.
    - **User Entry Timeout**: The interval at which RADIUS Agent refreshes its user map. Typically, the default query value (24 hours) is best.
    - **Authentication ports**: The ports over which RADIUS Agent sends and receives authentication requests.
    - **Accounting ports**: The ports over which RADIUS Agent sends and receives accounting requests.
11. Click **OK**.
12. Click **OK** to close the Settings dialog box.

Configuring RADIUS Agent to ignore user names

You can configure RADIUS Agent to ignore logon names that are not associated with actual users. For more information, see *Configuring an Agent to ignore user names*, page 175.

Configure the RADIUS client

Your RADIUS client must be configured to transmit authentication and accounting requests to the RADIUS server via the Websense RADIUS Agent.

Modify your RADIUS client configuration so that:

- The RADIUS client sends authentication requests to the machine where RADIUS Agent is installed, and to the port on which RADIUS Agent listens for authentication requests. This should be the same as the port specified during RADIUS Agent configuration (see *Configure RADIUS Agent and Filtering Service*, page 152).
- The RADIUS client sends accounting requests to the machine where RADIUS Agent is installed, and to the port on which RADIUS Agent listens for accounting requests. This should be the same as the port specified during RADIUS Agent configuration.

The procedure for configuring your RADIUS client differs depending on the type of client used. For more information, see the RADIUS client documentation.

Note

The RADIUS client should include the attributes **User-Name** and **Framed-IP-Address** in authentication and accounting messages it sends. RADIUS Agent uses the values of these attributes to interpret and store user name/ IP address pairs. If your RADIUS client does not generate this information by default, configure it to do so (see the RADIUS client documentation).

Configure the RADIUS server

To enable proper communication between Websense RADIUS Agent and your RADIUS server:

- Add the IP address of the RADIUS Agent machine to your RADIUS server's client list. This procedure depends on the type of RADIUS server in use. For instructions on modifying the client list, see the RADIUS server documentation.
- Define shared secrets between the RADIUS server and all RADIUS clients that use the Agent to communicate with the RADIUS server. The procedure for configuring shared secrets differs depending on the type of RADIUS server and client used. Shared secrets are usually specified as authentication security options.

  Configuring a shared secret for RADIUS clients and the RADIUS server provides secure transmission of RADIUS messages. Typically, the shared secret is a common text string. For more information, see the RADIUS server documentation.

The following document has details and recommendations for configuring an efficient and secure RADIUS implementation in your network. This may help determine how to configure your RADIUS server and clients, how to set up a shared secret, and more.

www.microsoft.com/windows2000/techinfo/administration/radius.asp

Note

The RADIUS server should include the attributes **User-Name** and **Framed-IP-Address** in authentication and accounting messages. RADIUS Agent uses the values of these attributes to interpret and store user name/IP address pairs. If your RADIUS server does not generate this information by default, configure it to do so (see the RADIUS server documentation).

Starting and stopping RADIUS Agent

After you have installed RADIUS Agent, follow the appropriate steps to start it. Your method of starting the Agent depends on the installation method used.

Starting in console mode

To start the Agent in console mode (as an application):

1. At the prompt, type:

   Windows: `RadiusAgent.exe -c`

   Linux/Solaris: `RadiusAgent -c`

   and then press **Enter.**

2. To stop the Agent at any time, press **Enter** again. It may take a couple of seconds for the Agent to stop running.

For command attribute descriptions, see *Command attributes*, page 160.

Starting in service mode (Windows)

To start the Agent in console mode (as an application):

1. Open the Windows Services dialog box: Select **Start** > **Programs** > **Administrative Tools**, and then double-click **Services**.
2. Right-click **Websense RADIUS Agent**, and then select **Start**.

> ✓ **Note**
>
> Do not start the RADIUS Agent service while the RADIUS server is down.

Starting in daemon Mode (Linux/Solaris)

To start RADIUS Agent as a daemon, type at a command prompt:

```
WebsenseAdmin start
```

and then press **Enter**.

This starts any installed Websense services that were not already running.

For command attribute descriptions, see *Command attributes*, page 160.

Stopping RADIUS Agent

Use the methods here to stop RADIUS Agent.

> **Note**
>
> User authentication does not occur while RADIUS Agent and the RADIUS server are down.

If you are running RADIUS Agent in console mode, press **Enter** at any time to stop the Agent.

If you are running RADIUS Agent in service/daemon mode, stop the Agent as follows:

Windows:

1. Open the Windows Services dialog box.
2. Right-click **Websense RADIUS Agent**, and then select **Stop**.

Linux/Solaris:

1. At the prompt, type:

   ```
   WebsenseAdmin stop
   ```

   > **Note**
   >
   > This command stops any Websense services running on this machine.

2. Press **Enter**.

Websense RADIUS Agent service is stopped.

Command attributes

The table describes the available command attributes for RADIUS Agent.

✓ **Note**

On Linux/Solaris, Websense, Inc. recommends using the script provided to start or stop Websense RADIUS Agent (**`WsRADIUSAgent start|stop`**), instead of the **`-r`** and **`-s`** command parameters.

Parameter	Description
`-i`	Installs RADIUS Agent service/daemon.
`-r`	Runs RADIUS Agent service/daemon.
`-s`	Stops RADIUS Agent service/daemon.
`-c`	Runs RADIUS Agent as an application process instead of as a service or daemon. When in console mode, RADIUS Agent can be configured to send log output to the console or to a text file.
`-v`	Displays the version number of RADIUS Agent.

`-?`
`-h`
`-help`
`<no option>`
	Displays usage information on the command line. Lists and describes all possible command line parameters.

Troubleshooting RADIUS Agent

RADIUS Agent has built-in diagnostic capabilities, but these are not activated by default. To activate RADIUS Agent logging and debugging:

1. Stop the RADIUS Agent service (see *Starting and stopping RADIUS Agent*, page 158).
2. On the RADIUS Agent machine, go to the RADIUS Agent installation directory (`\Websense\bin\`).
3. Open the file `wsradius.ini` in a text editor.
4. Locate the section named *`[RADIUSAgent]`*.
5. Change the line

   ```
   DebugMode=Off
   ```

   to

   ```
   DebugMode=On
   ```

   This enables logging and debugging.
6. Modify the line

   ```
   DebugLevel=N
   ```

   where `N` is the level of message verbosity (`1` indicates less detail, `3` indicates the most detail).
7. Modify the line

   ```
   LogFile=[filename.txt]
   ```

   where `[filename.txt]` is the log output file. By default, log output is sent to the RADIUS Agent console. If you are running the Agent in console mode, you can optionally keep this default value.
8. Save and close the `wsradius.ini` file.
9. Start the RADIUS Agent service (see *Starting and stopping RADIUS Agent*, page 158).

If remote users are not being identified and filtered as expected, the likely cause is communication problems between RADIUS Agent and your RADIUS server. Check your RADIUS Agent logs for errors to determine the cause.

For more information, see *Chapter 10: Troubleshooting*. Also visit the Websense Knowledge Base. Go to at www.websense.com, and then navigate to the Support & Knowledge Base page.

Websense eDirectory Agent

Websense eDirectory Agent works together with Novell eDirectory to transparently identify users so Websense software can filter them according to policies assigned to users or groups.

When you install eDirectory Agent, the Agent integrates with existing Websense components. However, some configuration is required to ensure that eDirectory Agent and Novell eDirectory are communicating properly. For more information, see *Configuring the eDirectory environment*, page 164.

eDirectory Agent does not authenticate users directly. Instead, the Agent gathers user logon session information from Novell eDirectory, which authenticates users logging on to the network.

Websense eDirectory Agent associates each authenticated user with an IP address, and records user name-to-IP-address pairings to a local user map. With the help of Websense User Service, eDirectory Agent supplies this information to Websense Filtering Service.

✓ **Note**

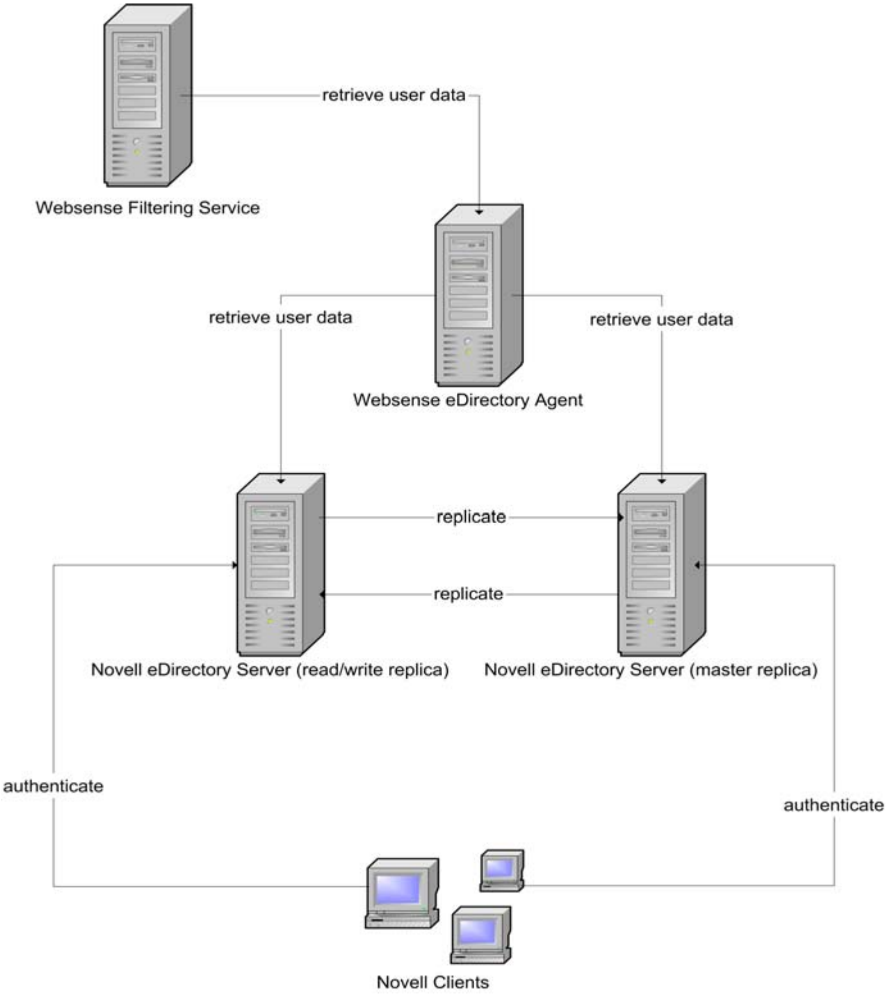
From a Novell Client running Windows, multiple users can log on to 1 Novell eDirectory server. This associates 1 IP address with multiple users. In this scenario, eDirectory Agent’s user map only retains the user name/IP address pairing for the *last* user logged on from a given IP address.

One instance of Websense eDirectory Agent can support 1 Novell eDirectory master, plus any number of Novell eDirectory replicas.

Following is an illustration of how eDirectory Agent works in conjunction with a Novell eDirectory master and replica.

✓ **Note**

Websense, Inc. does not support using Websense eDirectory Agent together with Websense DC Agent.


retrieve user data
Websense Filtering Service
retrieve user data
retrieve user data
Websense eDirectory Agent
replicate
replicate
Novell eDirectory Server (read/write replica)
Novell eDirectory Server (master replica)
authenticate
authenticate
Novell Clients

eDirectory Agent working with eDirectory master and replica

Configuring the eDirectory environment

Websense eDirectory Agent queries Novell eDirectory for user logon session information at a given interval. Specify certain network parameters so Websense eDirectory Agent can get user logon information from Novell eDirectory.

After installing Websense eDirectory Agent, do the following.

Configure Novell eDirectory

The location of Novell eDirectory is specified during installation of Websense eDirectory Agent. If you are using multiple Novell eDirectory replicas, ensure that you have specified the server where each replica is running. For more information, see *Configuring a multiple-replica environment*, page 171.

Note

If you have integrated Cisco Content Engine v5.3.1.5 or higher with Websense software:

- Run the following Websense services on the same machine as Websense and Cisco Content Engine:

  Websense eDirectory Agent
  Websense User Service
  Websense Filtering Service
  Websense Policy Server

- Ensure that all Novell eDirectory replicas are added to the `wsedir.ini` file on the same machine.
- Delete the `eDirAgent.bak` file.
- Run Websense Reporting Tools services on a machine *separate* from Cisco Content Engine and Websense software.

Websense software now supports using NMAS with Websense eDirectory Agent. Disabling NMAS is not necessary.

✓ **Note**

To use eDirectory Agent with NMAS enabled, eDirectory Agent must be installed on a machine that is also running the Novell Client for Windows NT/2000/XP.

For information about installing the Novell Client software, see the Novell documentation. For supported versions of the software, see the Websense installation guide.

Determine the eDirectory Agent protocol

Websense eDirectory Agent can use Netware Core Protocol (NCP) or Lightweight Directory Access Protocol (LDAP) to get user logon information from Novell eDirectory, depending on your configuration. By default, eDirectory Agent on Windows uses NCP. eDirectory Agent on Linux or Solaris must use LDAP.

If you are running eDirectory Agent on Windows, but still want the Agent to use LDAP to query Novell eDirectory, set the Agent to use LDAP instead of NCP. Generally, NCP provides a more efficient query mechanism. However, if your environment supports LDAP (for example, you have rules on a firewall that allow LDAP but not other protocols), you may want to continue using LDAP.

To set Websense eDirectory Agent on Windows to use LDAP instead of NCP:

1. Ensure that you have at least 1 Novell eDirectory replica containing all directory objects to monitor and filter in your network.
2. Stop the Websense eDirectory Agent service, using the **Services** applet accessible via **Control Panel** (*Windows NT*) or **Administrative Tools** (*Windows 200x*).

3. Go to the eDirectory Agent installation directory, and locate the text file named `wsedir.ini`.
4. Open the file in a text editor.
5. Modify this line as indicated:

   ```
   QueryMethod=0
   ```

   where 0 sets the Agent to use LDAP to query Novell eDirectory. (The default value of 1 tells Novell eDirectory Agent to use NCP.)
6. Save and close the file when all entries are complete.
7. Restart the Websense eDirectory Agent service.

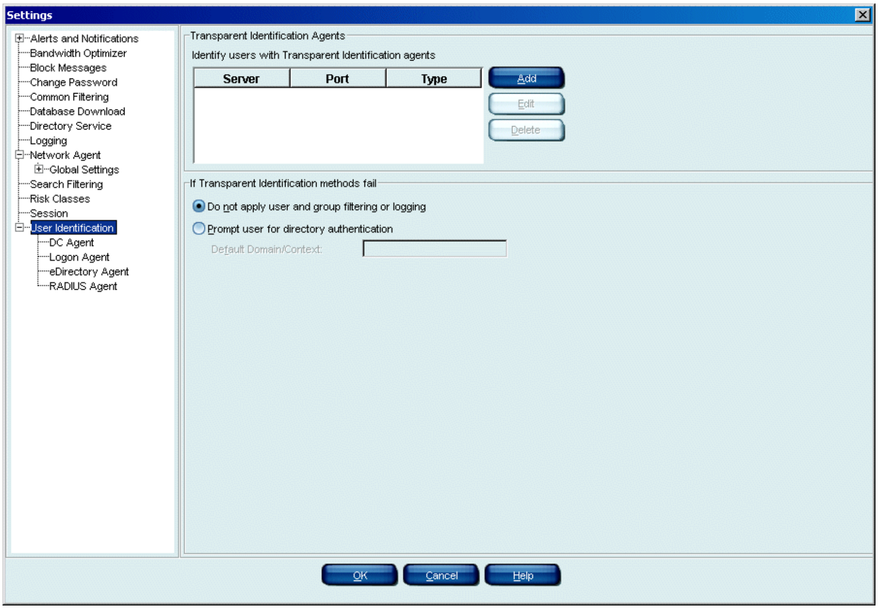
Configure eDirectory Agent and Filtering Service

Websense software was configured to communicate with eDirectory Agent during installation. Verify your configuration as follows.

1. Right-click the Policy Server icon, and then select **Log On to Server**.
2. Enter the password for this Policy Server, and then click **OK**.
3. Select **Server** > **Settings**. The Settings dialog box appears.

4. Select **User Identification** at the left.

   Installed agents appear in a list under **Identify users with these transparent identification agents**.



Identify users with Transparent Identification agents

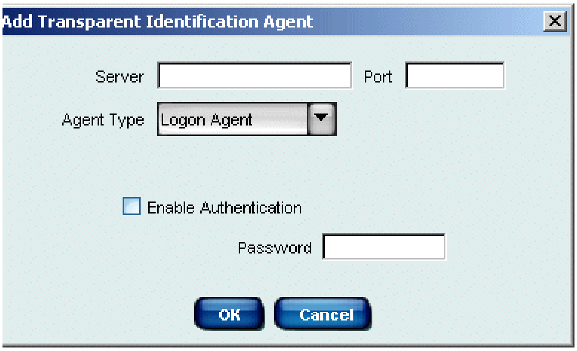
Server	Port	Type

● Do not apply user and group filtering or logging

○ Prompt user for directory authentication

5. *If* this is a new agent instance that does not appear in the list, add the agent as follows.

   a. Click **Add**. The Add Transparent Identification Agent dialog box appears.



Agent Type: Logon Agent

□ Enable Authentication

b. For **Server**, enter the IP address or machine name of the eDirectory Agent machine.

> ✓ **Note**
>
> Machine names containing certain extended ASCII characters may not resolve properly. If you are using a non-English version of Websense software, enter an IP address instead of a machine name.

c. For **Port**, enter the port number Filtering Service should use to connect to eDirectory Agent (port 30700).

> ✓ **Note**
>
> Websense, Inc. recommends using port 30700 for communication with Filtering Service. 30700 is specified for this purpose during installation.
>
> If you need to use a port other than 30700, contact Technical Support for assistance.

d. For **Agent Type**, select **eDirectory Agent**.

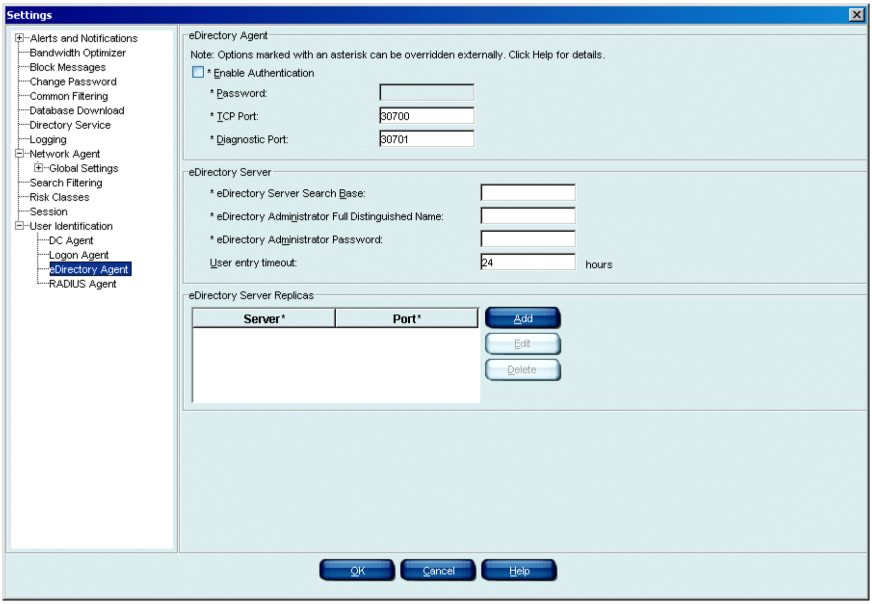
e. To establish an authenticated connection between Filtering Service and eDirectory Agent, check **Enable Authentication**.

f. If you checked **Enable Authentication**, enter a password for the authenticated connection to eDirectory Agent.

g. Click **OK**.

6. Expand **User Identification > eDirectory Agent** at the left. The eDirectory Agent user identification settings are displayed.

> **Note**
>
> These settings are global, and apply to all instances of eDirectory Agent. Fields marked with an asterisk (*) can be configured independently for a particular instance. For more information, see *Configuring different settings for an agent instance*, page 176.



eDirectory Agent

Note: Options marked with an asterisk can be overridden externally. Click Help for details.

□ * Enable Authentication

* Password:

* TCP Port: 30700

* Diagnostic Port: 30701

eDirectory Server

* eDirectory Server Search Base:

* eDirectory Administrator Full Distinguished Name:

* eDirectory Administrator Password:

User entry timeout: 24 hours

eDirectory Server Replicas

Server*	Port*

7. Under **eDirectory Agent Settings**, specify:
   - **TCP Port**: The port over which eDirectory Agent connects to the Websense User Service. Normally, Websense, Inc. recommends accepting the default port (30700).
   - **Diagnostic Port**: The port over which the eDirectory Agent troubleshooting tool listens for data from eDirectory Agent. Accept the default port (30701).

8. To establish an authenticated connection between Filtering Service and eDirectory Agent, check **Enable Authentication**.

9. If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
10. Under **eDirectory Server Settings**, specify:
    - **eDirectory Server Search Base**: The root context in your Novell eDirectory server.
    - **eDirectory Administrator Fully Distinguished Name**: The name of the administrative user for Novell eDirectory server.
    - **eDirectory Administrator Password**: The password for the Novell eDirectory server administrative user.
    - **User Entry Timeout**: How long entries remain in the Agent's user map. Websense, Inc. recommends using an interval 30 percent longer than a typical user logon session. This helps prevent user entries from being removed from the map before users are done browsing. If this value is set too low, a removed user could be filtered incorrectly until the next workstation poll occurs.
11. Click **OK** to close the Settings dialog box.

Configuring eDirectory Agent to ignore user names

You can configure eDirectory Agent to ignore logon names that are not associated with actual users. For more information, see *Configuring an Agent to ignore user names*, page 175.

Configuring a multiple-replica environment

One instance of the Websense eDirectory Agent can support 1 Novell eDirectory master, plus any number of Novell eDirectory replicas running on separate machines.

eDirectory Agent must be able to communicate with each machine running a replica of the directory service. This ensures that the Agent gets the latest logon information as quickly as possible, and does not wait for eDirectory replication to occur.

Novell eDirectory replicates the attribute that uniquely identifies logged-on users only every 5 minutes. Despite this replication time lag, eDirectory Agent picks up new logon sessions as soon as a user logs on to any eDirectory replica.

Initially, you specify Novell eDirectory server names or IP addresses during eDirectory Agent installation. If you set up additional replicas or remove old ones, update the eDirectory Agent configuration:

1. Stop the eDirectory Agent service (see *Starting and stopping eDirectory Agent*, page 172).
2. Add each eDirectory replica to Websense Manager (see *Configure eDirectory Agent and Filtering Service*, page 166, Step 5).
3. Start eDirectory Agent (see *Starting and stopping eDirectory Agent*, page 172).

Starting and stopping eDirectory Agent

Use the procedures below to start or stop the Agent. Your method of starting the Agent depends on the installation method used. For more information, see the installation guide.

> ✓ **Note**
>
> Be sure the eDirectory server is running before starting eDirectory Agent.

Starting in console mode

To start the Agent in console mode (as an application):

1. At the prompt, type:

   Windows: `eDirectoryAgent.exe -c`

   Linux/Solaris: `eDirectoryAgent -c`

   and then press **Enter.**

2. To stop the Agent immediately, press **Enter** again. It may take a couple of seconds for the Agent to stop running.

Starting in service mode (Windows)

1. Open the Windows Services dialog box: Select **Start** > **Programs** > **Administrative Tools**, and then double-click **Services**.
2. Right-click **Websense eDirectory Agent**, and then select **Start**.

Starting in daemon mode (Linux/Solaris)

Type at a command prompt:

```
WebsenseAdmin start
```

and then press **Enter**.

Stopping eDirectory Agent

Use these methods to stop eDirectory Agent.

Console mode

Press **Enter** at a command prompt (in the console window where you started the Agent) to stop the Agent.

Service/daemon mode

Windows:

1. Open the Windows Services dialog box.
2. Right-click `Websense eDirectory Agent`, and then select **Stop**.

Linux/Solaris:

1. At the prompt, type:

   WebsenseAdmin stop

   > ✓ **Note**
   > Using this command stops any Websense services running on this machine.

2. Press **Enter**.

Troubleshooting eDirectory Agent

eDirectory Agent has built-in diagnostic capabilities, but these are not activated by default. You can enable logging and debugging during installation, or at any other time.

1. Stop eDirectory Agent (see *Starting and stopping eDirectory Agent*, page 172).
2. On the eDirectory Agent machine, go to the eDirectory Agent installation directory.
3. Open the file `wsedir.ini` in a text editor.
4. Locate the section named `[eDirAgent]`.
5. Change the line

   ```
   DebugMode=Off
   ```

   to

   ```
   DebugMode=On
   ```

   This enables logging and debugging.
6. Modify the line

   ```
   DebugLevel=N
   ```

   where `N` is the level of message verbosity (0-3, where `1` indicates the least detail, and `3` indicates the most detail).
7. Modify the line

   ```
   LogFile=[filename.txt]
   ```

   where `[filename.txt]` is the log output file. By default, log output is sent to the eDirectory Agent console. If you are running the Agent in console mode, you can keep this default value.
8. Save and close the `wsedir.ini` file.
9. Start the eDirectory Agent service (see *Starting and stopping eDirectory Agent*, page 172).

Configuring an Agent to ignore user names

You can configure a transparent identification Agent to ignore logon names that are not associated with actual users. Some Windows 200x and XP services contact domain controllers using the workstation identities of active users in your network.

For example, while **workstationA/user1** is logged on to the network and is filtered by a Websense policy assigned to **user1**, a service starts up on that user's machine. The service assumes the identity **workstationA/ServiceName** to contact the domain controller. This can cause filtering problems, because Websense software treats **workstationA/ServiceName** as a new user with no policy assigned, and filters this user by the workstation policy, or by the **Global** policy.

1. Stop the Agent service (see *Starting and stopping eDirectory Agent*, page 172 for an example).
2. Go to the `\Websense\bin\` directory, and locate the text file named `ignore.txt`.
3. Open the file in a text editor.
4. Type a 1-line entry for each user name to be ignored. Websense software ignores user names listed this way, regardless of the associated workstation. Do not use wildcard characters, such as “*”.

   In this example:

   ```
   johnsmith
   aperez, enggroup1
   ```

   The user name **`johnsmith`** is ignored for ALL workstations. The user name **`aperez`** is ignored only for the domain **`enggroup1`**.
5. Save and close the file when all entries are complete.
6. Restart the Agent service.

The Agent ignores the user names you have specified, and Websense software does not consider these names in filtering.

Configuring different settings for an agent instance

The transparent identification agent configuration settings in Websense Manager are global, and apply to all instances of the agent you have installed. However, if you have multiple instances of DC Agent, eDirectory Agent or RADIUS Agent, you can configure one instance independently of the others.

Unique settings you specify for a particular agent instance override the global settings in the Settings dialog box. Settings that can be overridden are marked with an asterisk (*).

1. Stop all Websense services (see *Stopping or starting Websense services*, page 191). Be sure to include the transparent identification agent service (see *Starting and stopping eDirectory Agent*, page 172 for an example).
2. On the machine running the agent instance, go to the agent installation directory.
3. Open the appropriate file in a text editor:
   - for DC Agent: `transid.ini`
   - for eDirectory Agent: `wsedir.ini`
   - for RADIUS Agent: `wsradius.ini`
4. Locate the parameter to change for this agent instance (see *.ini parameter to field name correspondences*, page 178).

   For example, you can enable an authenticated connection between this agent instance and the Websense Filtering Service. To do this, you would specify a password value in the .ini file:

   ```
   password=[xxxxxx]
   ```
5. Modify any other values as desired.
6. Save and close the .ini file.
7. If you made a change to *DC Agent* settings, remove these files from the DC Agent installation directory:
   - `Journal.dat`
   - `XidDcAgent.bak`

   These files will be recreated when you start the Websense DC Agent service.
8. Update the agent settings.
   a. In Websense Manager, select **Server** > **Settings**.

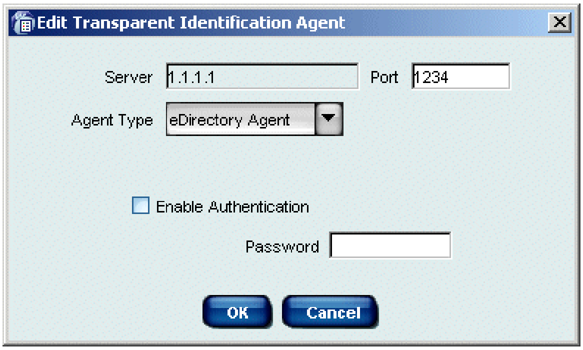
b. Select **User Identification** at the left.

c. Under **Identify users with these transparent identification agents**, select the agent and then click **Edit**.

The Edit Transparent Identification Agent dialog box appears.

Note

If you modified the `port` value for this agent instance (equivalent to the **TCP Port** in the Settings dialog box), remove and then re-add the agent. To remove the agent, select the agent and then click **Delete**. Click **Add** to add the agent instance again.



Server: 1.1.1.1
Port: 1234
Agent Type: eDirectory Agent
□ Enable Authentication
Password:

d. Enter the **Server** and **Port** this agent instance uses. If you specified a unique port number in the .ini file, ensure that your entry matches that value.

e. To use an authenticated connection between this agent instance and Filtering Service, check **Enable Authentication**, and specify a **Password**.

If you specified a unique authentication password in the .ini file, ensure that your entry here matches that password.

f. Click **OK**.

g. Click **OK** in the Settings dialog box.

h. Click **Done** to save your changes and close the Settings dialog box.

9. Start all Websense services (see *Stopping or starting Websense services*, page 191).

.ini parameter to field name correspondences

Websense Manager field label	**.ini parameter name**	**Description**
TCP Port *(all agents)*	port	The port over which the agent connects to the Websense User Service.
Diagnostic Port *(all agents)*	DiagServerPort	The port over which the eDirectory Agent or RADIUS Agent troubleshooting tool, or the Websense ConsoleClient tool, listens for data from the agent.
Password *(all agents)*	password	The password the agent uses to authenticate the Websense User Service when it contacts the agent. Specifying this password enables authentication.
Query interval *(DC Agent)*	QueryInterval	The interval at which DC Agent queries domain controllers.
Server, Port *(eDirectory Agent)*	Server=IP:port	The IP address and port number of the machine running eDirectory Agent.
eDirectory Server Search Base	SearchBase	The root context of the Novell eDirectory server.
eDirectory Administrator Fully Distinguished Name	DN	The name of the administrative user for Novell eDirectory server.
eDirectory Administrator Password	PW	The password for the Novell eDirectory server administrative user.
RADIUS server	RADIUSHost	The IP address or name of your RADIUS server machine.
RRAS Machine (Windows Only)	RRASHost	The IP address of the machine running RRAS. Websense queries this machine for user logon sessions.
From RADIUS Agent to RADIUS Server	AuthOutPort	The port on which the RADIUS server listens for authentication requests.

From RADIUS clients to RADIUS Agent	AuthInPort	The port over which RADIUS Agent accepts authentication requests.
From RADIUS Agent to RADIUS server	AccOutPort	The port over which the RADIUS server listens for RADIUS accounting messages.
From RADIUS clients to RADIUS Agent	AccInPort	The port over which RADIUS Agent accepts accounting requests.

Manual authentication

Sometimes a Websense transparent identification agent cannot identify users, such as when a user logs on before the agent is started, or the agent is otherwise not able to send user information to User Service. In these cases, or when an agent is not installed, you can still filter based on directory object policies.

Manual authentication prompts users for a user name and password the first time they access the internet through a newly-opened browser. Websense software then confirms the password with a Windows- or LDAP-based directory service, and retrieves information for that user.

When manual authentication is enabled, users are prompted to authenticate only if Websense software is not able to identify them transparently by receiving information from a transparent identification agent or from an integration product.

Users who cannot be identified through transparent or manual authentication (or users sharing a computer such as in a Windows Terminal Services) are filtered by workstation or network policies, or by the **Global** policy. Users on shared machines cannot be filtered by policies assigned to directory objects.

When manual authentication is enabled, users may not be able to access the internet and are presented with HTTP errors when:

- The user's password fails after 3 attempts to enter a password. This occurs when the password is invalid.
- The user clicks **Cancel** to bypass the authentication prompt.

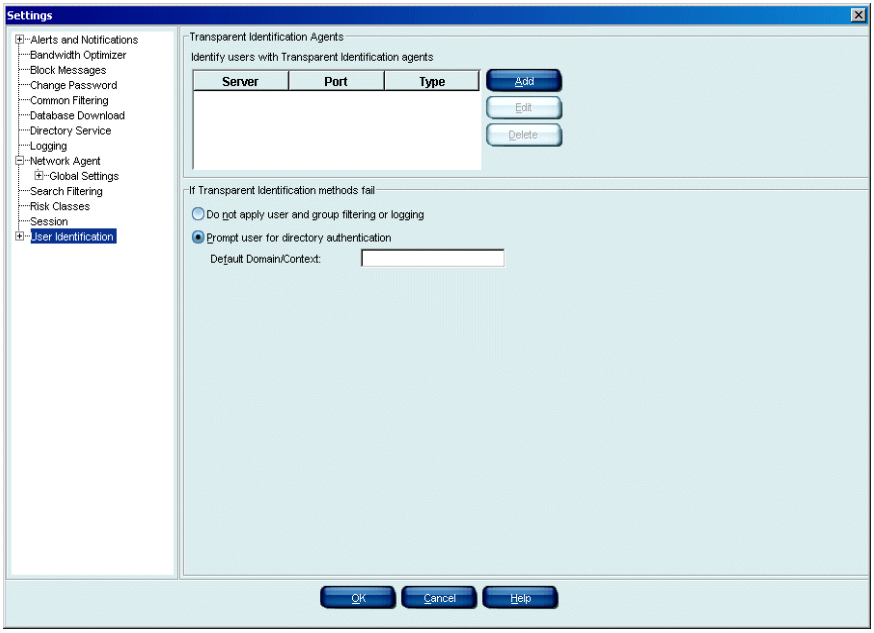
To ensure passwords and other client information are secure, optionally enable SSL encryption with manual authentication. For more information, see *Secure manual authentication*, page 182.

Enabling Websense manual authentication

1. Right-click the Policy Server icon, and then select **Log On to Server**.
2. Enter the password that was established when Policy Server was first connected, and then click **OK**.
3. Add the directory objects to filter individually (see *Manual authentication*, page 180).
4. Select **Server** > **Settings**. The Settings dialog box appears.
5. Select **User Identification** at the left. The user identification settings are displayed.
6. Select **Prompt user for directory authentication**.

Note

If you select **Prompt user for directory authentication**, you must enable Anonymous authentication within Microsoft Proxy Server. If Basic or NT Challenge/ Response authentication is enabled in Microsoft Proxy Server, do not select this option.



Transparent Identification Agents

Identify users with Transparent Identification agents

Server	Port	Type

If Transparent Identification methods fail

○ Do not apply user and group filtering or logging

● Prompt user for directory authentication

Default Domain/Context:

7. If Websense software is not installed in the same domain or context as most users, enter the default domain or context within the directory where your directory objects reside (for example, company/server1). Otherwise, leave the **Default Domain/Context** field blank.
8. Click **OK**.

Secure manual authentication

Websense secure manual authentication uses Secure Sockets Layer (SSL) encryption to protect authentication data being transmitted between client machines and Websense software. An SSL server built into the Websense Filtering Service provides encryption of user names and passwords transmitted between client machines and the Websense Filtering Service.

By default, secure manual authentication is disabled. To enable this functionality, install SSL certificates and keys as required in your environment. Certificates and keys must be in a location Websense software can access, be readable by the Websense Filtering Service, and be in PEM file format.

✓ **Note**

Secure manual authentication is not supported with Remote Filtering.

- Obtain and install client (user) certificates. A certificate consists of a public and a private key. The public key encrypts data, and the private key deciphers it.

  The Certificate Authority (CA) issuing the client certificate must be trusted by Websense. Typically, this is determined by a browser setting. You can generate a certificate from an internal certificate server, or obtain a client certificate from any third-party CA, such as VeriSign.
- Distribute client certificates to client workstations. The certificates on client machines can also prevent browser security warnings from appearing when users browse from secure to non-secure sites.
- Configure Websense software to access your certificates and keys (see *Activating secure manual authentication*, page 183).

Activating secure manual authentication

1. Go to the Websense installation directory on the machine running the Websense Filtering Service.
2. Stop the Websense Filtering Service.
3. Locate the file `eimserver.ini` (in `/Websense/bin/` by default).
4. Open the file in a text editor.
5. Locate the section named `[WebsenseServer]`.
6. Add the line:

   ```
   SSLManualAuth=on
   ```
7. Just below the previous line, add the following:

   ```
   SSLCertFileLoc=[path]
   ```

   where [path] is the location of your SSL certificate, including certificate filename. For example: `C:\secmanauth\certfile.pem`
8. Add the line:

   ```
   SSLKeyFileLoc=[path]
   ```

   where [path] is the location of your SSL key, including key filename. For example: `C:\secmanauth\key.pem`
9. Save and close the file.
10. Start the Websense Filtering Service.
11. Follow the instructions below to add secure communication between Websense software and your directory service.

Secure communication with directory service

Secure manual authentication provides encryption of user names and passwords transmitted between client machines and Filtering Service.

To ensure security over the *entire path* traversed by the user name and password, you must take another step.

You must configure your directory service to use SSL. This establishes secure communication between Websense software and your directory service.

To enable the SSL option with the directory service, open Websense Manager and select **Server** > **Settings** > **Directory Service** > **Advanced**, and then select **Use SSL**. Click **OK** to save your changes.

CHAPTER 7 Server Administration

Websense Filtering Service interacts with Network Agent or your integration product to provide internet filtering. Site requests are received by your integration product and sent to Filtering Service for processing.

Policy Server stores Websense configuration data (including filtering policy settings), and communicates configuration data to Filtering Service.

To configure Policy Server:

1. Add Policy Server to Websense Manager, so the components can communicate (see *Adding a server*, page 186).
2. Log on to Policy Server and configure server settings.

One or more Policy Servers can be configured from the same instance of Websense Manager. Each Policy Server stores data for all Filtering Services connected to it. In a large organization, it may help to install multiple instances of Policy Server for load-balancing purposes.

If your organization includes multiple administrators (whether you have 1 or several Policy Servers), the Distributed Administration and Reporting feature allows highly flexible management of clients and filtering settings. It also lets you distribute configuration settings to multiple servers from a central location. This feature is only available with Corporate Editions of Websense. For more information, see *Delegated Administration*, page 215.

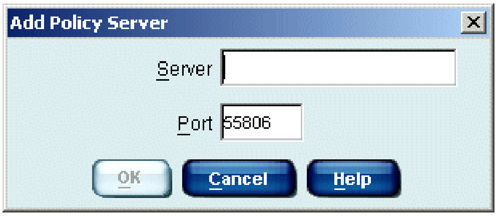
If you are not running Corporate Edition, you can still distribute Websense configuration data to multiple Policy Servers. For more information, see *Distributing policies to multiple servers*, page 306.

Adding a server

Policy Server cannot be configured until it is added via Websense Manager. To add Policy Server, you need the IP address or name of the Policy Server machine, which may or may not be the same machine where Websense Manager is installed.

1. Right-click in the navigation tree, and then select **Add Policy Server**.

   The Add Policy Server dialog box appears.



Add Policy Server

Server

Port 55806

2. Enter the IP address or name of the Policy Server machine in the **Server** field.
3. Enter the **Port** number for sending configuration information to Policy Server (default is 55806). This is the configuration port set during installation.
4. Click **OK**. A server icon with the IP address or machine name appears in the navigation tree.

Now you can log on to Policy Server and configure it, or add instances of Policy Server. Each Policy Server must be added and configured separately.

Logging on to a server

After adding a Policy Server, log on to it so you can configure server settings and begin filtering users.

1. Double-click the Policy Server icon in the navigation tree. The Set Websense Password dialog box appears.
2. Enter a password in the **New Password** field. Type it again in the **Confirm Password** field.

   On subsequent logons, enter your password to connect Websense Manager to the Server. You can change your password as described under *Changing the Policy Server password*, page 188.

> **Important**
>
> *Corporate Edition users:* Websense, Inc. recommends using your administrative network credentials as the Websense administrative user name and password.

3. Click **OK**. A topic list appears under the server icon in the navigation tree.

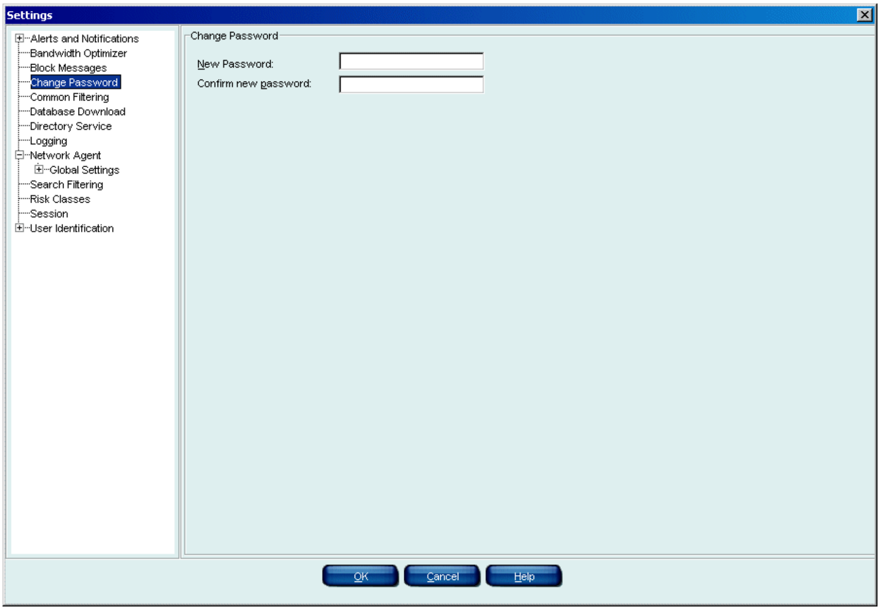
The IP address or machine name appears as the active **Policy Server** at the top of the navigation tree. If you are logged on to multiple instances of Policy Server at the same time, the IP addresses or machine names of all Policy Servers are displayed.

> **Note**
>
> It is not possible to connect multiple instances of Websense Manager simultaneously to the same Policy Server. This prevents configuration changes from being overwritten.

Changing the Policy Server password

You can change the administrative password used for Policy Server at any time. This password is also required for access to Websense Reporting Tools.

1. Select **Server** > **Settings**.
2. Select **Change Password** at the left. The **Change Password** settings are displayed.



3. Enter the password to use for Policy Server in the **New Password** field. The password is case-sensitive.
4. Re-type the new password to confirm it.
5. Click **OK**.

Configuring a server

Administrative options for running Policy Server are accessed via the **Server** > **Settings** command. If your network includes multiple Policy Servers, each must be configured separately.

The Settings dialog box contains settings for the following Websense features and operations.

- **Database Download**: Enter the Websense subscription key, set up server authentication and upstream proxy information if needed, and schedule days and times for downloading the Master Database (see *Setting the download schedule*, page 60).

  If you have purchased Websense Real-Time Security Updates, enable updates here (see *Websense Real-Time Security Updates™*, page 71).
- **Alerts and Notifications**: Configure settings for receiving Websense administrative alerts (see *Alerting*, page 199).
- **Logging**: Define the location of Log Server, installed with Reporter. Log Server must be installed before Websense software can log user requests (see *Logging and Reporting*, page 74).
- **Block Messages**: Customize the message displayed when Websense software blocks a requested site (see *Customized block messages*, page 52).
- **Directory Service**: Configure Websense software to access directory objects in your network (see *Manual authentication*, page 180).
- **User Identification**: Configure User Service to communicate with a transparent identification agent, and prompt users for directory authentication (see *Transparent identification*, page 130).
- **Network Agent**: Configure the HTTP ports for Websense software, and the network segments on which Network Agent monitors protocol and bandwidth usage (see *Initial configuration*, page 83).
- **Change Password**: Configure the administrative password used to log on to Policy Server (see *Changing the Policy Server password*, page 188).
- **Bandwidth Optimizer**: Configure the default values used as the foundation for bandwidth-based filtering. There are default maximum values for the entire network, and per protocol (see *Managing bandwidth*, page 295).

- **Risk Classes**: Configure the classes identifying URL categories according to areas of risk to your network. Risk classes help you measure internet usage by risk area (see *Logging and Reporting*, page 74).
- **Session**: Configure the length of Policy Server sessions (see *Session management*, page 228).
- **Common Filtering**: Set filtering preferences for:
  - When a user is in multiple groups (see *When multiple group policies apply*, page 37)
  - When a subscription expires or is exceeded (see *Subscriptions*, page 13)
  - Whether Websense can gather protocol usage data about your network (see *Protocol usage*, page 96)
  - Where Websense software searches for keywords (see *Keywords*, page 268)
  - Password override and continue time limits (see *Password override*, page 48 and *Continue*, page 43)
  - Quota session length and default quota time per day (see *Quotas*, page 44)

When you finish configuring settings, click **OK** to update Policy Server.

Stopping or starting Websense services

Websense services are configured to start each time the machine restarts. However, in some cases you need to stop or start Policy Server, Filtering Service, User Service, or Network Agent separately from a machine restart.

> **Note**
>
> If Filtering Service is in the process of downloading the Master Database, it does not stop running until the download is complete.

Windows

1. Open the Windows Services dialog box.

   Windows NT: Select **Start > Settings > Control Panel**, and then double-click **Services**.

   Windows 200x: Select **Start** > **Programs** > **Administrative Tools** > **Services**.

2. Right-click the Websense service name, and then select **Stop** or **Start**.

> **Note**
>
> If you are stopping or starting multiple services, stop the Websense Policy Server last, and start it first.

Solaris or Linux

On Solaris and Linux machines, all services stop and start together when you use this procedure.

1. Go to the `\Websense` directory.
2. Check the status of the Websense services with the command:
   - `./WebsenseAdmin status`
3. Stop, start, or restart all Websense services with the commands:
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`
   - `./WebsenseAdmin restart`

Warning

Do not use the **kill** command to stop a Websense service, as it may corrupt the service.

Removing a server

Removing a Policy Server from Websense Manager does not uninstall it from the machine; it simply removes the Server from Websense Manager's control. The settings remain intact, and the Server can be added again later, or added to a different instance of Websense Manager.

1. If the Policy Server to remove is connected: Right-click the server icon in the navigation tree, and then select **Log Off from Server** from the shortcut menu. You cannot remove a Server that is connected.
2. Right-click the disconnected Server in the navigation tree, and then select **Remove Policy Server**.
3. Select **Yes** when prompted to confirm deletion.

Saving the configuration

Server configuration and policy settings are stored in the `config.xml` file in the Websense installation directory. After changing the Websense configuration, back up this configuration file so you can restore the established settings should any problem occur.

Every time the `config.xml` file is updated, the previous version is saved as `config.xml.bak`. When Policy Server is running, `config.xml` is updated every 30 seconds or every 500 transactions, whichever comes first. Between updates, transactions are stored in the binary file `journal.dat`. Each time Policy Server starts, it applies new `journal.dat` entries to the data it reads from `config.xml`.

Backing up `config.xml` and `config.xml.bak` preserves the latest data in case Policy Server doesn't start normally.

Note

Before upgrading Websense software, back up the configuration file so settings are not lost in case of a power outage or problem during upgrade.

Backing up the configuration file

1. Stop Policy Server (see *Stopping or starting Websense services*, page 191).
2. Go to the Websense installation directory (`\Websense\bin` by default).
3. Copy the `config.xml` *and* `config.xml.bak` files, and move the copies to a shared network location.
4. Start Policy Server (see *Stopping or starting Websense services*, page 191).

Restoring the configuration file

This restores the configuration file to its previous settings.

1. Stop all Websense services (see *Stopping or starting Websense services*, page 191).
2. Copy the `config.xml` *and* `config.xml.bak` files to the Websense installation directory, using procedures appropriate for your operating system.
3. Start the Websense services (starting with the Websense Policy Server, if on Windows).

Changing an IP address

In a typical scenario, Websense software handles IP address changes behind-the-scenes. Websense software detects IP address changes for machines where its components reside, and adjusts so filtering continues uninterrupted.

For example, if the IP address of the machine running Policy Server changes, a behind-the-scenes broadcast system informs all other components of the change. The same is true for machines running other Websense components (Filtering Service, Network Agent, or User Service). Policy Server is the critical component in maintaining IP address information for all Websense components.

If you need to change the IP address of a machine running a Websense component, follow the instructions in this section. *Failure to reconfigure Websense after an IP address change could result in filtering problems.*

Important

Before changing the IP address on any machine running a Websense component, stop the Websense services on that machine. After the change, restart the Websense services (see *Stopping or starting Websense services*, page 191).

The Websense transparent identification agents can be identified by machine name, rather than IP address. Therefore, changing the IP address of an agent machine has no effect on other Websense components. However, if the agent machine *name* changes, you must update the name via Websense Manager (see *Configuring different settings for an agent instance*, page 176).

Network Agent

When an IP address on the Network Agent machine is changed:

- Restart the Websense Network Agent service for Websense software to recognize the change. Restart the service regardless of where Network Agent resides in relation to other Websense components.
- Exit and then start Websense Manager. This ensures that Websense Manager displays the updated address information.

Changing the IP address of any *proxy/cache machine* in your network requires that you configure Network Agent to recognize the new IP address. For more information, see *Initial configuration*, page 83.

When Network Agent resides on a multiple-NIC machine that is separate from Filtering Service, you must update the Network Agent machine's IP address configuration:

1. Stop the Websense Network Agent service (see *Stopping or starting Websense services*, page 191).
2. Go to the Websense installation directory on the Network Agent machine (`\Websense\bin\` by default).
3. Open the `websense.ini` file in a text editor.
4. Locate the `LocalServerIP` parameter. Edit the corresponding IP address as follows:

   ```
   LocalServerIP = <IP address>
   ```

   where `<IP address>` is the new IP address of the machine running Policy Server.
5. Save the file.
6. Start the Websense Network Agent service.

Policy Server

If you change the IP address of Policy Server:

1. Stop and then restart all Websense services on the Policy Server machine.
2. Add and log on to the updated Policy Server via Websense Manager (see *Adding a server*, page 186).
3. Remove the old Policy Server from Websense Manager.

If the Policy Server machine has multiple NICs, also update the `websense.ini` file to reflect the change:

1. Stop the Websense Policy Server (see *Stopping or starting Websense services*, page 191).
2. Go to the Websense installation directory.
3. Open the `websense.ini` file in a text editor.
4. Locate the `LocalServerIP` parameter. Edit the corresponding IP address as follows:

   ```
   LocalServerIP = <IP address>
   ```

   where `<IP address>` is the new IP address of the machine running Policy Server.
5. Locate the `PolicyServerIP` parameter. Edit the corresponding IP address as follows:

   ```
   PolicyServerIP = <IP address>
   ```

   where `<IP address>` is the same IP address entered for `LocalServerIP`.
6. Save the file.
7. Start the Websense Policy Server.

If you have installed Real-Time Analyzer or Client Policy Manager Reporter, then you also need to update the Policy Server IP address for the Websense Enterprise Web-based Manager. This is required for logging on to Real-Time Analyzer.

To ensure that applications using the Web-based Manager register the IP address change:

1. Stop the Websense Policy Server (see *Stopping or starting Websense services*, page 191).
2. Update the Policy Server IP address in *each* of these files:

   `\Websense\webroot\cgi-bin\websense.ini`

   `\Websense\webroot\Explorer\websense.ini`

   a. Go to the appropriate directory listed above.

   b. Open the `websense.ini` file in a text editor.

   c. Locate the `PolicyServerIP` parameter. Edit the corresponding IP address as follows:

   ```
   PolicyServerIP = <IP address>
   ```

   where <*`IP address`*> is the new IP address of the machine running Policy Server.

   d. Save the file.
3. Start the Websense Policy Server.

Integrated products and plug-ins

Changing an IP address for a Websense component may require that you update the plug-in configuration to reflect this change. The table below shows what to modify and which service to restart for particular plug-ins. If your integration product is not listed, no additional configuration is required.

Plug-in	What to update	What to restart
Microsoft Proxy/ISA	wsMSP.ini	Web Proxy service
Network Appliance NetCache	Service Farm IP	ICAP (disable/enable)
Squid	WsSquid.ini	Squid service

Changing the IP address of an integrated plug-in may not be advisable. Before changing the IP address on a machine running a plug-in, see your integration product documentation.

Alerting

To facilitate tracking and management of both Websense system and user internet activity, Websense software can alert administrators when selected events occur.

The available auto-generated alerts are:

- **System alerts**: Notification regarding subscription status, Websense Master Database activity, or administrator lockouts (see *Lockouts*, page 230).
- **Usage alerts**: Notification when internet activity for particular URL categories or protocols reaches threshold limits you have configured.

Alerts can be sent to selected recipients in any of these modes:

- Email
- Onscreen (Windows net send messaging)

Note

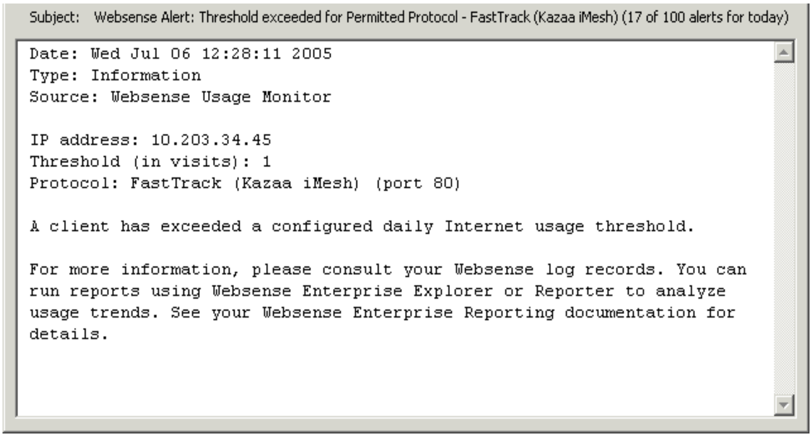
Onscreen alerts cannot be sent to machines running Linux or Solaris. However, they can be sent from a Linux/Solaris machine running Policy Server to Windows machines, provided that the Samba client is installed on that Linux/ Solaris machine.

- SNMP messaging

Note

SNMP messaging is only available with Corporate Editions of Websense.

An example of a usage alert sent as an email is shown. This alert was triggered because occurrences (or requests) for the FastTrack protocol exceeded the threshold limit configured by the administrator.



Subject: Websense Alert: Threshold exceeded for Permitted Protocol - FastTrack (Kazaa iMesh) (17 of 100 alerts for today)

```
Date: Wed Jul 06 12:28:11 2005
Type: Information
Source: Websense Usage Monitor

IP address: 10.203.34.45
Threshold (in visits): 1
Protocol: FastTrack (Kazaa iMesh) (port 80)

A client has exceeded a configured daily Internet usage threshold.

For more information, please consult your Websense log records. You can
run reports using Websense Enterprise Explorer or Reporter to analyze
usage trends. See your Websense Enterprise Reporting documentation for
details.
```

Sample email alert

Alerts can be generated for the Websense categories or protocols provided by default, or for custom categories you have added. For information about custom categories, *Adding a custom category*, page 265.

Flood control

Usage alerting has built-in controls for preventing excessive numbers of alert messages from being generated. Specify a limit for how many alerts are generated as category and protocol requests occur. The **Maximum usage alerts per event** setting limits all usage alerts to a maximum number per day (100 by default).

This setting is related to threshold limits for each category and protocol. For example, if a category has a threshold limit of 10, an alert is generated after 10 occurrences (or requests by the same client).

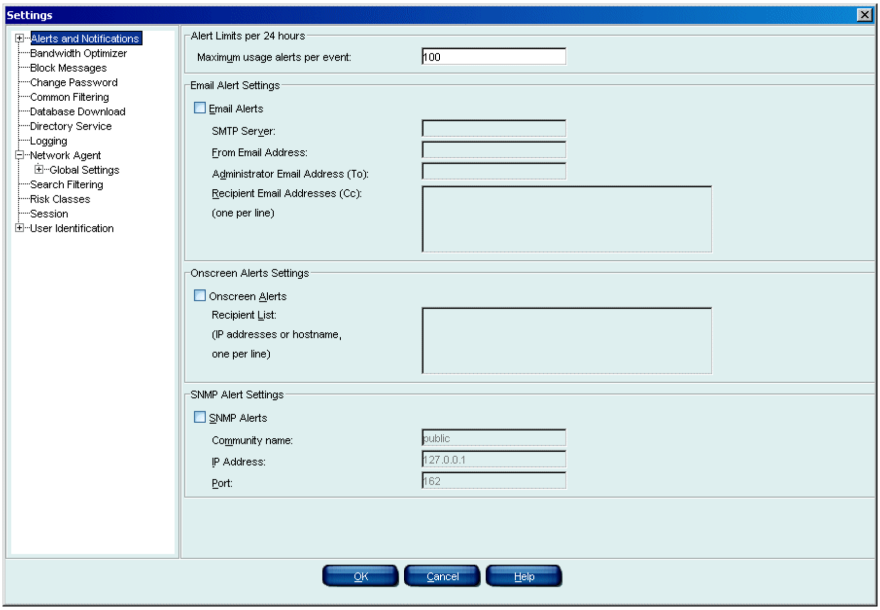
If the usage alert limit is 100, in 1 day the administrator is only alerted the first 100 times the category exceeds its threshold. In this case, only the first 1000 occurrences generate alerts (threshold of 10 multiplied by alert limit of 100).

Setting up alerting

If you are running a Corporate Edition of Websense software, you need Super Administrator access to Websense Manager to set up Websense alerting. A Super Administrator can configure alerts to be sent to any other Websense administrator. For information about administrative permissions, see *Administrator roles*, page 217.

If you are running a standard edition of Websense software, the first administrator to install Websense software has access to set up alerting.

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Alerts and Notifications** at the left. The alerting global settings are displayed.



Alert Limits per 24 hours
Maximum usage alerts per event: 100

Email Alert Settings
□ Email Alerts
SMTP Server:
From Email Address:
Administrator Email Address (To):
Recipient Email Addresses (Cc):
(one per line)

Onscreen Alerts Settings
□ Onscreen Alerts
Recipient List:
(IP addresses or hostname,
one per line)

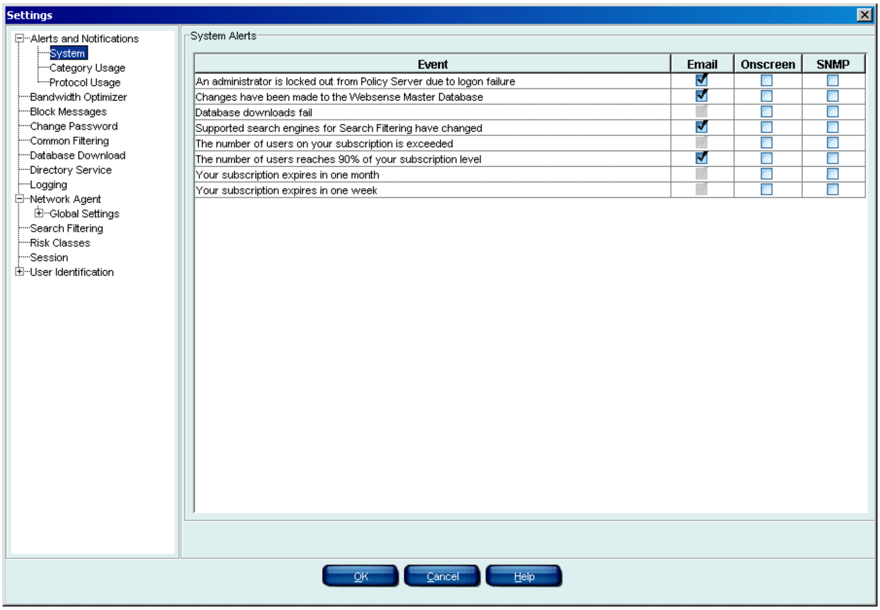
SNMP Alert Settings
□ SNMP Alerts
Community name: public
IP Address: 127.0.0.1
Port: 162

3. For **Maximum usage alerts per event**, specify the maximum number of usage alerts an administrator can receive per event, per day.

   For example, the URL category Sports has a configured threshold limit of 5, so an alert is generated after 5 occurrences (or requests by the same client). If the usage alert limit is 100, the administrator is only alerted the first 100 times the Sports category exceeds its threshold. So, alerts are only generated for 500 occurrences in a day (the threshold of 5 occurrences multiplied by 100 alerts).

4. Check **Email Alerts** to enable alerting via email.
5. Specify the following for email alerts:
   - **SMTP Server**: The email server through which email alerts should be routed.
   - **From Email Address**: The sender address that should appear on email messages (for example, “Websense”).
   - **Administrator Email Address (To)**: The primary address to which to send alerts.
   - **Recipient Email Addresses (Cc)**: Any additional recipients for email alerts.
6. Check **Onscreen Alerts** to enable Websense alerts via Windows net send messaging.
7. In the **Recipient List** field, enter the desired recipients for onscreen alerts (machine names or IP addresses only- do not use **localhost**).
8. *Corporate Edition users only:* Check **SNMP Alerts** to enable Websense alerting via SNMP messaging.
9. Specify the following for SNMP alerts:
   - **Community Name**: The name for the trap community on your SNMP Trap server.
   - **IP Address**: The IP address of the SNMP Trap server.
   - **Port**: The port SNMP messages should use.

10. Expand **Alerts and Notifications** > **System Alerts** at the left.



System Alerts

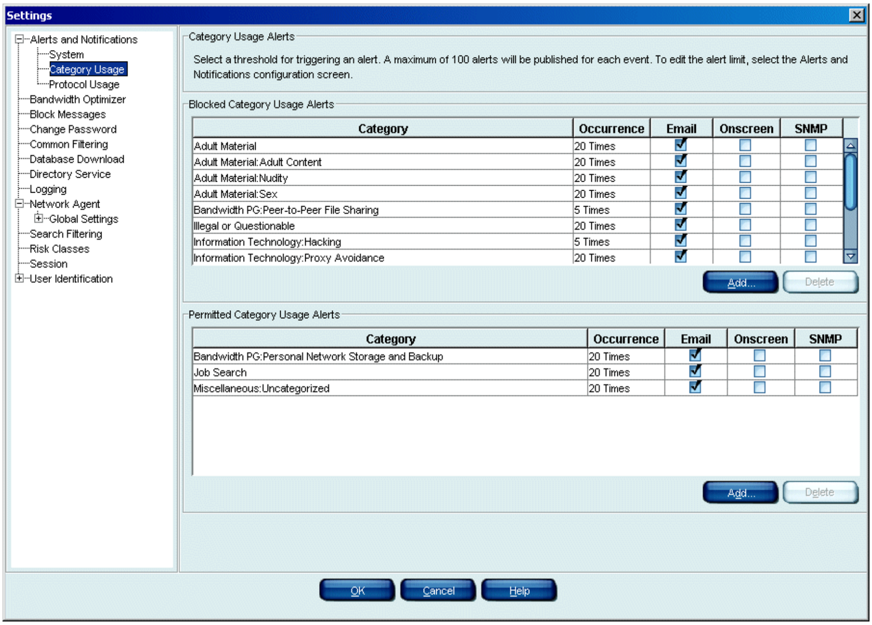
Event	Email	Onscreen	SNMP
An administrator is locked out from Policy Server due to logon failure	☑	□	□
Changes have been made to the Websense Master Database	☑	□	□
Database downloads fail	□	□	□
Supported search engines for Search Filtering have changed	☑	□	□
The number of users on your subscription is exceeded	□	□	□
The number of users reaches 90% of your subscription level	☑	□	□
Your subscription expires in one month	□	□	□
Your subscription expires in one week	□	□	□

11. For each system event to alert on, check the alerting modes to activate for that event. You can select single or multiple alerting modes for each event.

Note

When a download fails or the subscription has been exceeded, information is logged in the Application Event Log and in the `Websense.log` file on Windows machines. On Solaris or Linux machines, information is logged to `Websense.log` (in the installation directory).

12. Select **Category Usage Alerts** at the left.



Category Usage Alerts

Select a threshold for triggering an alert. A maximum of 100 alerts will be published for each event. To edit the alert limit, select the Alerts and Notifications configuration screen.

Blocked Category Usage Alerts

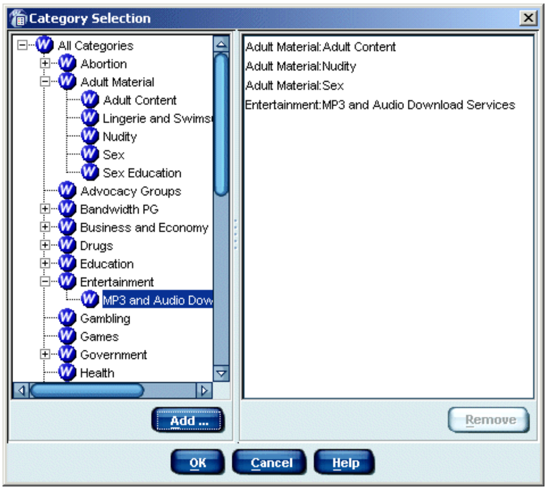
Category	Occurrence	Email	Onscreen	SNMP
Adult Material	20 Times	☑	□	□
Adult Material:Adult Content	20 Times	☑	□	□
Adult Material:Nudity	20 Times	☑	□	□
Adult Material:Sex	20 Times	☑	□	□
Bandwidth PG:Peer-to-Peer File Sharing	5 Times	☑	□	□
Illegal or Questionable	20 Times	☑	□	□
Information Technology:Hacking	5 Times	☑	□	□
Information Technology:Proxy Avoidance	20 Times	☑	□	□

Permitted Category Usage Alerts

Category	Occurrence	Email	Onscreen	SNMP
Bandwidth PG:Personal Network Storage and Backup	20 Times	☑	□	□
Job Search	20 Times	☑	□	□
Miscellaneous:Uncategorized	20 Times	☑	□	□

13. Under **Blocked Category Usage Alerts**, click **Add Category** to set up an alert for URL categories that are blocked in policies.

14. In the Category Selection dialog box, select 1 or more categories at the left, and then click **Add**. The selected categories appear at the right.



Adult Material:Adult Content
Adult Material:Nudity
Adult Material:Sex
Entertainment:MP3 and Audio Download Services

Note

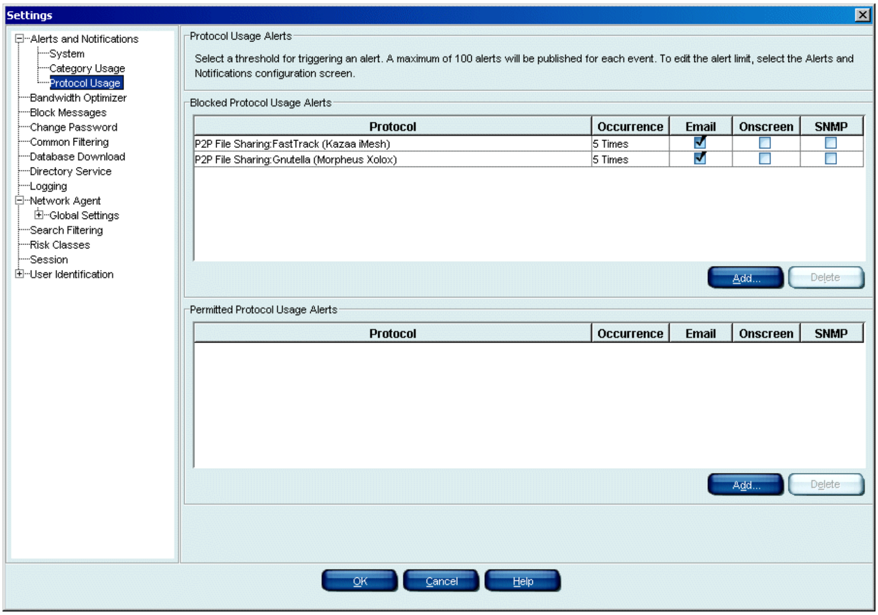
To remove a category, select the category and then click **Remove**.

15. Click **OK**.
16. For each category, specify:
    - How many occurrences cause an alert to be generated.
    - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).
17. Under **Permitted Category Usage Alerts**, click **Add Category** to set up an alert for categories that are permitted in policies.
18. In the Category Selection dialog box, select 1 or more category at the left, and then click **Add**. The selected categories appear at the right.
19. Click **OK**.
20. For each category, specify:
    - How many occurrences cause an alert to be generated.
    - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).

21. Select **Protocol Usage Alerts** at the left.

Note

Alerts are only generated for protocols that are logged. For how to enable logging for protocols, see *Editing a protocol set*, page 290.



Select a threshold for triggering an alert. A maximum of 100 alerts will be published for each event. To edit the alert limit, select the Alerts and Notifications configuration screen.

Blocked Protocol Usage Alerts

Protocol	Occurrence	Email	Onscreen	SNMP
P2P File Sharing:FastTrack (Kazaa iMesh)	5 Times	☑	□	□
P2P File Sharing:Gnutella (Morpheus Xolox)	5 Times	☑	□	□

Permitted Protocol Usage Alerts

Protocol	Occurrence	Email	Onscreen	SNMP

22. Under **Blocked Protocol Usage Alerts**, click **Add Protocol** to set up an alert for a protocol that is blocked in policies.
23. In the Protocol Selection dialog box, select 1 or more protocols at the left, and then click **Add**. The selected protocols appear at the right.

Note

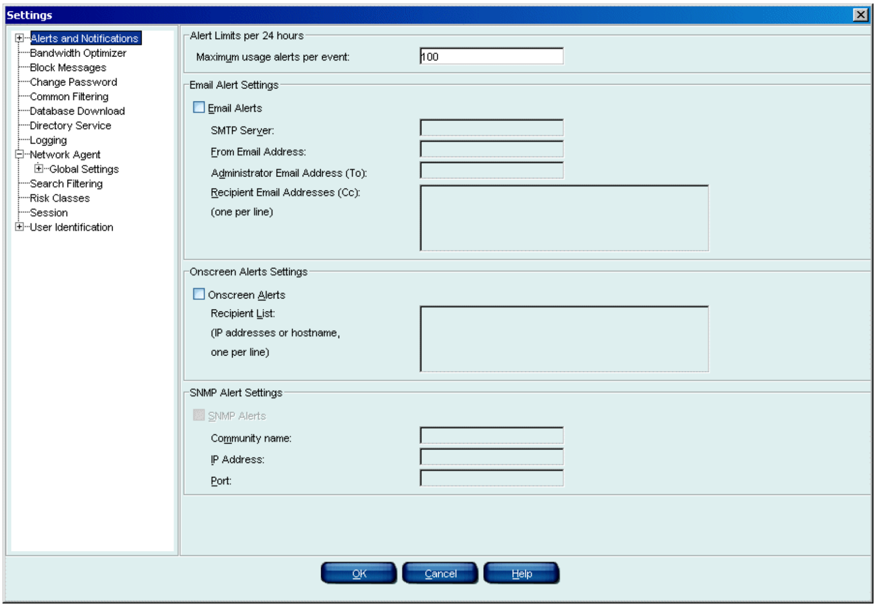
To remove a category, select the category and then click **Remove**.

24. Click **OK**.

25. For each protocol, specify:
    - How many occurrences cause an alert to be generated.
    - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).
26. Under **Permitted Protocol Usage Alerts**, click **Add Protocol** to set up an alert for protocols that are permitted in policies.
27. In the Protocol Selection dialog box, select 1 or more protocols at the left, and then click **Add**. The selected protocols appear at the right.
28. Click **OK**.
29. For each protocol, specify:
    - How many occurrences cause an alert to be generated.
    - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).
30. Click **OK** to close the Settings dialog box.

Disabling alerting

1. Select **Server** > **Settings**.
2. Select **Alerts and Notifications** at the left. The alerting global settings are displayed.



Alert Limits per 24 hours

Maximum usage alerts per event: 100

Email Alert Settings

□ Email Alerts

SMTP Server:

From Email Address:

Administrator Email Address (To):

Recipient Email Addresses (Cc):
(one per line)

Onscreen Alerts Settings

□ Onscreen Alerts

Recipient List:
(IP addresses or hostname,
one per line)

SNMP Alert Settings

□ SNMP Alerts

Community name:

IP Address:

Port:

3. Uncheck the alert mode to disable (**Email Alerts**, **Onscreen Alerts**, or **SNMP Alerts**).
4. Click **OK**.

Administrative auditing

Websense Enterprise Corporate Edition provides an audit trail of changes to policy and setting configuration. This makes it easy to track who has made configuration changes.

> **Note**
>
> This feature is available only with Corporate Editions of Websense software.

The audit log is accessible only by Super Administrators, and not by Delegated or Remote Administrators without full administrative access. For more information, see *Administrator roles*, page 217.

Access the audit log from Websense Manager, and optionally export the log to an encrypted external file.

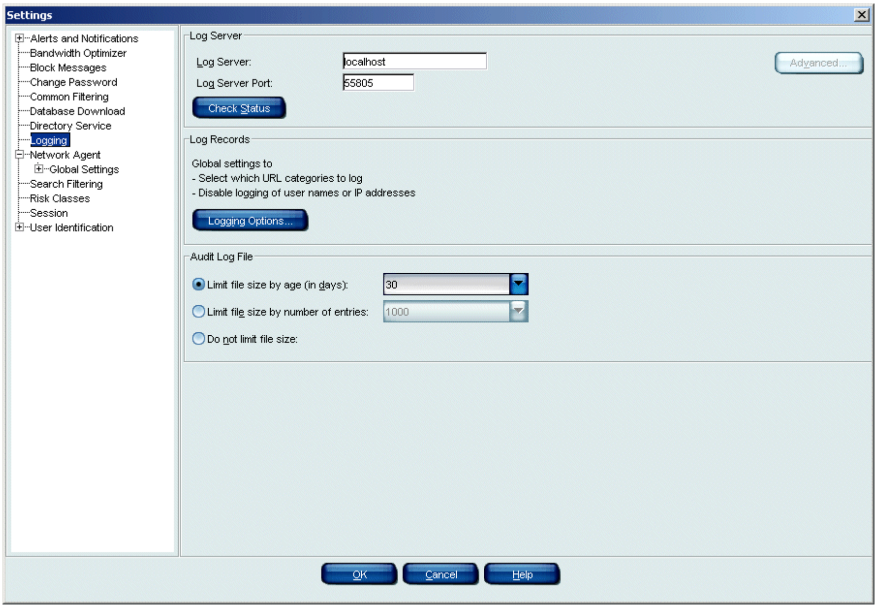
For each change, the audit log indicates:

- When the change was made
- Who made the change
- Where the change was made (on which machine)
- The component or area where the change was made
- The nature of the change

Over time, the audit log file can grow to a large size. To impose a limit on the audit log file size, configure size restrictions as follows.

1. Select **Server** > **Settings**. The Settings dialog box appears.

2. Select **Logging** at the left. The **Audit Log File** settings are displayed, along with other logging settings.



Log Server: localhost

Log Server Port: 55805

Global settings to
- Select which URL categories to log
- Disable logging of user names or IP addresses

● Limit file size by age (in days): 30

○ Limit file size by number of entries: 1000

○ Do not limit file size:

3. Select how to limit the file size.
   - **Limit file size by age (in days)**: Force the audit log file to discard entries after a certain number of days.
   - **Limit file size by number of entries**: Force the audit log file to keep only a certain number of entries at any one time. If size is limited in this way, excess entries are removed each night.
   - **Do not limit file size**: Allow the audit log file to keep entries until manually deleted.

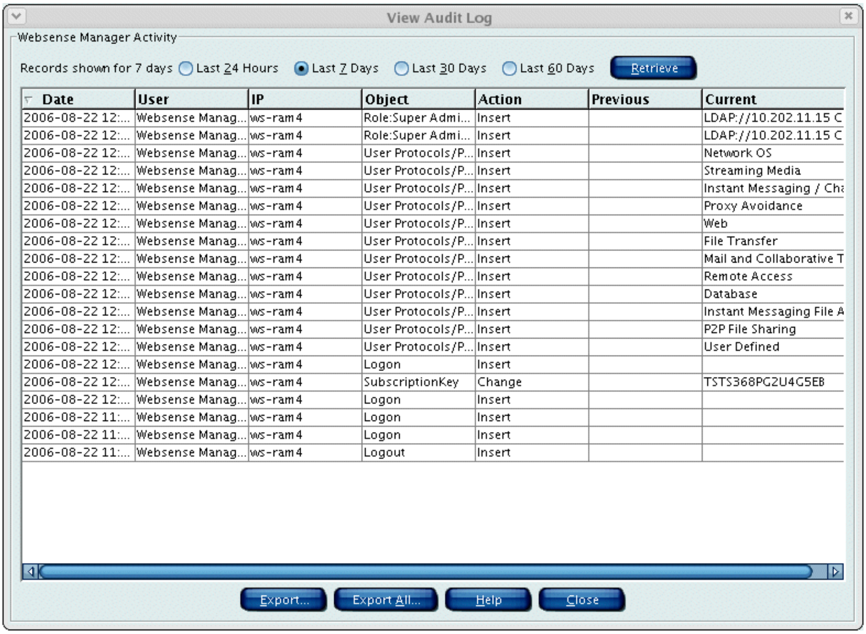
Note

If you have an integration product running on the same machine as Websense software, it is best to limit the audit log file to a smaller number of entries (500 or fewer).

4. Click **OK**.

Viewing or exporting the Audit Log

1. Select **Actions > View Audit Log**. The Audit Log dialog box appears.



Records shown for 7 days ○ Last 24 Hours ● Last 7 Days ○ Last 30 Days ○ Last 60 Days

Date	User	IP	Object	Action	Previous	Current
2006-08-22 12:...	Websense Manag...	ws-ram4	Role:Super Admi...	Insert		LDAP://10.202.11.15 C
2006-08-22 12:...	Websense Manag...	ws-ram4	Role:Super Admi...	Insert		LDAP://10.202.11.15 C
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Network OS
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Streaming Media
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Instant Messaging / Cha
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Proxy Avoidance
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Web
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		File Transfer
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Mail and Collaborative T
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Remote Access
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Database
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		Instant Messaging File A
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		P2P File Sharing
2006-08-22 12:...	Websense Manag...	ws-ram4	User Protocols/P...	Insert		User Defined
2006-08-22 12:...	Websense Manag...	ws-ram4	Logon	Insert		
2006-08-22 12:...	Websense Manag...	ws-ram4	SubscriptionKey	Change		TSTS368PG2U4G5EB
2006-08-22 12:...	Websense Manag...	ws-ram4	Logon	Insert		
2006-08-22 11:...	Websense Manag...	ws-ram4	Logon	Insert		
2006-08-22 11:...	Websense Manag...	ws-ram4	Logon	Insert		
2006-08-22 11:...	Websense Manag...	ws-ram4	Logout	Insert		

2. Next to **View Records** at the top, select the time period for which to view records.

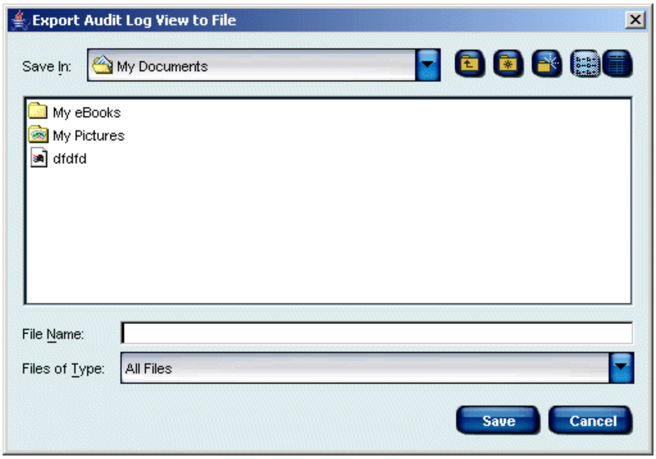
3. Double-click on a column heading to sort records by the criterion for that column.

> **Note**
>
> If a policy is only renamed, the audit log displays an entry for deletion of the original policy, and entry for insertion of the new (renamed) policy.

4. To export a portion of the audit log, click **Export**. This exports only the records *currently visible*.

   To export the entire log, click **Export All**.

The Export Audit Log View to File dialog box appears.



Save In: My Documents

Files of Type: All Files

5. Specify a location for the exported audit log file.
6. Type a file name for the exported file.
7. Click **Save**.
8. Click **OK**. The audit log file is saved as a tab-separated text file. This file can be optionally imported into external applications.

The audit log is continually updated and is always available for viewing or export by a Super Administrator.

Delegated Administration and Reporting

Websense Delegated Administration and Reporting provides flexibility in managing internet filtering and reporting and across multiple sites or Policy Servers. For more information, see *Chapter 8: Delegated Administration*.

✓ **Note**

This feature is available only with Corporate Editions of Websense. If you are running a standard (non-Corporate) edition of Websense, you can customize reporting roles and permissions only. Contact Websense, Inc. for information on subscribing to Corporate Edition.

Regardless of which Websense edition you are running, you can distribute configuration data from one Policy Server to other Policy Servers. However, Delegated Administration and Reporting allows greater flexibility in maintaining unique configurations for multiple servers. You can distribute roles and permissions in addition to filtering settings and server settings. If you are running a standard edition of Websense, you can only distribute filtering and server settings.

For information on central policy distribution, see *Distributing policies to multiple servers*, page 306. For information on central configuration distribution with Websense Enterprise Corporate Edition, see *Distributing configuration settings*, page 237.

CHAPTER 8

Delegated Administration

The Delegated Administration and Reporting feature provides powerful, flexible methods for managing internet filtering and reporting for particular groups of clients, and across multiple locations.

✓ **Note**

This feature is available only with a Corporate Edition of Websense software. If you are running a standard edition of Websense software, you can customize *reporting roles and permissions only*. Contact Websense, Inc., for information on upgrading.

Delegated Administration and Reporting let you customize filtering behavior through the use of configurable roles and permissions for administrative users. This provides greater granularity in employee internet access, plus additional layers of security against unwanted or invasive internet content.

One *Super Administrator* can set filtering restrictions from a central location, and then distribute those to multiple locations. This Super Administrator can grant limited administrative rights to *Delegated Administrators*, who manage internet usage in a more limited fashion. The Super Administrator can also customize access levels for *Remote Administrators*, administrative users for remote locations.

Delegated Administration and Reporting also allow central configuration of reporting permissions. While configuring roles for Delegated Administrators, a Super Administrator grants access to internet usage data generated by Websense Enterprise Explorer or Websense Real-Time Analyzer.

Overview: Setting up Delegated Administration

A distributed environment is based on relationships between Policy Servers. By default, the first Policy Server installed is the central server. However, you can set any server as the central Policy Server. Optionally share configuration settings with other Policy Servers (see *Central Configuration Distribution*, page 235).

For a quick-start tutorial, go to www.websense.com/global/en/SupportAndKB/ProductDocumentation/, *Getting Started* section.

To set up your distributed filtering environment, you need to:

- Determine which site acts as the central site and house the central Policy Server.
- Define additional Policy Servers in Websense Manager (see *Adding a server*, page 186).
- Ensure that users and groups in your directory service are added to Websense Manager as directory objects (see *Adding directory objects*, page 114).
- Designate a Super Administrator (see *Administrator roles*, page 217).
- Create roles to group similar clients and administrative permissions (see *Creating a role*, page 222).
- Specify the Delegated Administrators or Remote Administrators for the role (see *Assigning an administrative role*, page 224).
- Add the clients to be managed by the administrator in each role (see *Adding clients to an administrative role*, page 226).
- Configure filtering setting restrictions by creating a Web Filter Lock (see *Defining filtering restrictions*, page 231).
- Distribute the Web Filter Lock to other sites (see *Distributing configuration settings*, page 237).
- Allow the Delegated or Remote Administrators to maintain additional filtering settings at their sites.

To facilitate client and policy maintenance by multiple administrators, Websense software features built-in Policy Server session management. This prevents an administrator from overwriting configuration changes made by another administrator via Websense Manager. For more information, see *Session management*, page 228.

Managing roles

Roles provide a convenient way to organize and control user rights and internet access. After Websense software is installed, the first user to log on to Websense Manager has full administrative access, equivalent to Super Administrator access. (The user name is **WebsenseAdministrator**, and cannot be changed.) However, by default this user is not assigned the Super Administrator role. This user can designate himself as a Super Administrator, and then assign the Delegated Administrator role to other administrative users.

✓ **Note**

In the unlikely event that the Websense Master Database was not downloaded during installation, the first user to log on to Websense Manager can only view and configure reporting roles.

Administrator roles

Assigning roles to all administrative users organizes who has administrative access, and what level of access each user has. Roles also facilitate tracking of administrative actions.

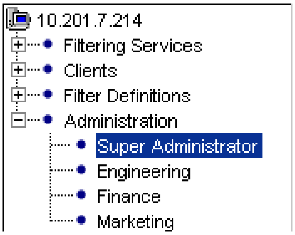
Track administrative actions via the Auditing feature (see *Administrative auditing*, page 209). By default, Websense software provides an audit trail of changes to policy, system and role configuration. The audit log entries indicate the identity of the user making each change. This makes it easy to track who has made configuration changes.

Administrative roles are as follows:

- **Super Administrator**: Full administrative user. If there are multiple sites, this is the administrator at the central site.
- **Delegated Administrator**: Administrative user designated by the Super Administrator to manage 1 or more roles. Has limited access to policy configuration and role management. Access levels are determined by the Super Administrator.

- **Remote Administrator**: Administrative user at a remote site. Has access for policy configuration at his site, but cannot distribute policy or system configuration to Policy Servers at other sites. At the remote site, this administrator is referred to as a Super or Delegated Administrator.

Roles are displayed in Websense Manager, with other Websense filtering objects. Roles appear under **Administration** in the navigation tree.



Roles in the navigation tree

Roles facilitate maintaining policies specific to departments or areas in your organization. As clients change departments or new clients arrive, policy assignments remain intact because they are managed at the role level.

Before creating additional roles, ensure that at least 1 Super Administrator has been designated. Add the primary administrative user to the Super Administrator role as follows:

1. In the navigation tree, expand **Administration** > **Super Administrator**. The Super Administrator role details are displayed in the content pane.
2. Next to **Managed Administrators**, click **Edit**. The Edit Administrators dialog box appears.
3. Select the directory object to designate as the Super Administrator, and then click **Add**. For help with custom LDAP groups, see *Directory services*, page 99.
4. Click **OK**.

Note

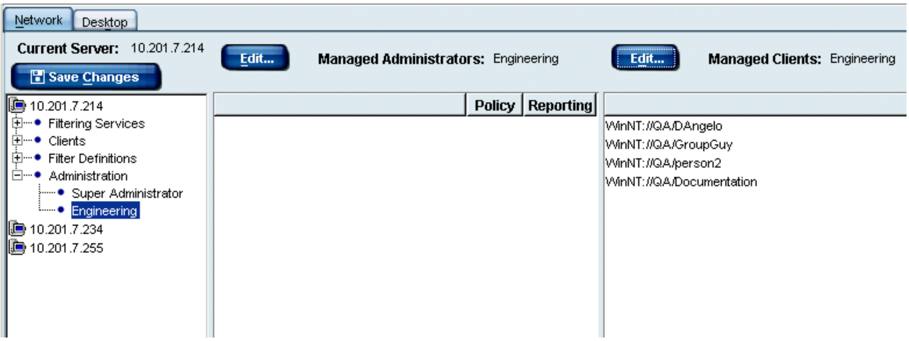
Default filtering settings configured by a Super Administrator are copied over when new administrative roles are created. Ensure that the **Default Settings** category set and protocol set are both active in the Global policy. Then edit them as desired *before* setting up roles. For more information, see *The Global policy*, page 300.

Managed clients

Each administrative role has an associated Managed Clients list. Any administrator in a particular administrative role can define internet access for those Managed Clients.

For example, set up administrative roles for the Engineering, Finance and Marketing departments in your organization, and designate a Delegated Administrator for each role. Then add all users in your Engineering department as Managed Clients in the Engineering role, all Finance users as Managed Clients in the Finance role, and so on.

Users associated with a particular role are displayed as **Managed Clients** when the role name is selected, as shown:



Current Server: 10.201.7.214

Managed Administrators: Engineering

Managed Clients: Engineering

WinNT://QA/DAngelo
WinNT://QA/GroupGuy
WinNT://QA/person2
WinNT://QA/Documentation

Users assigned the Engineering role

To simplify administration of users:

- Create roles corresponding to areas of your organization;
- Add 1 or more Delegated Administrators for that role;
- Grant Delegated Administrators access to manage the users in that role.

You can add directory objects, workstations or networks as clients. In order for directory objects to be properly defined by role, those clients must log on to your directory service. Ensure that your directory service is configured to communicate with Websense software (see *Directory services*, page 99).

Note

If you plan to change to a different directory service, implement that change before assigning roles. Otherwise, directory objects need to be re-added and roles re-assigned after the change.

Working with roles

You must be logged on to Websense Manager as the default administrative user (see *Administrator roles*, page 217) or Super Administrator to modify administrative roles.

To view and modify an administrative role, expand **Administration** in the navigation tree, and then select the desired role.

When you create a role, specify how users in that role will be managed by associating these items with the role:

- Clients to be managed by the administrator for the role (see *Managed clients*, page 219)
- One or more Delegated Administrators to create and manage filtering policies governing clients in the role

Also specify:

- Which elements of policies each Delegated Administrator can modify
- Which clients each Delegated Administrator can include in reports (all clients, or only clients in a particular role)

> **Note**
> While full administrative roles are available only with Corporate Edition, configurable reporting roles are available in standard editions of Websense software. Using this role-based reporting, you can both set permissions to show or hide user names in reports, and specify whether administrators can save and schedule Favorite reports, manage Log Database contents, and access Real-Time Analyzer.

After you create a role, Delegated Administrators can log on to the role to configure policy settings for managed clients using either of two methods:

- Log on to Policy Server and select a role to administer in the **Select Role** dialog box.
- Select a role to administer from the **Current Roll** list box in the upper right-hand corner of Websense Manager.

Creating a role

The Super Administrator is responsible for creating roles to designate administrators for various groups or areas in the organization. Adding clients to an administrative role makes it easy for the associated Delegated Administrators to manage internet access collectively for those clients.

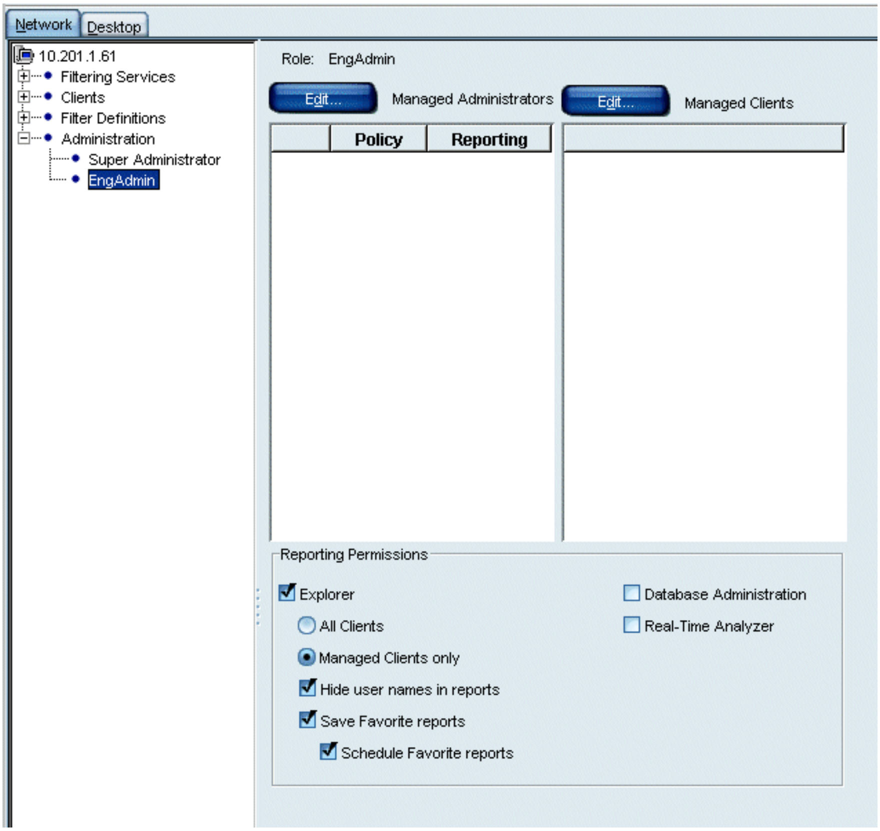
To create a role:

1. Right-click in the navigation tree, and then select **Add Role**. The Add New Role dialog box appears.
2. Enter a unique name for the role, and then click **OK**. The role you created appears under **Administration** in the navigation tree, and is available for association with Delegated Administrators and clients.

✓ **Note**

If you are running a standard (non-Corporate) edition of Websense, only *reporting roles* are configurable. Roles you create appear under **Report Administration** in the navigation tree.

3. Select the role you just created in the navigation tree. The user and permission details for that role appear in the content pane.



Role: EngAdmin

Reporting Permissions

☑ Explorer

○ All Clients

● Managed Clients only

☑ Hide user names in reports

☑ Save Favorite reports

☑ Schedule Favorite reports

□ Database Administration

□ Real-Time Analyzer

4. Under **Reporting Permissions - [role name]** at the bottom of the content pane, specify reporting rights for administrators in this role.

   - **Explorer**: Allows Delegated Administrators in this role to generate reports using Websense Explorer. For more information, see the Reporting documentation.

- **All Clients**: Allows administrators in this role to report on all clients added to Websense Manager. **Managed Clients Only** restricts reporting only to clients in this administrator's role.

✓ **Note**

All Clients gives Delegated Administrators the ability to see and report on all clients, even those outside the roles they manage.

- **Hide user names in reports**: Makes report entries anonymous in reports these administrators run.
- **Save custom reports**: Allows these administrators to create and save report criteria for repeated use.
- **Schedule custom reports**: Allows these administrators to set Favorite reports to run in Explorer.

- ■ **Database Administration**: Allows these administrators to use the Database Administration Reporting tool to manage log database contents (see the Reporting documentation).
- ■ **Real-Time Analyzer**: Allows these administrators to access Real-Time Analyzer.

5. Click **Save Changes** above the navigation tree.

If you log off from Policy Server or your configuration session times out, the next time you log on to the server, the new role is available for administration.

Assigning an administrative role

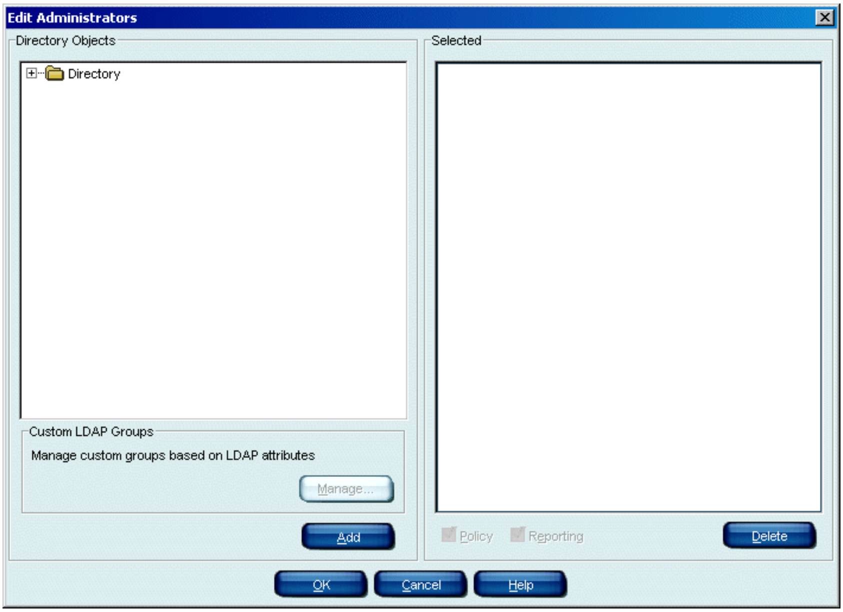
As a Super Administrator, you can designate who administers various roles in your organization. The users you designate become Delegated Administrators for those areas.

✓ **Note**

If you plan to change to a different directory service, implement that change before assigning roles. Otherwise, directory objects must be re-added and roles re-assigned after the change.

1. In the navigation tree, expand **Administration**.

2. Select the role to assign to the administrative user. The user and permission details for that role appear in the content pane.
3. Next to **Managed Administrators** in the content pane, click **Edit**. The Edit Administrators dialog box appears.



4. Select the directory object to add as an administrator. For help with custom LDAP groups, see *Adding directory objects*, page 114.

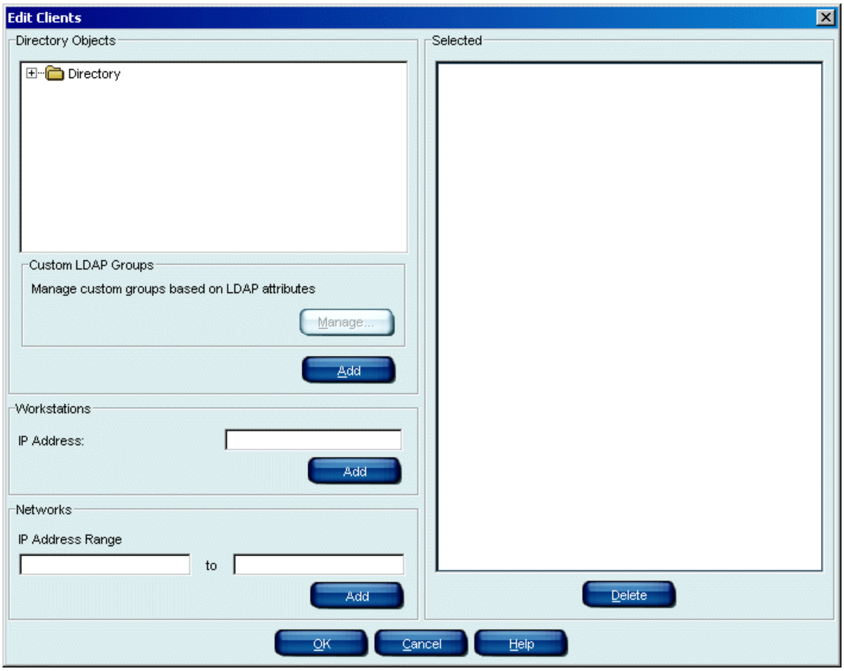
> **Note**
>
> You can add user or group directory objects, but not domains.

5. Click **Add**. The object appears under **Selected** at the right.
6. Check **Policy** to enable this administrator to edit filtering policies governing this clients in this role.
7. Check **Reporting** to enable this administrator to run internet usage reports.
8. Click **OK**.

Adding clients to an administrative role

The clients you associate with an administrative role are managed collectively by the administrators designated to the same role.

1. In the navigation tree, expand **Administration**.
2. Select the role to assign to this client. The user and permission details for that role appear in the content pane.
3. Next to **Managed Clients** in the content pane, click **Edit**. The Edit Clients dialog box appears.



4. Select the client object (directory object, workstation or network) to assign this role.

   For help with custom LDAP groups, see *Adding directory objects*, page 114.

Note

You can add user or group directory objects, but not domains.

5. Click **Add**. The object appears under **Selected** at the right.
6. Click **OK**.

Removing an administrator from a role

If you no longer need an administrator for a role, or need to change who administers that role, remove the administrator.

1. In the navigation tree, expand **Administration**.
2. Select the role from which to remove an administrator.
3. Next to **Managed Administrators** in the content pane, click **Edit**. The Edit Administrators dialog box appears.
4. Under **Selected** at the right, select the user to remove.
5. Click **Remove**.
6. Click **OK**.

Session management

To streamline administration of Policy Servers and prevent configuration conflicts, the Delegated Administration and Reporting feature includes built-in controls for Policy Server sessions in Websense Manager.

When an administrator is logged on to Policy Server via Websense Manager, there is a time limit for the session (30 minutes by default). This time limit is configurable, and can be set to as long as 4 hours.

When an administrator attempts to log on to Policy Server, he is only allowed access if no other administrator is logged on at that time.

When a Policy Server session is about to expire, a warning message appears. At this time, the logged-on administrator can click **Continue** and keep working.

If the session remains inactive, the administrator is logged off, and informed that his session has ended. As soon as the session ends, another administrator can log on.

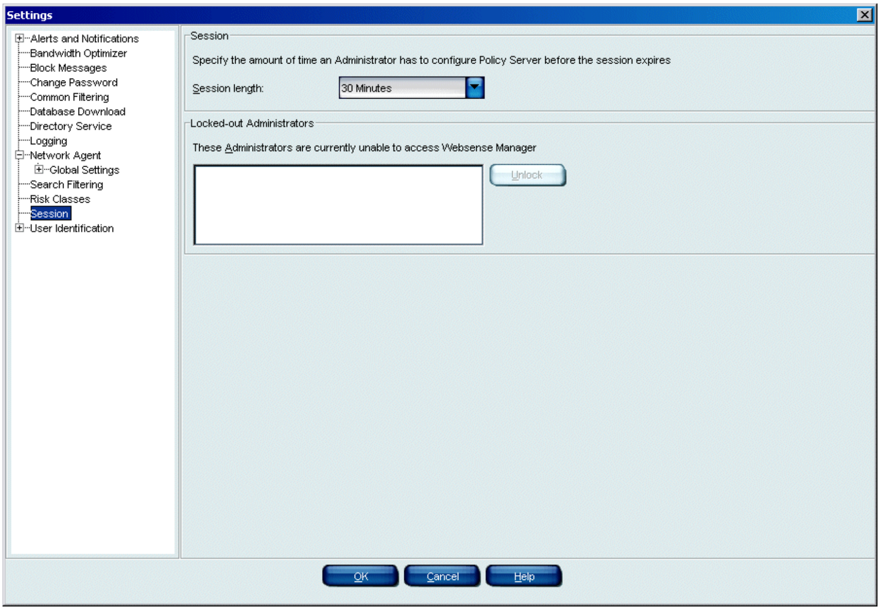
Note

To ensure that configuration settings are preserved as you are working, click **Save Changes** above the navigation tree.

After a session has expired, the administrator has been logged off from Policy Server, and must log on again to continue working.

Changing Policy Server session length

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Session** at the left. The **Session** settings are displayed.



Session

Specify the amount of time an Administrator has to configure Policy Server before the session expires

Session length: 30 Minutes

Locked-out Administrators

These Administrators are currently unable to access Websense Manager

3. Select the desired session length value.
4. Click **OK**.

   Policy Server sessions for the current Policy Server expire after the selected amount of time. Session settings are unique for each Policy Server. If a Super Administrator distributes policy and server settings to other sites, session settings are *not* distributed globally.

Note

If you kill the Websense Manager process (via the `kill -9` command on Linux/Solaris, or the Windows Task Manager), restart the Websense Policy Server and Websense Filtering Service before starting Manager (see *Stopping or starting Websense services*, page 191).

Lockouts

An administrator is locked out from using Websense Manager after the administrator makes 3 failed attempts to log on to Policy Server.

Only the Super Administrator can reset a lockout and allow logon. If a Super Administrator is locked out, then another Super Administrator must reset the lockout.

If there is only 1 Super Administrator and this user has been locked out, contact Technical Support for assistance (see *Websense Technical Services Support Center*, page 337).

Resetting a lockout

1. Select **Server > Settings**.
2. Select **Session** at the left. The **Session** settings are displayed.
3. Next to **Locked-out Administrators**, select the user name of the administrator who has been locked out.
4. Click **Unlock**.
5. Click **OK**.

The selected administrator can log on to Policy Server again, provided no other administrators are logged on to the same Policy Server at that time.

Defining filtering restrictions

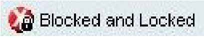
A Super administrator can define key filtering restrictions to be applied to all clients. These restrictions limit which policy elements can be modified by Delegated Administrators. Filtering limitations defined by the Super Administrator are called a Web Filter Lock.

A Super Administrator can also define filtering restrictions on a central Policy Server, and then distribute these settings to other servers. For more information, see *Central Configuration Distribution*, page 235.

When the Web Filter Lock is created and distributed, the Super Administrator can allow Delegated Administrators at other sites to modify the filtering settings that comprise the Web Filter Lock. Or, the Lock can be secured so no modifications can be made.

At a remote site, the Websense Manager content pane indicates which filtering settings have been set and locked by the Super Administrator at the central site. At remote sites, only Super Administrators can modify locked settings.

Block settings applied and locked by the Super Administrator are indicated by a small lock icon. Filtering settings exhibiting this icon are not modifiable by Delegated Administrators.


Blocked and Locked

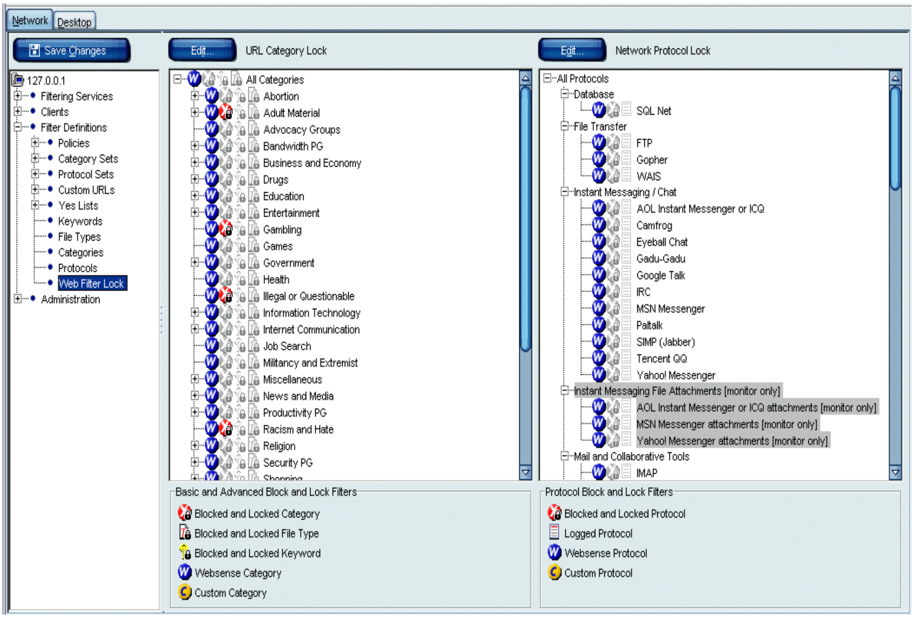
Sample filtering status icon

This section describes how to create a Web Filter Lock. For more information on configuring filtering settings, see *Chapter 9: Setting Up Web Filtering*.

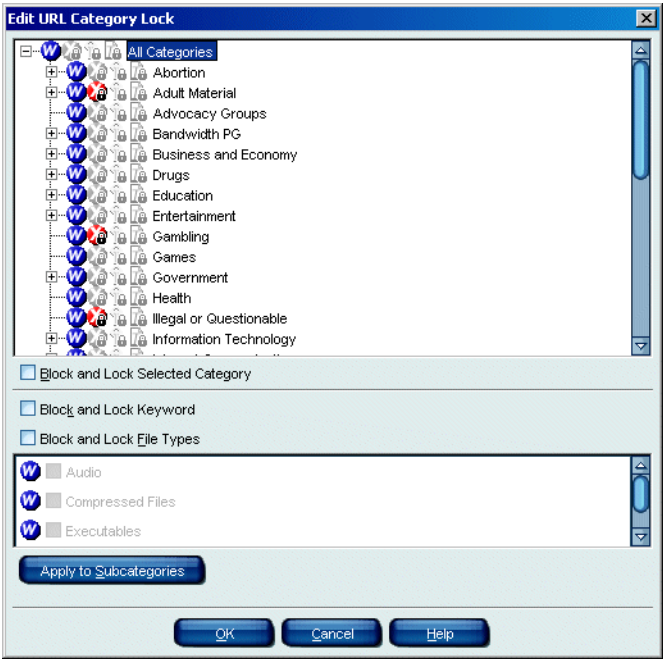
Creating a Web Filter Lock

Use this procedure to create a Web Filter Lock for use by Delegated Administrators, or distribution to remote Policy Servers.

1. In the navigation tree, expand **Filter Definitions > Web Filter Lock**. The URL category and protocol filtering settings comprising the Web Filter Lock are displayed.



2. Next to **URL Category Lock**, click **Edit**. The Edit URL Category Lock dialog box appears.



□ Block and Lock Selected Category

□ Block and Lock Keyword

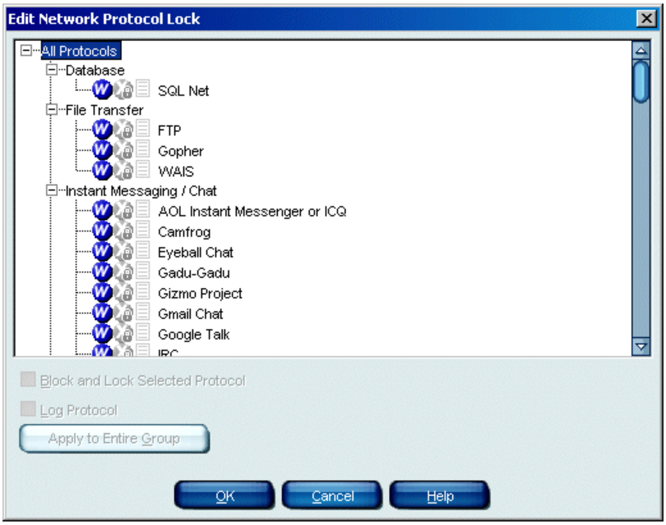
□ Block and Lock File Types

3. Select a category, and then check **Block & Lock Selected Category**. The icon next to the category name changes to reflect its new filtering setting.
4. To apply the same filtering option to the subcategories associated with the category, click **Apply to Subcategories**.
5. To block keywords for the category, check **Block & Lock Keyword**. If this box is checked, enter keywords (see *Adding keywords*, page 270).
6. To apply restrictions based on file extensions, check **Block & Lock File Types**, and then check the file types to block.
7. To apply the same restrictions to the subcategories associated with the category, click **Apply to Subcategories**.

Note

To block a particular file type for *all* categories at once, simply select **All Categories**, block the file type, and then click **Apply to Subcategories**.

8. Repeat Step 3 through Step 7 for each category to set.
9. Click **OK** to close the Edit URL Category Lock dialog box.
10. Next to **Network Protocol Lock**, click **Edit**. The Edit Network Protocol Lock dialog box appears.



Edit Network Protocol Lock

- All Protocols
  - Database
    - SQL Net
  - File Transfer
    - FTP
    - Gopher
    - WAIS
  - Instant Messaging / Chat
    - AOL Instant Messenger or ICQ
    - Camfrog
    - Eyeball Chat
    - Gadu-Gadu
    - Gizmo Project
    - Gmail Chat
    - Google Talk
    - IRC

□ Block and Lock Selected Protocol

□ Log Protocol

11. Select a protocol, and then check **Block & Lock Protocol**.
12. Optionally check **Log Protocol** to include usage for this protocol in alerts and reports.

> **Note**
>
> For administrators to receive usage alerts for a protocol, Log Protocol must be checked. For more information, see *Alerting*, page 199.

13. To apply the selected filtering options to the whole protocol group, click **Apply to Entire Group**.
14. Click **OK**.
15. Click **Save Changes** above the navigation tree.

These filtering restrictions can be implemented by Delegated or Remote Administrators. The Web Filter Lock is the basis for filtering settings that Delegated Administrators maintain.

The Web Filter Lock does *not* affect clients in roles managed directly by the Super Administrator. The Super Administrator has the ability to create or override the Web Filter Lock.

Central Configuration Distribution

The Delegated Administration feature facilitates sharing filtering settings and certain global configuration settings across multiple Policy Servers. Central Configuration Distribution allows a single administrator to define and distribute the following from a central Policy Server:

- Filtering restrictions (Web Filter Lock) to be implemented at other sites (see *Defining filtering restrictions*, page 231)
- Global server settings
- Permission for Remote Administrators to modify these settings at their respective sites

The Super Administrator performing distribution can completely control filtering restrictions and server settings, or allow Remote Administrators to modify certain elements for their sites.

Note

If you are running multiple Policy Servers but only 1 Log Server, see *Multiple Policy Servers with a single Log Server*, page 238 for how to distribute policy data.

Not all server settings are distributed via Central Configuration Distribution. Many server settings are designed to apply to 1 particular server. Distributing only global settings ensures that server-specific configuration does not get overwritten.

Only these global server settings are pushed to other Policy Servers from the central server:

- Risk Classes: all settings (see *Risk classes*, page 78)
- Common Filtering
  - Use more restrictive blocking (see *When multiple group policies apply*)
  - Block users when subscription expires or is exceeded (see *Subscriptions*, page 13)
  - Keyword search options (see *Setting up keyword blocking*, page 269)
  - Password override timeout (see *Enabling password override*, page 122)
  - Continue timeout (see *Continue*, page 43)
  - Quota session length (see *Quotas*, page 44)
  - Default quota time per day (see *Quotas*, page 44)
  - Default quota sessions per day (see *Quotas*, page 44)

Policy Server relationships

By default, the first Policy Server installed is the central Policy Server. Additional Policy Servers are viewed from the central site as remote servers. However, these relationships can change, as you can set any server to be the central Policy Server. Likewise, an administrator managing a non-central site is viewed from the central site as a Remote Administrator. The non-central site can also have additional, Delegated Administrators.

Changing the Central Policy Server

Generally, once a central site is established, it is unlikely that its central status would change. If this does occur, all other servers inherit any global settings distributed from the central server.

1. Select **Server** > **Change Central Server**. The Change Central Policy Server dialog box appears.
2. Select the IP address of the Policy Server to make the central server.
3. Enter the password to be used for access to the new central server.
4. Click **OK**. The **Set New Central Policy Server** confirmation box appears.

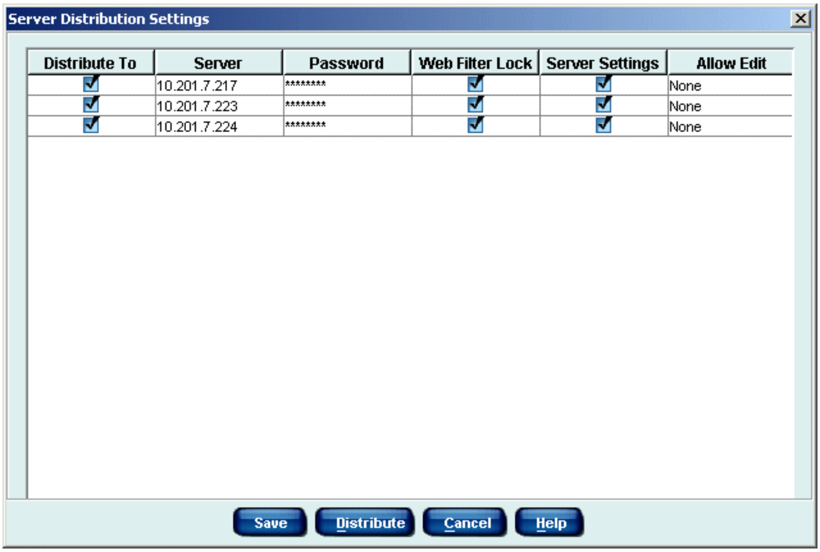
5. Click **OK**. You are disconnected from the current central server, and need to reconnect to the server to continue working.

Distributing configuration settings

Once you have defined a Web Filter Lock (see page 232), you can distribute the Lock to additional sites.

Selected configuration elements are distributed to remote Policy Servers for use by the Remote Administrators at those sites.

1. Ensure that all destination Policy Servers are added to Websense Manager (see *Adding a server*, page 186).
2. Select **Server** > **Distribution Settings**. The Server Distribution Settings dialog box appears.



Server Distribution Settings

Distribute To	Server	Password	Web Filter Lock	Server Settings	Allow Edit
☑	10.201.7.217	********	☑	☑	None
☑	10.201.7.223	********	☑	☑	None
☑	10.201.7.224	********	☑	☑	None

3. Check the box for each Policy Server to which to distribute settings.
4. Enter the password for each destination Policy Server.
5. Select the elements to distribute to each server. To distribute filtering restrictions, check **Web Filter Lock** (see *Defining filtering restrictions*, page 231). To distribute global server settings, check **Server Settings** (see *Central Configuration Distribution*, page 235).
6. For each destination server, click in the **Allow Edit** column, and then select which elements to allow the Remote Administrator to modify.

7. If you are ready to distribute now, click **Distribute**. (Alternatively, click **Save** to save the distribution settings for later use.)
8. In the Confirm Policy Distribution dialog box, click **Continue** to complete distribution.

Multiple Policy Servers with a single Log Server

Websense, Inc., recommends against running multiple Policy Servers with only 1 Log Server. However, if your environment requires such a setup, there is another way to distribute data to remote servers.

In this case, distribute complete policy configuration data to all Policy Servers to ensure that usage data sent to Log Server is consistent. For example, if usage is tracked based on custom categories configured only on 1 Policy Server, usage at another site is logged incorrectly. Synchronizing policy settings across servers maintains the integrity of report output.

⚠ **Warning**

Distributing configuration data in this way overwrites existing settings on the destination Policy Servers, including role definitions. Back up the policy configuration file first (see *Saving the configuration*, page 193).

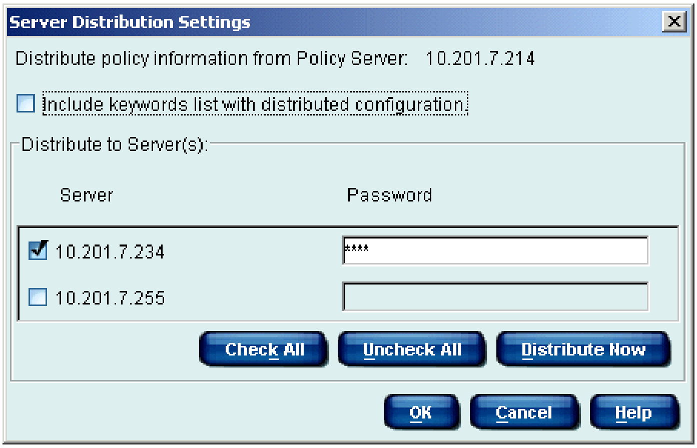
With this distribution method, the following is pushed to all Policy Servers:

- Directory objects (users, groups, workstations, networks) defined in Websense Manager
- Policies and policy settings
- Category sets and their settings
- Bandwidth-based filtering settings (for category sets or protocol sets)
- Custom URLs
- Yes lists
- Keywords
- Custom categories
- **Use more|less restrictive blocking** settings
- Protocol sets
- Custom protocols
- Custom file types
- Roles and role configuration settings
- Common Filtering settings

To distribute policy settings to multiple servers in a Websense Enterprise Corporate Edition environment:

1. Select **Server > Settings**. The Settings dialog box appears.
2. Select **Logging** at the left.

3. Click **Advanced**. The Server Distribution Settings dialog box appears.



Server Distribution Settings

Distribute policy information from Policy Server: 10.201.7.214

□ Include keywords list with distributed configuration

Distribute to Server(s):

Server	Password
☑ 10.201.7.234	****
□ 10.201.7.255	

4. Check the IP addresses of the destination Policy Servers. Use **Check All** or **Uncheck All** to select or deselect all servers.

5. If you have separate directory services at different locations, do the following. (If all locations share the same directory service information, then you do not need to perform this step.)

   a. *Before* distributing policy data from the source location, ensure that objects associated with policies to be distributed exist in the destination directory services. If necessary, have local administrators create directory objects and name them to match the directory objects at the source location.

   b. *After* distributing a policy for the first time, assign the policy to the local directory objects it should govern (see *Assigning policies to clients*, page 304). The policy does not take effect locally until you create the appropriate objects in the local directory service, and then assign the policy to those objects.

6. For each Policy Server selected, enter the password for that server.

   Note

   You must enter a valid password for each destination Policy Server. If no password is entered, distribution will fail for any server that does not have a valid password.

7. Click **Distribute Now** to distribute data now. Otherwise, click **OK** to save distribution settings for later and exit the Server Distribution Settings dialog box.

   Any pre-existing settings on other servers are discarded.

CHAPTER 9 Setting Up Web Filtering

In a first-time installation, Websense software filters users according to your **Initial Filtering** selection during installation. If you selected **Filter Internet traffic based on a predefined policy**, the **Global** policy enforces the Default Settings category set and Default Settings protocol set for all users. If you selected **Monitor Internet traffic only**, the **Global** policy monitors and logs internet traffic, but permits all requests.

When upgraded from an earlier Websense software version, the software brings forward all configuration settings, including policies assigned to clients (users, groups, workstations and networks). After upgrading, review your policies to ensure that they are still appropriate.

About filtering policies

Policies govern user internet access. A policy is a schedule that tells Websense software how and when to filter URLs and protocols. Policies are comprised of:

- **Category sets**: The filtering settings for each URL category, selected in Websense Manager and stored collectively for use in policies.
- **Protocol sets**: The filtering settings for each protocol, selected in Websense Manager and stored collectively for use in policies.
- A schedule that determines when the policy is active for clients governed by it.

Category sets and protocol sets are scheduled into policies by time and day of the week.

Policy-based filtering lets you assign varying levels of internet access to clients. By editing and creating policies, you can schedule different category sets and protocol sets to be applied at different times and for different clients.

Edit the **Global** policy to accommodate your organization, or use it as it is (see *The Global policy*, page 300). Either way, it takes effect for each client until another policy is assigned.

To apply different filtering restrictions to different clients, create new policies or use the sample policies installed with Websense software. For example, you could create:

- One policy that blocks all internet access during working hours but allows access to sports, shopping, and entertainment sites after normal business hours and on weekends;
- A second policy that allows access to all sites during working hours except those containing adult material;
- A third policy that provides unfiltered access to all internet sites 24 hours a day, 7 days a week.

With diverse policies, you can fine-tune filtering by assigning policies to users as appropriate. For example, assign the most restrictive policy to users who rarely need internet access to perform their work. Assign a more liberal policy to employees who rely on internet access for work, and unfiltered access to upper management.

Managing sites and categories

In addition to the filtering settings for URL categories and network protocols, use yes lists, Custom URLs, keywords, file types and bandwidth limits to fine-tune filtering.

Category Sets/Yes Lists

The Websense Master Database contains over 90 categories, covering internet subject matter such as adult material, job search, games, and weapons. It is organized into parent categories and subcategories. For example, the Information Technology category includes subcategories such as Computer Security, Hacking and Proxy Avoidance.

After you enter your subscription key, the list of categories appears in Websense Manager. Once you have entered the key, the list of categories appears, but some categories are marked **[monitor only]**. This indicates that these categories must be purchased separately. Websense software records access to these sites for reporting purposes, but the filtering setting is **Permit** and cannot be changed until the categories are purchased.

✓ **Note**

If you selected **Monitor Internet traffic only** for the **Initial Filtering** option during installation, all categories are marked **[monitor only]**.

You can create custom categories for storing sites to control that are not in the Master Database, and for reclassifying sites so they are filtered differently. For more information, see *Adding a custom category*, page 265.

Filtering settings determine whether Websense software blocks, permits, or limits a site by quota or continue options. Filtering settings for each category are selected via Websense Manager and stored collectively as *category sets*. Category sets are scheduled into policies by time and day of the week.

A yes list is a list of explicitly-allowed URLs used in place of a category set. When a yes list is used in a policy, users governed by that policy are only allowed to access sites on the yes list. For more information, see page 250.

About file types

In addition to filtering based on category sets, you can filter based on file extensions. Combine access to a category set with restrictions on particular types of files from sites within that category set. For example, permit the category **Sports**, but block video files from sites in the **Sports** category.

By default, all files directly associated with category sets using the **Block**, **Limit by Quota**, or **Continue** options are blocked, but you can explicitly permit certain file types. Websense software first determines the URL category of an internet request, and then checks any file extensions against filtering settings for that category. For information, see *Filtering order*, page 35.

To modify filtering settings for categories, see *Editing a category set*, page 257.

To edit the category set for a particular policy only, see *Editing a policy*, page 302.

✓ **Note**

To implement full filtering for video *and* audio internet media, combine protocol-based filtering with file type filtering. In this case, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

When a user tries to access a file whose extension is blocked, the **Reason** field on the Websense block page indicates that the file type was blocked. For more information, see *Block messages*, page 50.

Websense software provides several predefined file types, or groupings of file extensions used for similar purposes.

Implement filtering policies using predefined file types, modify the existing file type definitions, or create new file types. Websense file types are continually updated in the Master Database. You can acquire updates via the nightly Master Database download.

Note

The standard block message does not appear if a GIF or JPEG image comprises just a portion of a permitted page. When the **.gif** or **.jpg** file extension is associated with a blocked file type, the image region appears blank, instead of containing a block message.

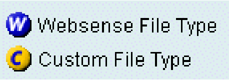
The table shows a sampling of file type definitions.

Audio	Compressed Files	Executables	Video
.aif	.ace	.bat	.asf
.aifc	.arc	.com	.asx
.aiff	.arj	.exe	.avi
.au	.b64		.ivf
.m3u	.bhx		.m1v
.mid	.cab		.mov
.midi	.gz		.mp2
.mp3	.gzip		.mp2v
.oog	.hqx		.mpa
.rmi	.iso		.mpe
.snd	.jar		.mpg
.wav	.lzh		.mpv2
.wax	.mim		.qt
.wma	.rar		.ra
	.tar		.ram
	.taz		.wm
	.tgz		.wmp
	.tz		.wmv
	.uu		.wmx
	.uue		.wxv
	.xxe		
	.z		
	.zip		

Adding a new file type

Add up to 32 file types (groups of file extensions).

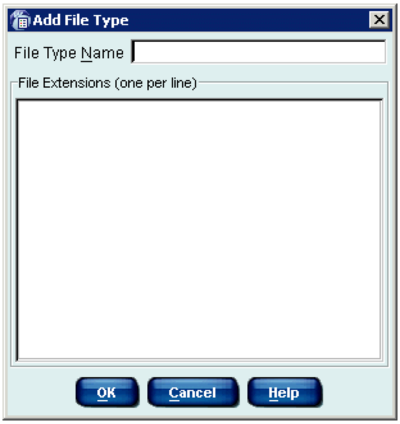
1. Expand **Filter Definitions** > **File Types** in the navigation tree. A list of file types is displayed in the content pane.
2. Websense predefined file types and custom file types are distinguished by the icons shown.



W Websense File Type

C Custom File Type

3. Click **Add File Type**. The Add File Type dialog box appears.



4. Enter a **File Type Name**. (This must differ from any existing file type names.)
5. Type the file extensions, 1 per line, to include in this file type definition. You do not need a dot “.” before each 3-letter extension.
6. Click **OK**. The new file type appears in the **File Types** list.

Editing an existing file type

1. Expand **Filter Definitions** > **File Types** in the navigation tree. A list of file types is displayed in the content pane.
2. Select the file type to modify, and then click **Edit File Type**. The Edit File Type dialog box appears.
3. Add or remove file extensions. (You can only remove file extensions from custom file types.)

> ✓ **Note**
>
> If you add an extension that is already used in a Websense file type definition, your entry takes precedence over the Websense definition. If such a file is blocked, it is filtered and logged as the type you defined, not as the Websense type. You can duplicate a particular extension this way only once.

4. Click **OK**.

Websense category sets

Websense software includes 3 permanent category sets. These cannot be deleted. Only the **Default Settings** category set can be edited.

- **Always Block**: Blocks access to all internet and intranet sites.
- **Default Settings**: The default category set used when a request is not filtered by any other category set. Blocks sites in some categories, permits sites in others, and uses the Limit by Quota filtering option in the remaining categories. Can be edited.
- **Never Block**: Allows total, unrestricted access to all sites.

Websense software also installs category sets designed as models that can be used as is, edited, or deleted.

- **Basic Filtering**: Blocks commonly-restricted categories.
- **Monitor Only**: Permits all categories, and allows logging and reporting on all categories.

Yes lists

Yes lists provide a more flexible method of defining filtering policies. Yes lists can be used to:

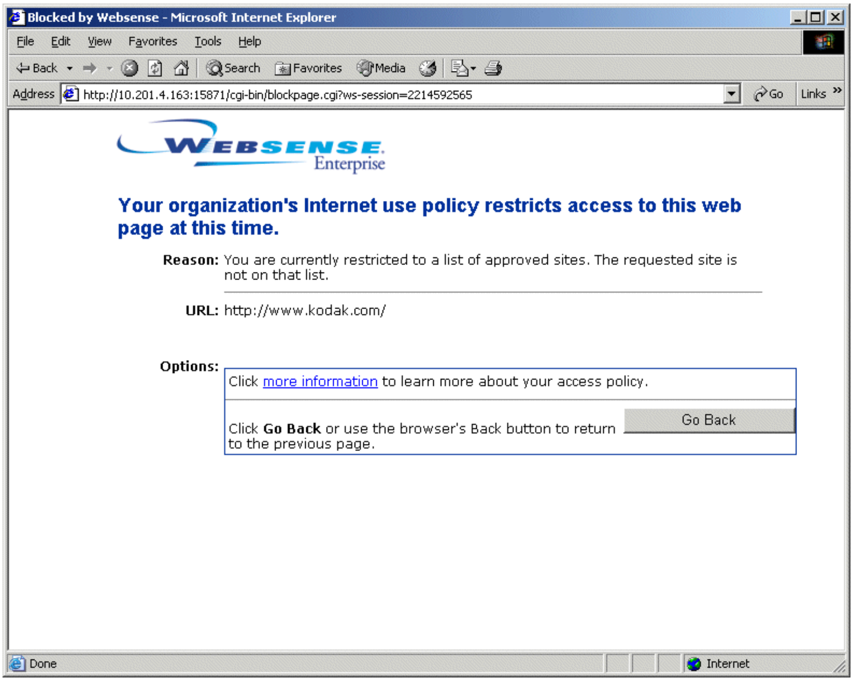
- Allow limited sets of websites for different users or groups governed by the policy using the yes list.
- Single out specific sites to be permitted, even when the categories they are in are blocked.

Websense software can support 2,500 yes lists containing 25,000 URLs in all.

A yes list is active for a particular time period in a policy. Only 1 yes list or category set can be applied to a time period.

URLs on a yes list are allowed for clients governed by the policy that uses the yes list. For example, a policy named Finance has a yes list that includes only financial internet sites. If this policy governs the Accounting group, then members of Accounting can access *only* URLs on the yes list.

When a user is governed by a yes list, a block page is returned for any requested URL not included on that yes list.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
WEBSENSE Enterprise
Done
Internet

http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=2214592565

Your organization's Internet use policy restricts access to this web page at this time.

Reason: You are currently restricted to a list of approved sites. The requested site is not on that list.

URL: http://www.kodak.com/

Options: Click more information to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page. Go Back

Block page for requested URL not on a yes list

Yes lists and filtering precedence

There are special considerations when more than 1 filtering setting applies to a client. Multiple filtering settings can be involved when a user is in more than 1 group, and the groups are governed by different filtering policies. A URL could also be on a yes list and on a custom URL list, both of which affect the same group.

Yes lists and multiple groups

The **Use more restrictive blocking** setting (see *When multiple group policies apply*, page 37) determines what happens when multiple group policies apply. By default, this setting is off. Filtering behavior involving yes lists in combination with **Use more restrictive blocking** may not always be as expected.

Websense software determines which filtering setting is more or less restrictive at the category set/yes list level.

	***Use more restrictive blocking* off (default scenario)**	***Use more restrictive blocking* on**
yes list + **Always Block** category set	yes list (request permitted)	**Always Block** (request blocked)
yes list + permitted category	category set (request permitted)	yes list (request permitted)
yes list + blocked category	category set (request blocked)	yes list (request permitted)
yes list + limited by quota/ continue category	category set (request limited by quota/ continue)	yes list (request permitted)
yes list + Custom URL/Not Filtered	Custom URL/Not Filtered (request permitted)	yes list (request permitted)

By default, if a URL is both in a particular category and on a yes list, and both are in active policies, the least restrictive filtering case is used—so the filtering setting for the *category* takes precedence. A category set is considered less restrictive than a yes list.

When **Use more restrictive blocking** is active, a yes list takes precedence because it is the more restrictive filtering case. If a user is in multiple groups with different policies, and one policy has a yes list instead of a category set, the user can access *only* the URLs on the yes list.

By default, yes lists take precedence over the **Always Block** category set. When **Use more restrictive blocking** is active, this behavior is reversed: If a yes list and the **Always Block** category set both apply at the same time, **Always Block** takes precedence as the more restrictive case.

Yes Lists and Custom URLs/Not Filtered

Yes lists and Custom URLs/Not Filtered are separate entities. Yes lists are viewed, created and modified much like custom URLs. However, yes lists only become active when applied in policies. Meanwhile, custom URL lists always affect filtering for all users.

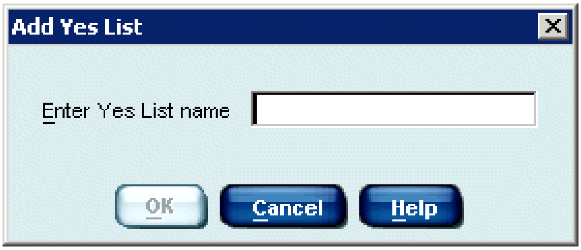
By default, if the same URL is on both a yes list and the Custom URLs/Not Filtered list, the URL is permitted. The exception is if the **Always Block** category set is active at the time, and **Use more restrictive blocking** is *on*.

The list that is active at the time of a request allows the URL, and is logged for reports. For more information, see *Custom URLs*, page 259.

Adding a yes list

Create a yes list by assigning it a name, and then entering a list of allowed URLs. Then, apply the yes list to clients (see *Applying a yes list to clients*, page 255).

1. Right-click in the navigation tree, and select **Add Yes List**. The Add Yes List dialog box appears.



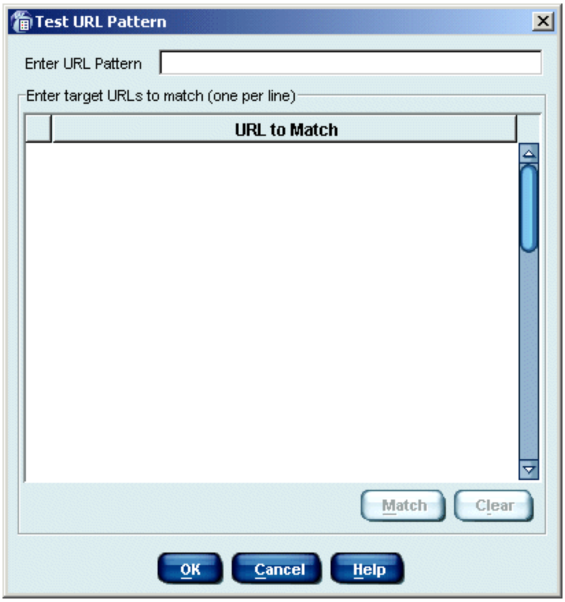
2. Enter a name for the yes list (for example, **HR Sites**).
3. Click **OK**. The yes list you created appears under **Yes Lists** in the navigation tree.
4. Click to select the yes list just created. Details for the yes list appear in the content pane.

5. Enter the URLs or URL patterns to be included in this yes list. URL patterns can be in regular expression form (see *URL pattern matching*, page 68).

   URLs must be separated with at least a space.

6. If you entered URL patterns, verify that a pattern matches the desired URL:

   a. Click **Test URL Pattern**. The Test URL Pattern dialog box appears.



   b. Enter the URL pattern to test.

   c. Type the intended (target) URLs.

   d. Click **Match**, and verify that the matched URLs are correct.

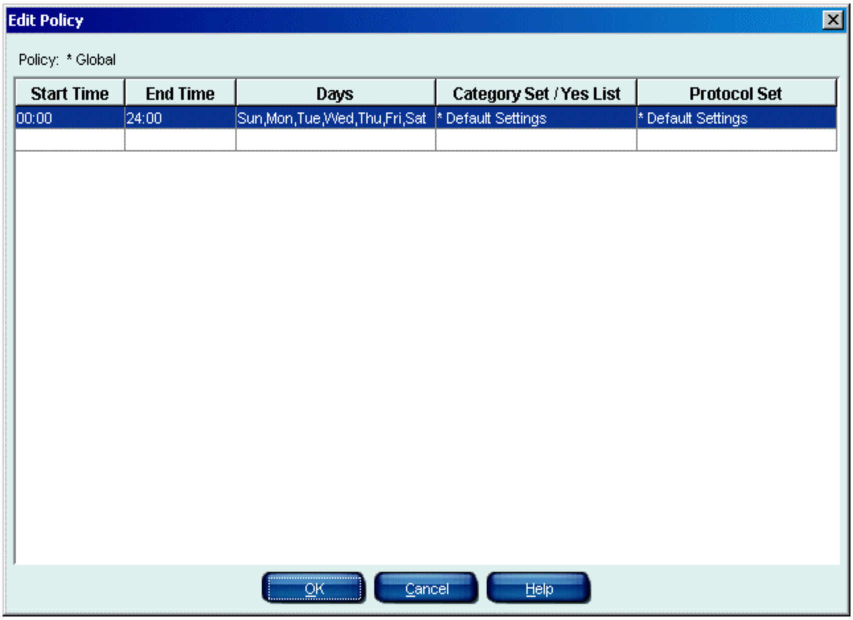
   e. Click **Clear** to clear the URLs and test another pattern.

   f. Click **OK** when finished.

7. Click **Save Changes** above the navigation tree.

Applying a yes list to clients

1. Create a yes list (see *Adding a yes list*, page 253).
2. Locate the policy to govern this group of clients. To create a policy, see *Adding a policy*, page 301.
3. Select the desired policy in the navigation tree to display its definition in the content pane.
4. Click **Edit**. The Edit Policy dialog box appears.



Policy: * Global

Start Time	End Time	Days	Category Set / Yes List	Protocol Set
00:00	24:00	Sun,Mon,Tue,Wed,Thu,Fri,Sat	* Default Settings	* Default Settings

5. Double-click under **Category Set/Yes List** and select the yes list created earlier.

Note

Only 1 yes list can be selected for a time period in a policy. This also means that only 1 yes list can be applied to a particular object (user, group, workstation or network).

6. To make any other changes to the policy, see *Editing a policy*, page 302.
7. Click **OK**.
8. Click **Save Changes** above the navigation tree.

9. Assign the policy to a group (see *Assigning policies to clients*, page 304). This group can access only the URLs on the yes list during the time periods specified in the policy.

Adding a category set

Add as many category sets as needed. For example, create a category set for Marketing that permits all sites except adult material, and another for Accounting that also blocks entertainment and shopping sites.

Once a new category set is created, it must be added to a policy to determine when to enforce it and for which clients.

To add a category set:

1. Right-click in the navigation tree, and then select **Add Category Set**. The Add Category Set dialog box appears.
2. Enter a name for the new category set, and then click **OK**.
3. In the Category Set Model dialog box, select an existing category set as the basis for the new set.
4. Click **OK**.

The new category set remains a replica of the category set it is based on until it is edited, and is not enforced until it is added to a policy (see *About filtering policies*, page 243).

Editing a category set

Edit category sets to change the filtering settings for any or all categories.

To review a category set, expand **Category Sets** in the navigation tree and select the category set name.

1. Select a category set in the navigation tree to display its settings in the content pane. (The **Always Block** and **Never Block** category sets are not shown because these do not have variable filtering settings.)
2. Click **Edit**. The Edit Category Set dialog box appears.
3. Select a category, and then select the desired filtering options.

Filtering Setting	Function
Permit	Permits access to all sites in the selected category.
Block	Blocks access to all sites in the selected category.
Limit by Quota	Lets the user continue and view the site or view any other site in a quota category for a short time.
Continue	Lets the user continue and view the site for a limited amount of time, defined via **Server > Settings > Common Filtering**. For more information, see *Continue*, page 43.
Block Keyword	Blocks sites whose URLs contain keywords assigned to the category set (see *Keywords*, page 268). If this option is selected, you must define keywords (see *Adding keywords*, page 270).
Block File Types	Blocks files having extensions associated with file types assigned to the category set.
Block Selected Category when [Entire Network/ HTTP] traffic exceeds [N%/ Default] of available bandwidth	Blocks internet content based on bandwidth usage associated with the URL categories governed by a filtering policy. For example, a policy blocks the sites in its category set if total network bandwidth usage exceeds 50% of available network bandwidth. For more information, see *Bandwidth and categories*, page 297.

4. To apply the same filtering option to the subcategories associated with this category, click **Apply to Subcategories**..

5. To apply the same restrictions to the subcategories associated with the category, click **Apply to Subcategories**.
6. Repeat for each category to modify.
7. Click **OK** to close the Edit Category Set dialog box.
8. Click **Save Changes** above the navigation tree.

If the category set is already included in a policy, the new filtering settings are enforced when that category set is active. If the category set is not part of any policy, it must be added to a policy. For more information, see *Editing a policy*, page 302.

> ✓ **Note**
>
> Filtering options for Premium Groups cannot be changed unless the groups have been purchased from Websense, Inc.

Copying a category set

To create identical category sets with different names:

1. Select the category set to copy in the navigation tree.
2. Click **Save As** in the content pane. The Add Category Set dialog box appears.
3. Type the new name of the copied category set.
4. Click **OK**.
5. Click **Save Changes** above the navigation tree.

Custom URLs

Custom URLs let you:

- Add sites to Websense software that are not in the Websense Master Database.
- Filter sites differently than their Master Database categories.

Websense software considers custom URLs before URLs in the Master Database, and therefore filters the site according to the category assigned to the custom URL.

Websense Manager offers two custom URL lists:

- The Custom URLs/Not Filtered list lets you specify internet sites to be permitted for all users, regardless of how the site's category is filtered. (The exception is the **Always Block** category set, which blocks all internet access.)
- The Custom URLs/Recategorized list lets you:
  - Classify sites that are not in the Master Database by adding them to a database category. Websense software filters these sites according to the filtering setting for that category.
  - Reclassify sites that already exist in the Master Database. Single out sites to be filtered differently than their original categories. For example, block a site in an otherwise-permitted category.

You can also create new categories in which to store custom URLs (see *Adding a custom category*, page 265).

Custom-permitting sites

The Custom URLs/Not Filtered list permits specified sites for all clients, except those filtered by the **Always Block** category set or governed by a yes list (see *Yes lists*, page 250).

When a URL is added to the Custom URLs/Not Filtered list with its original Master Database category association, the URL is permitted as a custom URL, and logged under the original category name. However, if a URL is added under a different category, the URL is permitted as a custom URL, but logged under the *new* category name.

✓ **Note**

Unlike with sites in the Master Database, Websense software cannot match a custom URL with its equivalent IP address. To permit both the text URL and the IP address of a site, add both to the Custom URLs/Not Filtered list.

To custom-permit a URL, see *Adding a custom URL*, page 262.

Recategorizing URLs

Recategorizing custom URLs lets you:

- Filter sites not contained in the Master Database
- Reclassify existing Master Database sites to filter them differently

Associate each site with either a Master Database category or a custom category (see page 265). All sites on the Custom URLs/Recategorized list are filtered according to the settings for their associated categories (Filtering options vary by category set.)

✓ **Note**

Websense software considers custom URLs before Master Database URLs, and therefore filters the site according to the category assigned to the custom URL.

Adding a site to the Custom URLs/Recategorized list does not mean Websense software blocks it. To block the site, associate it with a category that is blocked or limited by quota in the appropriate category set.

For example, the category **Business & Economy** is permitted. To block a particular commercial real estate site in that category, add that site to a recategorized custom URLs list, and associate it with the blocked category **Shopping: Real Estate**.

✓ **Note**

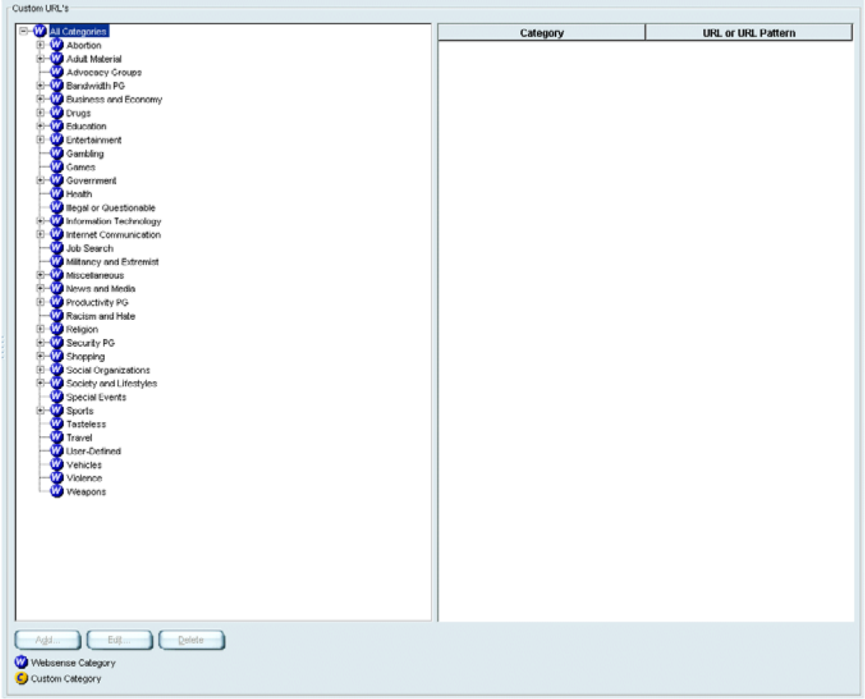
If a recategorized custom URL is associated with a category set whose filtering option is set to **Permit** or **Limit by Quota,** then the recategorized custom URL is permitted or quota-limited whenever the category set is active.

Unlike sites in the Master Database, Websense software cannot match a custom URL with its equivalent IP address. To filter both the text URL and the IP address of a site, add them both as recategorized custom URLs.

To recategorize a URL, see *Adding a custom URL*, page 262.

Adding a custom URL

1. Expand **Custom URLs/Not Filtering** or **Custom URLs/Recategorized** in the navigation tree. The custom URL editor is displayed in the content pane.



2. Select a category with which to associate the site.
3. Click **Add.** The Add Custom URL dialog box appears.
4. Type the full URL for each site to filter under this category. Press **Enter** after each entry (each URL must be on a separate line).

Include the protocol for any non-HTTP site – for example, https://63.212.171.196:443. If the protocol is omitted, Websense software filters the site as an HTTP site.

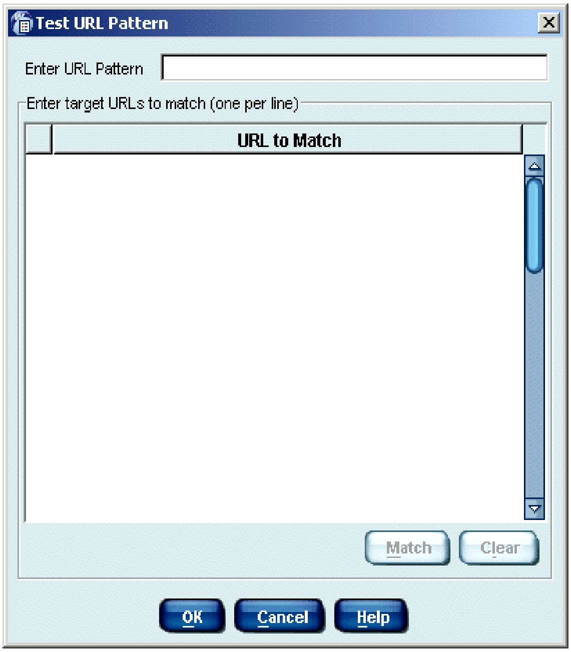
Note

Websense software recognizes custom URLs exactly as they are entered (much like keywords). If Yahoo! sites are blocked, but you enter http://www.yahoo.com as recategorized custom URL, that site is permitted only if users type the full address. If a user types just yahoo.com, the site is still blocked. Meanwhile, if yahoo.com is entered as the custom URL, all sites with yahoo.com in the address are permitted.

5. Alternatively, enter URL patterns to be treated as custom URLs, 1 at a time. URL patterns can be in regular expression form.

   To verify that regular expressions match the desired URLs:

   a. Click **Test URL Pattern**. The Test URL Pattern dialog box appears.



   b. Enter the URL pattern to test.
   c. Type the intended (target) URLs. Press **Enter** after each entry.
   d. Click **Match**, and verify that the matched URLs are correct.
   e. Click **Clear** to clear the URLs and test another pattern.
   f. Click **OK** when finished.

6. Click **OK**. Newly-added URLs appear at the end of the list.
7. Repeat Step 2 through Step 6 for each category to which to add custom URLs.
8. Click **Save Changes** above the navigation tree.

Sites with multiple addresses

The custom URLs feature also lets you ensure that sites or sub-pages not classified under specific categories in the Master Database are effectively filtered.

Sites With Multiple URLs

Some sites can be accessed via multiple URLs. Set up each URL as a custom URL to ensure that the site is permitted or blocked as intended.

For example, http://www.performancebikes.com is a recategorized custom URL for a bicycle shop's site. However, the site can be accessed via http://www.performance*bikes*.com or http://www.performance*cycles*.com. In this case, only requests for http://www.performance*bikes*.com (the exact recategorized URL) are blocked. Requests for http://www.performance*cycles*.com are permitted.

To ensure that users are always filtered when requesting a custom URL, enter a separate custom URL for each URL that can be used to access the site.

Sites with redirected URLs

An organization might move its website to a new server, and then use the HTTP redirect or refresh feature to redirect users to the new URL. If you add the original site to the Custom URLs/Not Filtered list, users are still blocked when they are redirected, because the new site has not been set up as a custom URL. In this case, set up separate custom URLs for the original and new URLs.

To determine whether a site redirects to a different URL, request the site through your browser. After the site opens, check the URL in the address bar. If this URL is different, set up separate unfiltered custom URLs for both addresses.

Adding a custom category

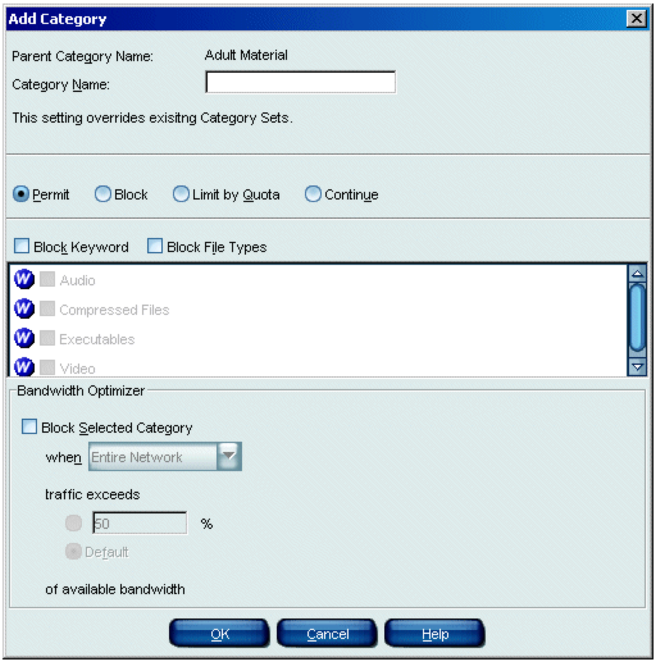
Custom categories provide more precise filtering and reporting. For example, create a custom category called **Business Related** and populate it with sites used for daily business. Add sites not in the Master Database to this category, as well as sites listed under different categories in the database.

Custom categories become subcategories of existing Master Database categories, and are filtered according to parent category settings.

Add or view custom categories wherever a category list is shown in Websense Manager, up to 100 custom categories.

1. Expand **Filter Definitions** > **Categories** in the navigation tree. Alternatively, select any custom URLs list or keyword topic in the navigation tree. A category list appears.
2. Right-click the category under which to create a custom category, and then select **Add a Custom Category**. The Add Category dialog box appears.

3. Enter a **Category Name**. Do not use special characters, such as ! or #.



Add Category

Parent Category Name: Adult Material

Category Name:

This setting overrides exisitng Category Sets.

● Permit ○ Block ○ Limit by Quota ○ Continue

□ Block Keyword □ Block File Types

□ Audio

□ Compressed Files

□ Executables

□ Video

Bandwidth Optimizer

□ Block Selected Category

when Entire Network

traffic exceeds

○ 50 %

○ Default

of available bandwidth

4. Select a filtering setting for this category (**Permit** by default). This setting applies to all category sets (except for **Monitor Only**, **Always Block** and **Never Block** – see *Websense category sets*, page 249).

5. To apply keyword, file type, or bandwidth-based filtering, check the appropriate settings.

6. Click **OK**. The custom category appears everywhere there is a category list.

7. Click **Save Changes** above the navigation tree.

To modify filtering settings for this category in particular category sets, see *Editing a category set*, page 257.

For more information on filtering settings, see *Editing a category set*, page 257.

Editing a category

Apply a global filtering setting to a Websense or custom category. This setting overrides filtering settings you have defined in category sets.

1. Expand **Filter Definitions** > **Categories** in the navigation tree.
2. Select the category to edit.
3. Click **Edit Category**. The Edit Category dialog box appears.
4. Select a filtering setting for this category (**Permit** by default). This setting applies to all category sets (except for **Monitor Only**, **Always Block** and **Never Block** – see *Websense category sets*, page 249).
5. To apply keyword, file type, or bandwidth-based filtering, check the appropriate boxes. For more information, see *Editing a category set*, page 257.
6. Click **OK**. The custom category appears everywhere there is a category list.
7. Click **Save Changes** above the navigation tree.

Deleting a custom category

Deleting a custom category also deletes any keywords and custom URLs associated with that category.

1. Right-click the custom category to delete in any category list, and then select **Remove this Category**.
2. Select **Yes** when asked to confirm.
3. Click **Save Changes** above the navigation tree.

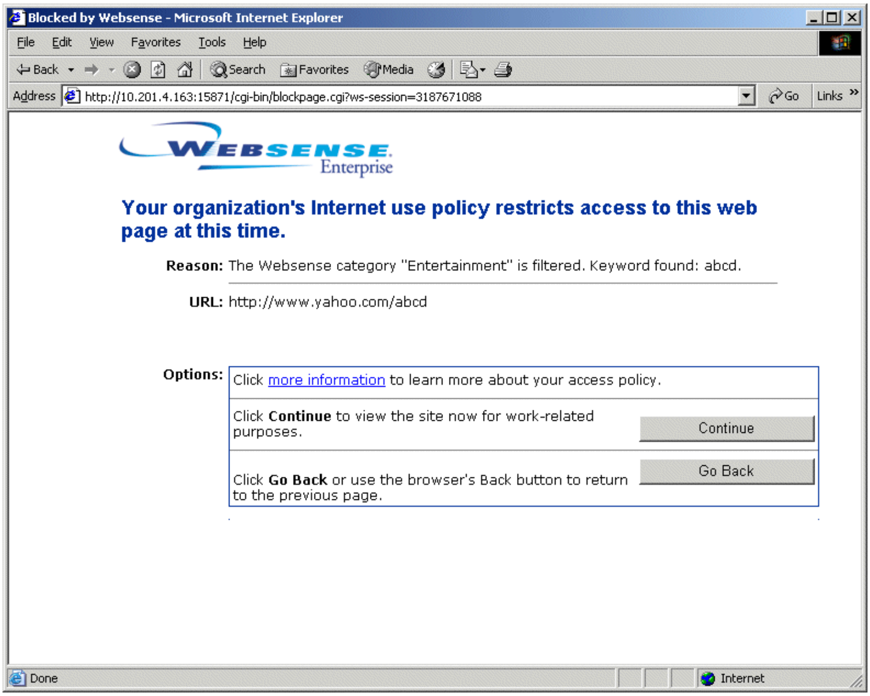
Keywords

Keywords offer protection against sites that have not explicitly been added to the Master Database or a custom URLs list. Keywords are associated with categories in the Master Database.

When the **Block Keyword** setting is active for a category, Websense software blocks any site in that category whose URL contains an associated keyword. You must specify a keyword for the category (see *Adding keywords*, page 270).

The site is blocked by the keyword feature regardless of whether the category is blocked or permitted according to the active policy. For example, even if the category Adult Content is permitted according to the active policy, the URL http://www.webporn.com is blocked if you have associated the keyword “porn” with the Adult Content category.

When a request is blocked based on a keyword, this is indicated on the Websense block page.



Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=3187671088
Go Links
WEBSENSE Enterprise
Continue
Go Back
Done
Internet

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Entertainment" is filtered. Keyword found: abcd.

URL: http://www.yahoo.com/abcd

Options:

Click more information to learn more about your access policy.

Click **Continue** to view the site now for work-related purposes.

Click **Go Back** or use the browser's Back button to return to the previous page.

Block page for a blocked keyword

The **Block Keyword** option is available at the category set level. For more information, see *Editing a category set*, page 257.

Keyword blocking may result in unintended blocking. For example, blocking the keyword *sex* blocks access to sites such as http://www.sex.com (an adult material site), but can also block search engine requests for words like *sextuplets* or *City of Essex*, which have the word embedded in them.

Setting up keyword blocking

1. Select **Server** > **Settings**. The Settings dialog box appears.
2. Select **Common Filtering** at the left, and then select the desired **Keyword search options**. Available settings are:
   - **CGI only**: Blocks sites when keywords appear in CGI query strings (after the "?" in a URL). Websense software does not search for keywords before the "?" when this is selected.

     Example: **http://search.yahoo.com/bin/search? p = Websense**

     CGI query string

     For more information, see *CGI requests*, page 70.
   - **URL only**: Blocks sites when keywords appear in the URL. If the requested address contains a CGI query string, Websense software searches for keywords up to the "?".
   - **URL and CGI**: Blocks sites when keywords appear anywhere in the address. If a CGI query string is present, Websense software searches for keywords both before and after the "?".

   Warning

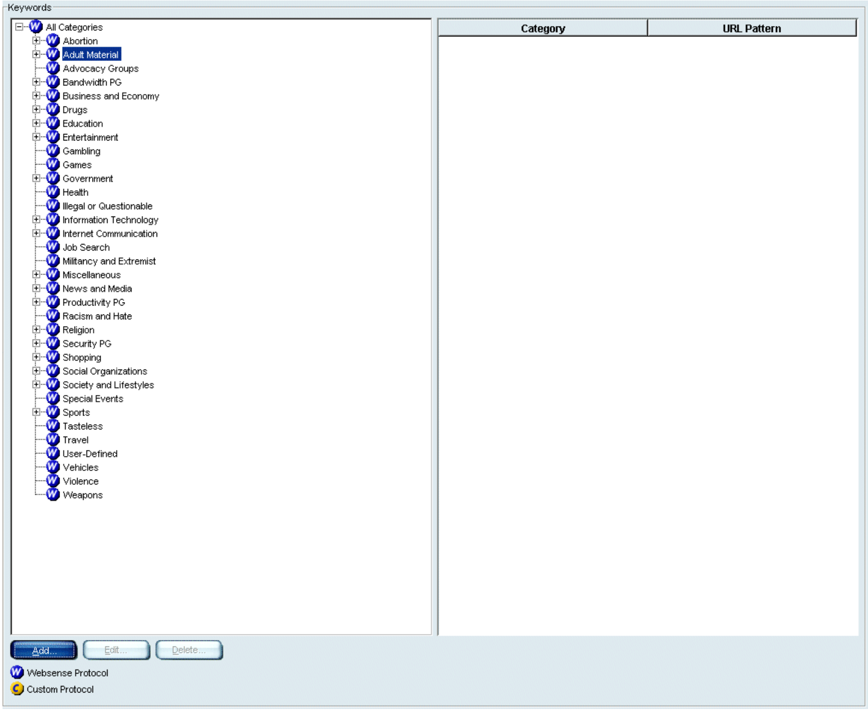
   Do not select **Disable keyword blocking**. This turns off all keyword blocking, even if **Block keywords** is selected for a category.

   For more information, see *CGI requests*, page 70.
3. Click **OK**.
4. Expand **Filter Definitions** in the navigation tree, and select **Keywords** to open the keyword editor.
5. Add keywords (see *Adding keywords*, page 270) and associate them with Websense categories.

6. Select a named category set in the navigation tree, and then click **Edit Category Set.**
7. Check **Block Keyword** for any category to which you associated keywords (see page 257).
8. Add the keyword-blocking category set to a policy (see *Editing a policy*, page 302), and then assign this policy to clients (see *Assigning policies to clients*, page 304).

Adding keywords

1. Select **Keywords** in the navigation tree to display the keyword editor.



2. Select a category under **Choose a category**.
3. Click **Add**. The Add Keyword dialog box appears.

4. Enter the keywords for the selected category.

    - Enter each word on a separate line. Filtering Service interprets each line as a single keyword.
    - Do not use spaces between words. URL and CGI strings do not contain spaces between words. Filtering Service matches exact words or character strings that you have entered as keywords.
    - Enter a backslash (\) before any special characters such as a period (.), comma (,), pound sign (#), question mark (?), asterisk (*), or plus sign (+).

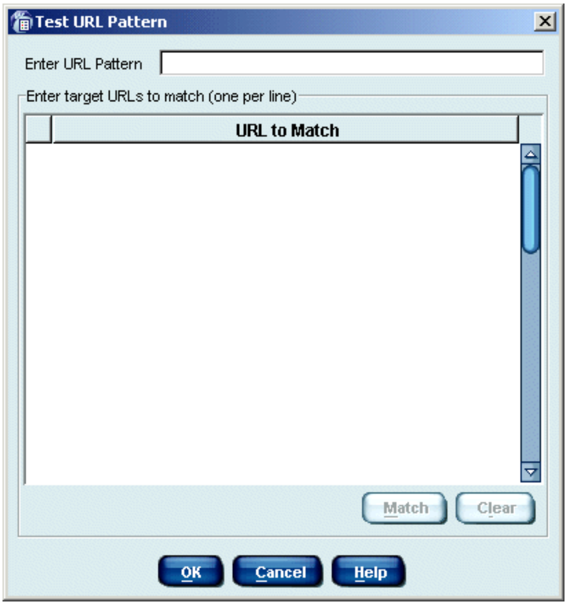
      For example, to block all URLs or CGI strings that include the characters *.cfm*, enter *\.cfm*. If you do not use the backslash, Websense software ignores the period, and matches any URL or CGI string that includes *cfm*.

      A special character may also be within a keyword. Instead of entering *team#1*, enter *team\#1* to make the pound sign (#) part of the keyword.

5. Click **OK**. The keywords and their associated category are listed at the bottom of the keyword editor.

6. If you entered regular expressions, verify that the expressions match the desired URLs:

a. Click **Test URL Pattern**. The Test URL Pattern dialog box appears.



b. Enter the URL pattern to test.

c. Type the intended (target) URLs.

d. Click **Match**, and verify that the matched URLs are correct.

e. Click **Clear** to clear the URLs and test another pattern.

f. Click **OK** when finished.

7. Click **Add Keywords**.

8. Repeat Step 2 through Step 7 for each category to which to add keywords.

9. Click **Save Changes** above the navigation tree.

Note

Keyword blocking occurs only after you enable it via the Settings dialog box and in the appropriate category sets (see *Setting up keyword blocking*, page 269).

Deleting keywords

1. Select **Keywords** in the navigation tree to display the keyword editor.
2. Under **Choose a Category**, select the category from which to delete keywords.
3. Select the keyword to delete from the list at the bottom of the content pane.

   To select multiple keywords, press the **Ctrl** key while clicking keywords. To select a range of keywords, hold down the **Shift** key while clicking the first and last keywords in the range.
4. Click **Remove**. Click **Yes**, and then confirm the request.
5. Repeat Step 2 through Step 4 to delete keywords from a different category.
6. Click **Save Changes** above the navigation tree.

Disabling keyword blocking

You do not have to delete keywords from every category to turn off all keyword blocking.

1. Select **Server > Settings**, and then select **Common Filtering** at the left.
2. Select **Disable keyword blocking** for **Keyword search options**.

Managing protocols

The Dynamic Protocol Management and Bandwidth Optimizer features enable internet filtering based on protocol, application and bandwidth usage. The Websense Network Agent enables protocol management. For more information, see *Network Agent*, page 81.

Websense software allows filtering of internet protocols other than HTTP, HTTPS and FTP. This includes protocols, internet applications, or other data transfer methods such as those used for instant messaging, streaming media, file sharing, file transfer, internet mail, and other network or database operations.

Websense software can also filter protocols or applications that bypass a firewall by tunneling through ports normally used by HTTP traffic. Instant messaging data, for example, can enter a network whose firewall blocks instant messaging protocols by tunneling through HTTP ports. Websense software accurately identifies these protocols, and filters them according to policies you configure.

✓ **Note**

Protocols or internet applications are blocked only if they are not already running. Existing sessions are not interrupted if the policy blocking protocols takes effect after they are already running.

Websense reports show the original protocol providing the data, and whether or not that protocol was successfully permitted or blocked. For more information about Reporting Tools and their capabilities, see the Reporting documentation.

This section discusses protocols in these contexts:

- Defining and managing protocols and internet applications as objects
- Port and destination server address blocking
- Filtering based on bandwidth usage
- User identification
- Configuring protocol-based filtering

Defining protocols

Websense, Inc., groups together similar types of internet protocols and applications to manage internet traffic.

Existing protocol definitions are called Websense protocols, and are sorted into named groups such as **Instant Messaging** and **File Transfer**. Protocol groups are housed in the Websense Master Database, and are verified and updated as frequently as nightly. For a list of available protocols, go to www.websense.com, and then navigate to the Products & Services page. Select the Master Database option.

Websense protocols are defined by the ports they use, IP address, or a signature identifying the protocol.

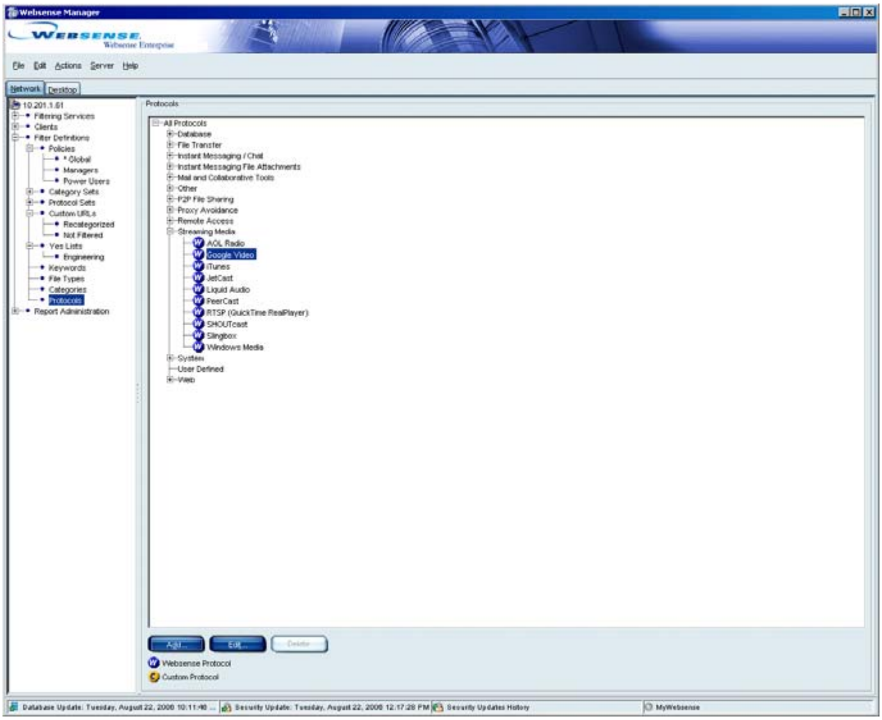
> **Note**
>
> Users may initially be able to access certain blocked P2P File Sharing protocols. This is because P2P File Sharing protocols are signature-based rather than port-based. A connection can be made over any available network port. However, any file sharing or download activities are subsequently blocked.

In addition to the protocols Websense, Inc., provides, create and edit custom protocols. Custom protocol definitions can be based on IP addresses or port numbers, and can be edited. Websense protocol definitions cannot be edited.

A *protocol set* is a list of the protocols managed by a particular policy, plus the filtering settings applied to each of those protocols. View and edit protocols and protocol sets via Websense Manager.

1. Expand **Filter Definitions** in the navigation tree, and then select **Protocols**.

2. Select a protocol to display its definition.



Protocol list in Websense Manager

Protocol definitions are not used in filtering unless they are used in a policy. It is possible to have protocols defined, but not actively used in filtering (i.e., not marked for blocking or logging).

By default, new protocols are permitted but not logged. You can change this behavior for a new protocol (see *Creating a custom protocol*, page 285). To change this only for a particular policy, edit the protocol set used in that policy.

How protocols are filtered

When a protocol request is made, Websense software:

- Determines the protocol (or internet application) name.
- Identifies the protocol based on the request destination address.
- Searches for related port numbers or IP addresses in custom protocol definitions.
- Searches for related port numbers, IP addresses, or signatures in Websense protocol definitions.

If Websense software cannot determine any of this information, all content associated with the protocol is permitted.

Blocking ports, IP addresses and signatures

Websense software can block internet content transmitted over particular ports or IP addresses, or marked by particular signatures, regardless of the nature of data.

Websense software filters internet content transmitted over particular ports or IP addresses, or marked by particular signatures, regardless of the nature of data.

By default, blocking a port intercepts all internet content entering your network over a particular port, regardless of its source.

To block traffic over a specific port, associate that port number with a protocol, and then define that protocol as **Blocked**. For example, if the Internet Relay Chat protocol (IRC) is defined as **Blocked**, and has the port number 161 associated with it, all IRC traffic bound for port 161 is blocked.

To define a protocol by port number, see *Creating a custom protocol*, page 285 and *Adding to a Websense protocol definition*, page 289.

Note

Occasionally, *internal* network traffic sent over a particular port may not be blocked, even when the protocol using that port is blocked. The protocol may send data via an internal server more quickly than the Websense Network Agent can capture and process the data. This does not occur with data originating outside the network.

Some Websense-defined protocols allow blocking of outbound internet traffic destined for an external server—for example, a specific instant messaging server. Only Websense-defined protocols with dynamically-assigned port numbers can be blocked as outbound traffic. For example, if the Websense protocol MSN Messenger is blocked, MSN Messenger traffic sent from within your network to an external server is blocked.

To suggest that a particular server be added to the list of destination servers that can be blocked, go to:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php

TCP and UDP support

Websense software logs bandwidth used for TCP-based protocols, and for selected UDP-based protocols. All data is included in bandwidth usage measurements regardless of any restrictions placed on end-user internet access. For more information about managing network bandwidth, see *Managing bandwidth*, page 295.

In addition to filtering applications that use TCP-based protocols, Websense software filters applications that use both TCP- and UDP-based messages. If an application's initial request over the network is made via TCP, but subsequent data is sent via UDP, Websense software blocks the initial TCP request and thus blocks any subsequent UDP traffic.

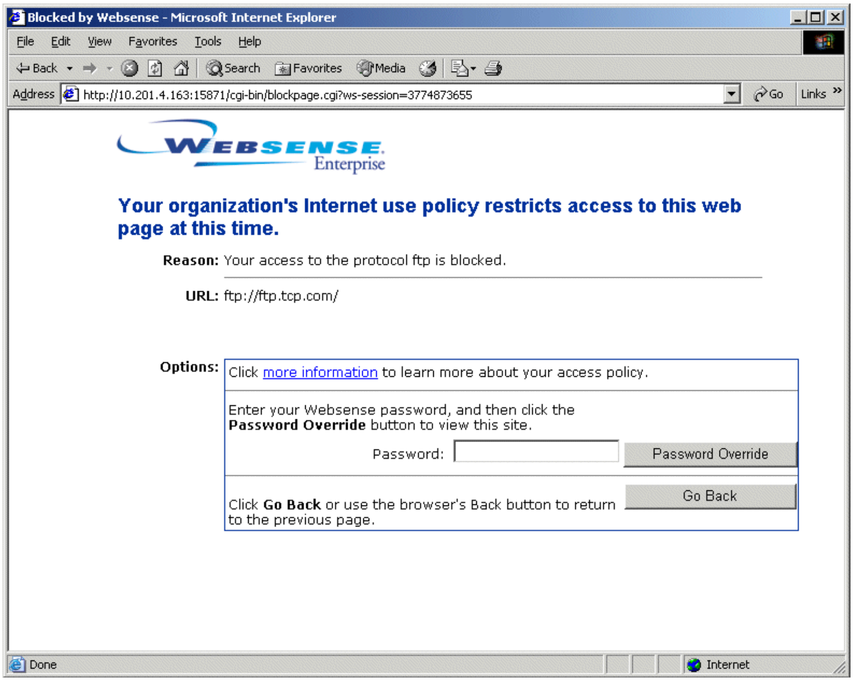
✓ **Note**

UDP requests are not actually blocked, though they are logged as blocked.

Block messages and protocols

When a protocol is blocked, and a user requests content associated with that protocol, Websense software notifies the user.

- For blocked HTTP requests, a standard HTML block page is displayed, as shown. The exception is when no proxy is used (for example, Websense software is integrated with a firewall). In this case, a block message is displayed instead of an HTML block page.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.201.4.163:15871/cgi-bin/blockpage.cgi?ws-session=3774873655
Go Links
WEBSENSE Enterprise
Password Override
Go Back
Done
Internet

Your organization's Internet use policy restricts access to this web page at this time.

Reason: Your access to the protocol ftp is blocked.

URL: ftp://ftp.tcp.com/

Options: Click more information to learn more about your access policy.

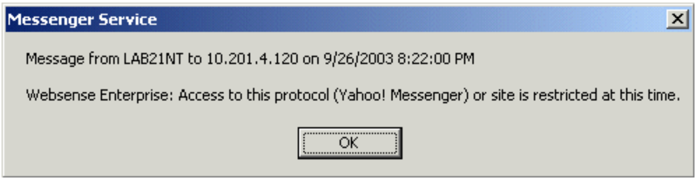
Enter your Websense password, and then click the **Password Override** button to view this site.

Password:

Click **Go Back** or use the browser's Back button to return to the previous page.

Protocol block page

- For non-HTTP blocked requests, a protocol block message is displayed, as shown. The exception is that FTP, HTTPS and Gopher requests made from within a browser *and* passing through a proxy server trigger a block page instead.



Messenger Service

Message from LAB21NT to 10.201.4.120 on 9/26/2003 8:22:00 PM

Websense Enterprise: Access to this protocol (Yahoo! Messenger) or site is restricted at this time.

Default protocol block message on Windows

The user might also be presented with an error message from the requested application, indicating that the application cannot run. Application error messages are not generated by Websense software.

✓ **Note**

If you configure a protocol to be blocked beginning at a certain time, sessions initiated before that time remain active. Once a user terminates the active session, Websense software blocks any requests for the protocol.

Displaying protocol block messages in Windows

To display protocol block messages on client machines running Windows NT, XP or 200x, the Windows Messenger service must be enabled (it is active by default). Check the Windows Services dialog box on the client machine to see if the Messenger service is running.

✓ **Note**

The Windows Messenger Service is disabled by default. Enable this service in order for protocol block messages to display properly.

To display protocol block messages on a Windows 98 machine, you must start `winpopup.exe`, found in the `Windows` directory of your local drive. Start this application from a command prompt, or configure it to start by copying it into the `Startup` folder. For instructions, see the documentation for your operating system.

✓ **Note**

Protocol block messages are not displayed on client machines running Linux or Solaris. This does not affect filtering. Block *pages* display regardless of operating system.

Websense software filters protocol requests whether or not protocol block messages are configured to display on user workstations.

Protocol filtering

To configure filtering for protocols, edit a protocol set (see *Editing a protocol set*, page 290). Filtering settings are applied to individual protocols, and then enforced when a protocol set is applied to a policy.

For information on filtering protocols based on bandwidth usage, see *Managing bandwidth*, page 295.

✓ **Note**

By default, new protocol definitions are permitted, and are not logged.

To manage a particular protocol the same way for all users, define a protocol to be always permitted or always blocked for all users. (The protocol must have the same filtering setting in all active protocol sets at any one time.) Websense software caches protocols defined this way, and processes requests for these protocols immediately, without re-evaluating the request.

✓ **Note**

By default, Websense software cannot filter traffic tunneled over a SOCKS/WinSOCK proxy server. For instructions on enabling Websense filtering in a SOCKS/WinSOCK environment, see the installation guide.

Instant Messaging Attachment Manager

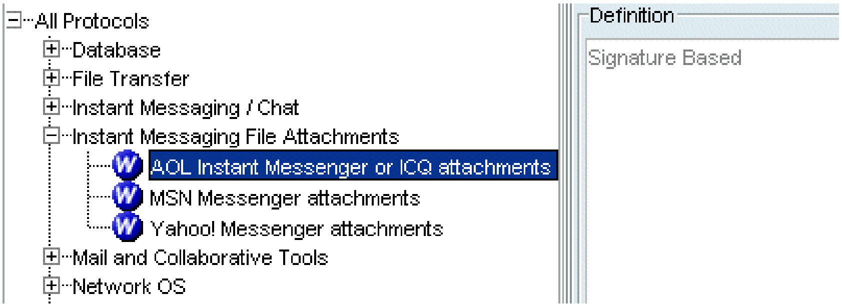
The Instant Messaging (IM) Attachment Manager is an optional feature available for purchase. If you have purchased this feature and have the appropriate subscription key, you can restrict file attachment sending and file sharing with IM clients such as AOL/ICQ, Microsoft (MSN) and Yahoo. This lets you permit IM traffic while blocking the transfer of attachments by those IM clients.

Instant Messaging File Attachments comprises a separate group of network protocols for IM file attachments. This group includes entries for IM clients such as MSN, AOL/ICQ, and Yahoo.

Note

IM attachment filtering can be applied to internal traffic as well. To enable this, define the portion of your network to monitor (see *Global Settings*, page 86).

When the IM Attachment Manager is activated, the Instant Messaging File Attachments protocols are displayed with the protocol list.


All Protocols
Database
File Transfer
Instant Messaging / Chat
Instant Messaging File Attachments
AOL Instant Messenger or ICQ attachments
MSN Messenger attachments
Yahoo! Messenger attachments
Mail and Collaborative Tools
Network OS
Definition
Signature Based

Instant Messaging File Attachments protocols

The Instant Messaging File Attachments group is included in all protocol sets. Modify the filtering setting for these protocols in any protocol set, or create a new protocol set that indicates a particular filtering setting for this group. For more information, see *Protocol filtering*, page 281.

Protocols and user identification

Websense software filters protocol requests based on the source IP address associated with the request, rather than on individual user account information. Websense software maintains a user map in local memory, containing user-name-to-IP-address pairings. For each internet request, Websense software compares the source IP address of an internet request with data in its user map.

If transparent identification is enabled, and no match is found between the source IP address and a user name, Websense software attempts to transparently identify the user making the request. With transparent identification, the user is *not* prompted by a web browser to log on. Transparent identification is the best option for accurate filtering and logging of protocol requests. For more information, see page 130.

If the user cannot be identified, or your network configuration does not support transparent identification, Websense software resolves the user name based on information in the user map. Otherwise, the request is filtered according to the workstation or network policy (if assigned), or by the **Global** policy.

If Websense manual authentication (see page 180) is enabled, Websense software prompts users to log on to the web browser. If Websense software cannot identify the user making a protocol request, it filters based on policies assigned to the workstation or network (if any), and then defaults to the **Global** policy. This is also true whenever the manual authentication timeout period is reached. The default interval successfully limits the frequency of manual authentication timeouts.

Permanent protocol sets

While category sets provide the basis for internet site filtering, protocol sets are the basis for filtering internet content by protocol.

These protocol sets are predefined in Websense Manager:

- **Default Settings**: The default protocol set used when no other protocol set is assigned to a time period in a policy. **Default Settings** is the protocol set assigned to the **Global** policy if your site selected **Filter Internet traffic based on a predefined policy** during installtion. It can be edited to meet the needs of your organization.
- **Never Block**: When active, allows total, unrestricted access to all protocols. The **Never Block** protocol set cannot be modified.

Websense software also installs protocols sets designed to act as templates that can be modified or deleted.

- **Basic Filtering**: Blocks commonly-restricted protocols.
- **Monitor Only**: Permits all protocols, and allows logging and reporting on all protocols.

Customizing protocols and protocol sets

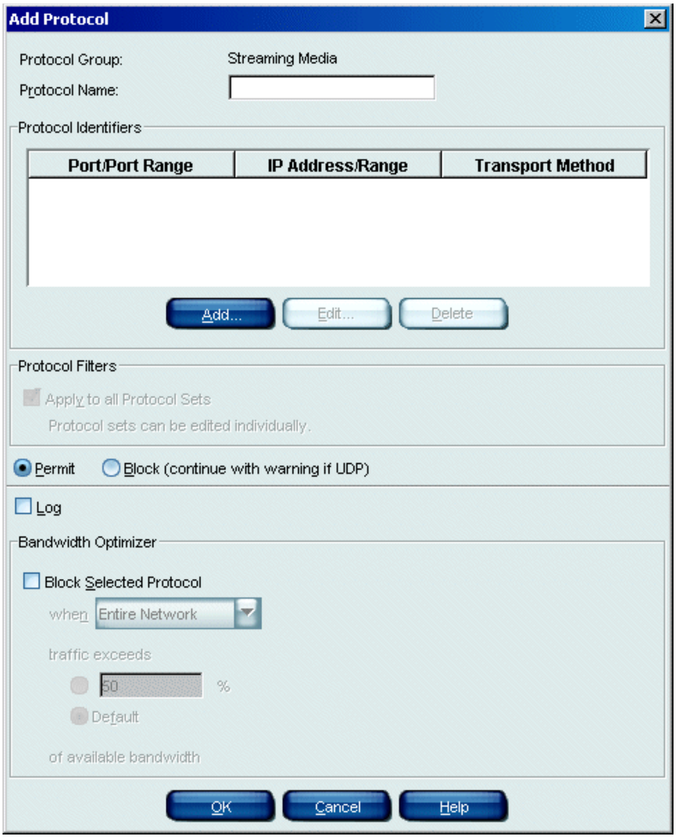
In addition to the protocol sets Websense, Inc., provides, define as many protocol sets as needed. You can also create your own protocols to be applied to filtering policies, or remove custom protocols that are no longer needed in policies. This section shows how to:

- Create a custom protocol (see page 285).
- Edit a custom protocol (see page 288).
- Add to a Websense protocol definition (see page 289).

Creating a custom protocol

New protocols must be defined by port number or IP address.

1. Expand **Filter Definitions** > **Protocols** in the navigation tree. The existing protocol groups are displayed.
2. Select the protocol group to which to add the new protocol.
3. Click **Add Protocol**. The Add Protocol dialog box appears.



Add Protocol

Protocol Group: Streaming Media

Protocol Name:

Protocol Identifiers

Port/Port Range	IP Address/Range	Transport Method

Add... Edit... Delete

Protocol Filters

☑ Apply to all Protocol Sets

Protocol sets can be edited individually.

● Permit ○ Block (continue with warning if UDP)

□ Log

Bandwidth Optimizer

□ Block Selected Protocol

when Entire Network

traffic exceeds

○ 50 %

● Default

of available bandwidth

OK Cancel Help

4. For **Protocol Name**, enter a name for the protocol.

Note

If you create a custom protocol that uses the same port numbers as a Websense protocol, the custom protocol definition takes precedence in filtering and logging.

5. Under **Protocol Identifiers**, click **Add**.
6. Enter the ports or IP addresses this protocol should use in your network, and select a **Transport Method** to associate with this protocol.

   Follow these guidelines for creating protocol identifiers:

   - At least 1 criterion (port, IP address or transport type) must be unique and non-overlapping for each protocol identifier. This is true for multiple protocol identifiers within a single custom protocol, *and* for identifiers across custom protocols.
   - If you select **All Ports** or **All external IP addresses**, that criterion overlaps with any other ports or IP addresses entered in a second protocol definition.
   - Port ranges or IP address ranges are *not* considered unique if they overlap. For example, the port range 80-6000 overlaps with the range 4000-9000.

   These examples show some valid and invalid protocol identifier combinations:

Port	IP Address	Transport Method	Accepted combination?
70	ANY	TCP	Yes - the port number makes each protocol identifier unique.
90	ANY	TCP	

Port	IP Address	Transport Method	Accepted combination?
70	ANY	TCP	No - the IP addresses are not unique. 10.2.1.201 is included in the “ANY” set.
70	10.2.1.201	TCP	

Port	IP Address	Transport Method	Accepted combination?
70	10.2.3.212	TCP	Yes - the IP addresses are unique.
70	10.2.1.201	TCP	

✓ **Note**

Use caution when defining a protocol on port 80 or 8080. Network Agent listens for internet requests over these ports.

Since custom protocols take precedence over Websense protocols, if you define a custom protocol using port 80, all other protocols that use port 80 are filtered and logged like the custom protocol.

7. Under **Protocol Filters**, select whether this protocol should be permitted or blocked, and whether requests for this protocol should be logged.

   When you add a custom protocol, this setting is applied in all protocol sets.

8. If you have purchased Bandwidth Optimizer, you can block this protocol based on bandwidth usage. For more information, see *Managing bandwidth*, page 295.
9. Click **OK**.
10. Configure a policy to filter protocols (see *Configuring protocol-based filtering*, page 293).

Editing a custom protocol

1. Expand **Filter Definitions** > **Protocols** in the navigation tree. Existing protocol groups are displayed in the content pane.
2. Select the protocol to edit.
3. Click **Edit Protocol**. The Edit Protocol dialog box appears.
4. To change a protocol identifier, select the row, and then click **Edit**. Modify criteria, following the guidelines under *Creating a custom protocol*, page 285. Click **OK**.
5. To change the filtering setting for this protocol, check **Apply to all protocol sets**.
   a. Select **Permit** or **Block**.

   > **Note**
   >
   > This filtering setting overrides the filtering settings in individual protocol sets.

   b. *Bandwidth Optimizer customers:* To apply bandwidth limitations for this protocol, check **Block Selected Protocol**, and then select bandwidth limits.
6. Click **OK**.

> **Note**
>
> You can remove custom protocols that are no longer needed. However, you cannot remove Websense protocols.

Adding to a Websense protocol definition

You cannot add a port number or IP address directly to a Websense protocol definition. However, you can create a custom protocol with the same name, and then add ports to its definition. The named protocol uses all port numbers assigned to either instance of its definition.

When a custom protocol and a Websense protocol have the same name, Websense software looks for protocol traffic at the ports or IP addresses specified in both protocol definitions. Assume the Websense protocol uses port 23, and the custom protocol uses port 24. If traffic is found over port 24, the request is logged with the custom protocol name.

To modify the port numbers designated to a protocol:

1. Expand **Filter Definitions** > **Protocols** in the navigation tree. The existing protocol groups are displayed.
2. Under **Protocols** in the content pane, expand the appropriate protocol group.
3. Create a new protocol with the same name as the existing one (see *Creating a custom protocol*, page 285).

   Add or change port numbers.

   Note

   In reports, custom protocol names are preceded by "C_." For example, if you created a custom protocol for SQL_NET and specified additional port numbers, reports display **C_SQL_NET** for instances where the protocol used the additional port numbers.

4. Click **Save Changes** above the navigation tree.

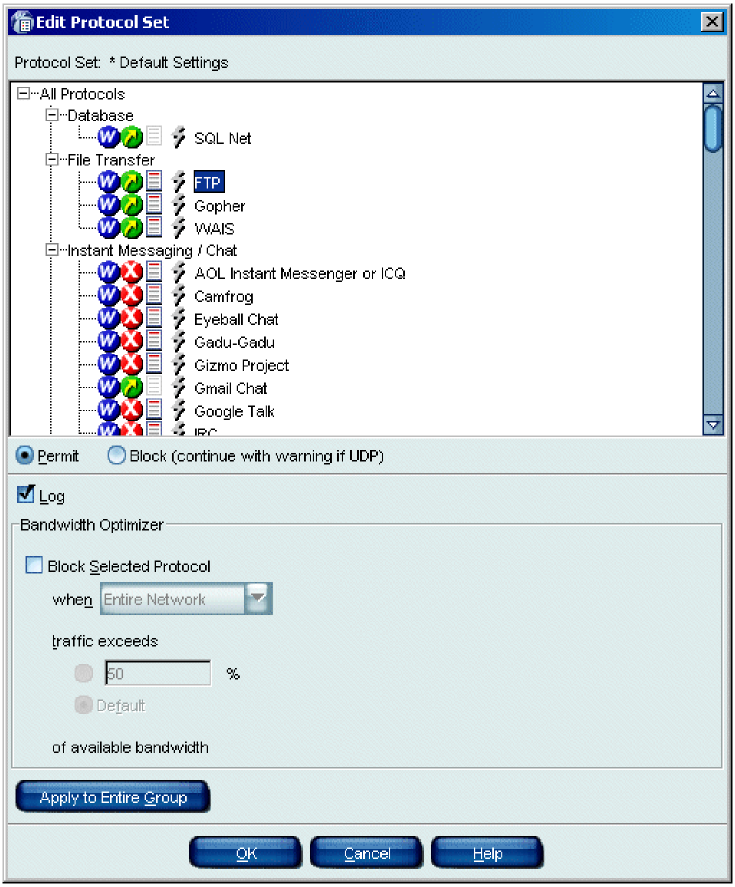
Adding a protocol set

1. Right-click in the navigation tree, and then select **Add Protocol Set**. The Add Protocol Set dialog box appears.
2. Enter a name for the new protocol set, and then click **OK**. The Protocol Set Model dialog box appears.
3. Select an existing protocol set on which to base the new set, and then click **OK**.
4. The protocol set you just created appears in the navigation tree, under **Filter Definitions** > **Protocol Sets**. It remains a replica of the protocol set it is modeled after until it is edited, and is not used in filtering until it is added to a policy.

Editing a protocol set

1. Expand **Filter Definitions** > **Protocol Sets** in the navigation tree.
2. Select the protocol set to be edited. Its settings are displayed in the content pane.

3. Click **Edit** (in the upper left-hand corner of the content pane). The Edit Protocol Set dialog box appears.



Edit Protocol Set

Protocol Set: * Default Settings

- All Protocols
  - Database
    - SQL Net
  - File Transfer
    - FTP
    - Gopher
    - WAIS
  - Instant Messaging / Chat
    - AOL Instant Messenger or ICQ
    - Camfrog
    - Eyeball Chat
    - Gadu-Gadu
    - Gizmo Project
    - Gmail Chat
    - Google Talk
    - IRC

● Permit ○ Block (continue with warning if UDP)

☑ Log

Bandwidth Optimizer

□ Block Selected Protocol

when Entire Network

traffic exceeds

○ 50 %

● Default

of available bandwidth

4. Customize the filtering settings for a protocol by selecting the protocol and specifying filtering options.

Filtering Setting	Function
Permit	Permits data transmitted by the selected protocol.
Block	Blocks data transmitted by selected protocol.

Filtering Setting	Function
Log	Tells Websense software whether to show usage data for this protocol in report output. Reports include the number of attempted requests for the protocol, and bandwidth usage for that protocol.
Block Selected Protocol when [Entire Network/ HTTP] traffic exceeds [N%/ Default] of available bandwidth	Applies bandwidth filtering options to the selected protocol. Default maximum bandwidth values are specified via **Server** > **Settings** > **Bandwidth Optimizer**. This option is available only if you have purchased the Websense Enterprise Bandwidth Optimizer feature (see *Managing bandwidth*, page 295).

By default, any new protocols created or downloaded after Websense software was installed have the **Permit** option checked, and the **Log** option *un*checked.

✓ **Note**

If you set the **Block** and **Log** options for the Websense protocol **Gnutella**, you may see a very large number of log records for this protocol. To prevent excessive logging, disable the **Log** option for **Gnutella** (see page 290).

5. To apply the selected filtering options to the whole protocol group, click **Apply to Entire Group**.
6. Click **OK**.
7. Click **Save Changes** above the navigation tree.

If the protocol set is already included in a policy, the new filtering settings are enforced for associated protocols. If the protocol set is not part of any policy, it must be added to a policy before Filtering Service can enforce it.

You can also modify protocol filtering options when editing a policy, as described in the next section, *Configuring protocol-based filtering*. Changes made to a protocol set apply wherever that protocol set is used in a policy.

Configuring protocol-based filtering

Protocols are filtered according to policy settings. The Websense Network Agent enables protocol management, and must be installed to activate this capability.

✓ **Note**

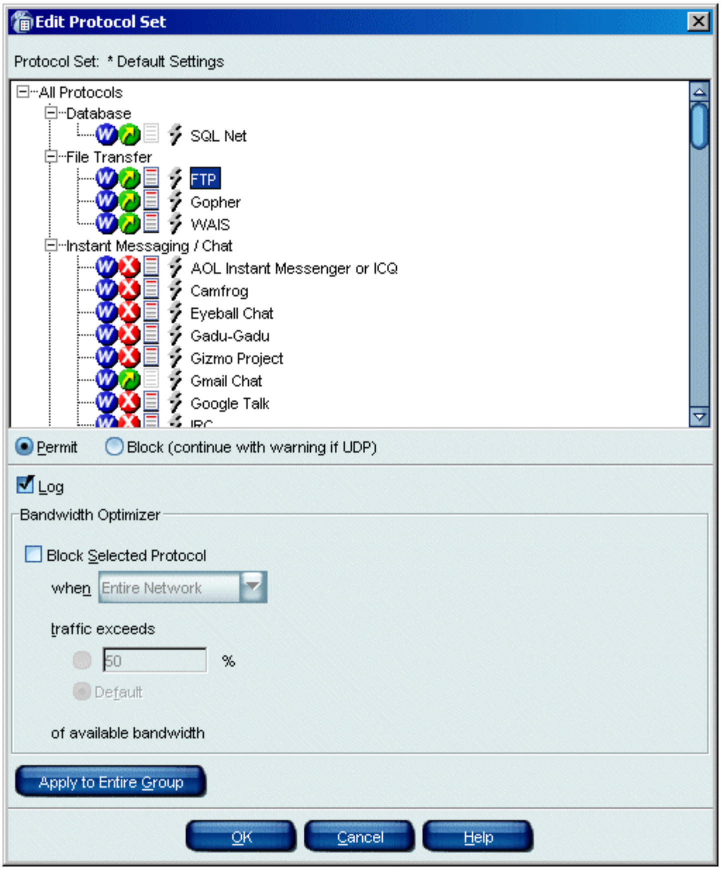
To implement full filtering for video *and* audio internet media, a good solution is to implement protocol-based filtering in conjunction with file type filtering (see *About file types*, page 246). In this case, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

Before implementing protocol management or bandwidth-based filtering, verify that the default server settings for Network Agent fit your network configuration (see *Initial configuration*, page 83).

To configure a policy to filter requests based on protocols or applications:

1. In the navigation tree, expand **Filter Definitions** > **Policies**.
2. Select the policy with which to manage protocols. The policy details are displayed in the content pane.
3. In the policy section of the content pane, click **Edit**.
4. For each time period in the policy, select a protocol set to manage during that time period.
5. Double-click in the **Protocol Set** column, and then select the protocol set to edit.

6. Click **Edit**. The Edit Protocol Set dialog box appears.



Protocol Set: * Default Settings

● Permit ○ Block (continue with warning if UDP)

☑ Log

□ Block Selected Protocol

when Entire Network

○ 50 %

● Default

7. Select the protocol for which to configure filtering settings.

8. Select the filtering settings to apply to the selected protocol or protocols (see *Protocol filtering*, page 281).

Note

You can also modify protocol filtering settings by editing a protocol set, as described under *Editing a protocol set*, page 290. Changes made to a protocol set apply wherever that protocol set is used in a policy.

9. To apply the selected filtering settings to all protocols within this group, click **Apply to Entire Group**.

10. Click **OK**, and then click **OK** again to return to the Websense Manager window.
11. Click **Save Changes** above the navigation tree.

Managing bandwidth

Websense Enterprise® Bandwidth Optimizer, purchased optionally, provides threshold filtering that restricts internet content based on available bandwidth.

You can manage bandwidth associated with particular protocols or URL categories.

Bandwidth and protocols

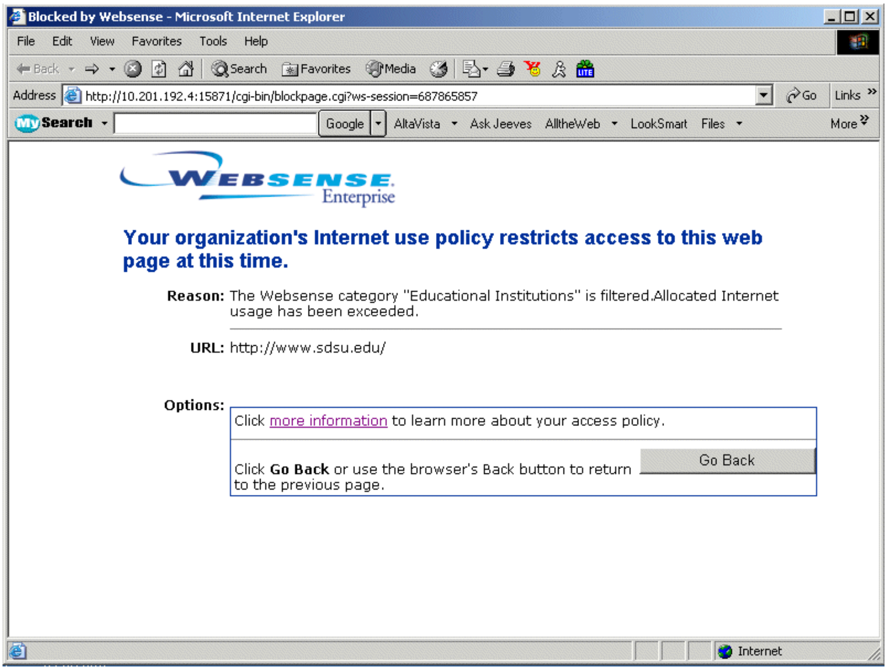
Block content provided by a particular protocol based on total network bandwidth usage, or on bandwidth usage associated with a particular protocol. This includes bandwidth used by IM Attachments and Peer-to-Peer protocol traffic.

For example, block AOL instant messaging if total network bandwidth usage exceeds 50% of available network bandwidth, or if current bandwidth usage for AOL exceeds 10% of the total network bandwidth. To set bandwidth limitations for protocols, see *Editing a category set*, page 257.

Bandwidth usage per protocol is usage over all the ports, IP addresses or signatures defined for that protocol. A port-based protocol uses all ports specified in its definition. Some protocols or internet applications use a single port, while others *hop* ports, or use more than 1 port for data transfer. Some peer-to-peer applications can select from multiple ports to transfer data.

Websense software monitors and blocks protocols that use multiple ports via multiple port entries in its protocol definitions. However, if an internet application uses a port outside its definition, network traffic over that port is not included in bandwidth usage measurements. Websense, Inc., updates Websense protocol definitions regularly to ensure bandwidth measurement accuracy.

When a request is blocked based on bandwidth limitations, the Websense block page displays this information in the **Reason** field.


Blocked by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Search Google AltaVista Ask Jeeves AlltheWeb LookSmart Files More
WEBSENSE Enterprise
Internet

http://10.201.192.4:15871/cgi-bin/blockpage.cgi?ws-session=687865857

Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Educational Institutions" is filtered.Allocated Internet usage has been exceeded.

URL: http://www.sdsu.edu/

Options: Click more information to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page. Go Back

The default limits for available network bandwidth are the basis for bandwidth-based filtering settings. For more information, see *Bandwidth limits*, page 298.

Network Agent sends network bandwidth data to Filtering Service at a predetermined interval. This default interval ensures that Websense software accurately monitors bandwidth usage, and receives measurements that are closest to an average.

Bandwidth and categories

You can filter based on bandwidth usage associated with the URL categories governed by a filtering policy. For example, a policy could block sites if total network bandwidth usage exceeds 50% of available network bandwidth.

Alternatively, apply bandwidth limitations to a URL category based on overall network HTTP bandwidth usage. For example, block the category **Sports** when bandwidth usage by *all* HTTP traffic reaches 60% of available network bandwidth. When overall HTTP usage is at or above 60%, sites in the **Sports** category are blocked. When overall HTTP usage is below 60%, sites in the **Sports** category are filtered according to filtering options specified in policies.

For more information about filtering HTTP internet requests based on bandwidth usage, See *Editing a category set*, page 257.

✓ **Note**

When bandwidth-based filtering options are active, Websense software begins bandwidth-based filtering 10 minutes after initial configuration, and 10 minutes after each Websense Policy Server restart. This delay ensures accurate measurement of bandwidth data and use of this data in filtering.

Bandwidth limits

Before specifying bandwidth settings in policies, verify the default bandwidth limits that serve as the basis for filtering settings. The default maximum values are:

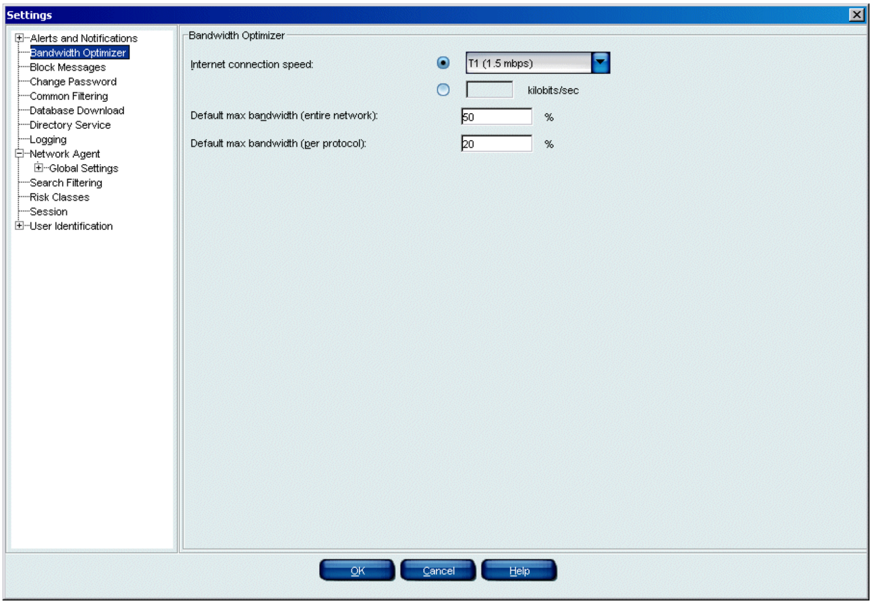
- **Default max bandwidth (entire network)**: 50%
- **Default max bandwidth (per protocol)**: 20%

Note

Bandwidth settings are only displayed if Bandwidth Optimizer has been purchased.

To change the default maximum values for bandwidth:

1. Select **Server** > **Settings**.
2. Select **Bandwidth Optimizer** at the left.



Bandwidth Optimizer

Internet connection speed: ● T1 (1.5 mbps)

○ kilobits/sec

Default max bandwidth (entire network): 50 %

Default max bandwidth (per protocol): 20 %

Default values for Bandwidth Optimizer

3. Edit the bandwidth percentage values as desired.
4. Click **OK**.

The new values are applied whenever filtering based on bandwidth usage is active.

Note

Default bandwidth values apply to all instances of Network Agent, whether or not they reside on the same machine as Websense Manager. These values are stored in Policy Server, which communicates with all instances of Websense Manager.

If you have multiple Policy Servers, each Policy Server affects only its own network segment. For more information, see page 42.

To manage bandwidth usage associated with a particular protocol, edit the protocol set associated with the appropriate policy. The bandwidth settings for each protocol comprise a part of the policy's overall filtering definition.

You can also apply bandwidth limitations to a particular category set (see *Editing a category set*, page 257). When you filter URL categories based on HTTP bandwidth usage, Websense software measures total HTTP bandwidth usage over all ports specified as HTTP ports for Websense software (see *Network Interface Card (NIC) settings*, page 91).

Working with policies

Use category sets and protocol sets as building blocks to refine your filtering policies.

The Global policy

The **Global** policy provides an immediate way to manage internet access throughout your organization. Use the **Global** policy as is, or modify it. Because the **Global** policy is the default policy, it cannot be deleted.

If your site selected **Filter Internet traffic based on a predefined policy** during the installation of Websense software, then the **Global** policy restricts requests according to the **Default Settings** category set and the **Default Settings** protocol set, 24 hours a day, 7 days a week.

If your site selected **Monitor Internet Traffic only** during installation, then the **Global** policy logs and monitors all requests but does not block any.

Initially, the **Default Settings** category set and protocol set permit most categories and protocols, but block those considered inappropriate by the business and education communities. You can edit the Default Settings category set and protocol set to cause the **Global** policy to filter according to your preferences. For more information, see *Category Sets/Yes Lists*, page 245 and *Customizing protocols and protocol sets*, page 284.

Edit the **Global** policy to enforce different category sets or protocol sets according to a schedule you establish. Websense software then filters users according to the new schedule. For more information, see *Editing a policy*, page 302.

Sample policies

Websense software comes with additional policies that are designed as models and can be used as is, edited, or deleted. To view a sample policy, expand **Policies** in the navigation tree and select the policy. Policy details are displayed in the content pane.

Custom policies

Custom policies let you apply more or less restrictive filtering for specific users or computers (clients) without affecting filtering for the entire organization.

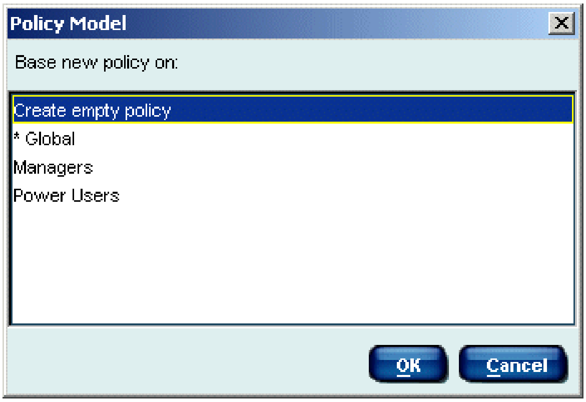
To enforce a custom policy:

1. Add a new policy via Websense Manager.
2. Edit the policy to define its filtering restrictions (see page 302).
3. Add a client via Websense Manager (see page 114).
4. Assign the new policy to the client (see page 304).

Adding a policy

The first step in creating a custom policy is adding a new policy.

1. Right-click in the navigation tree, and then select **Add Policy**. The Add Policy dialog box appears.
2. Enter a name (1-25 characters) for the new policy in the Add Policy dialog box.
3. Click **OK**. The Policy Model dialog box appears.



4. Select an existing policy on which to base your new policy, or select **Create empty policy**.
5. Click **OK**.

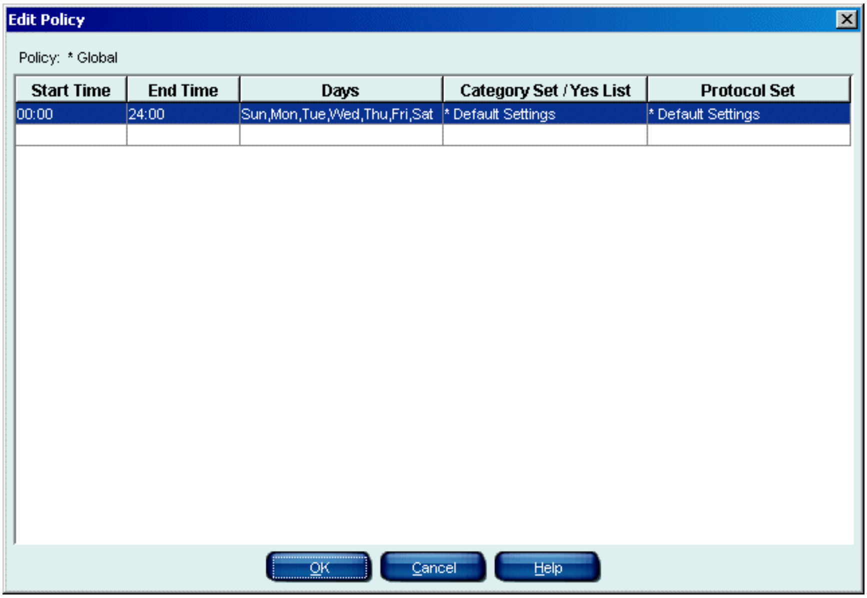
Edit your newly-created policy to specify filtering restrictions.

Editing a policy

A policy consists of specified time periods during which particular URL category and protocol filtering settings are active.

Edit a policy to add, change, or delete time periods, and to change the active category set for each time period.

1. Expand **Filter Definitions** > **Policies** in the navigation tree.
2. Select a policy to display the start and end times, days, category set and protocol set that make up the policy.
3. In the policy section of the content pane, click **Edit**. The Edit Policy dialog box appears.



Policy: * Global

Start Time	End Time	Days	Category Set / Yes List	Protocol Set
00:00	24:00	Sun,Mon,Tue,Wed,Thu,Fri,Sat	* Default Settings	* Default Settings

4. Double-click under **Start Time** and **End Time** to define a time period during which to enforce these restrictions.

   Do not define a time period that spans midnight. To use the same category set from 5:00 pm to 8:00 am, define 2 time periods for it: one with start time 17:00 (5:00 pm) and end time 24:00 (midnight) and another with start time 00:00 (midnight) and end time 08:00 (8:00 am).
5. Double-click in the **Days** column, and select each day of the week to enforce these restrictions. Click **Done**.

6. Double-click in the **Category Set/Yes List** column and select the category set or yes list to enforce during the days and times in the current row (*Category Sets/Yes Lists*, page 245).
7. Double-click in the **Protocol Set** column and select the protocol set to enforce during the days and times in the current row. For more information, see *Managing protocols*, page 274.
8. Repeat Step 4 through Step 7 to edit other rows, add new rows to the policy, or delete rows. Each time period is defined on a separate row.

   Add or delete a row by right-clicking on a row to access the shortcut menu, and then choosing **Add Row** or **Delete Row**.
9. Click outside the table to exit the table area.
10. Click **OK**.
11. Click **Save Changes** above the navigation tree.
12. Assign this policy to clients so Websense software can use it to filter internet requests (see *Assigning policies to clients*, page 304).

Assigning policies to clients

The **Global** policy is assigned to all users by default. To assign a different policy to a user, group, workstation, or network, first add the client to Websense Manager (see *Adding directory objects*, page 114).

Assign a policy to 1 client, or assign the same policy to multiple clients at once. To view which clients a policy is assigned to, see *Viewing assigned policies*, page 305.

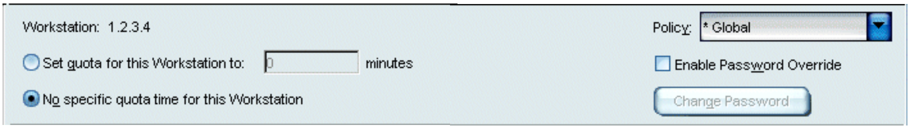
Note

Filtering Service applies 1 policy per site request. If more than 1 policy applies (for example a machine and its user are each assigned a policy), Filtering Service evaluates those policies in a specific order. For more information, see *Filtering order*, page 35.

Assigning a policy to a single client

Assign a policy to a single user, group, workstation or network, or change the policy assigned to a single client.

1. Select the appropriate user, group, workstation, or network in the navigation tree. Current policy details appear in the content pane.



Workstation: 1.2.3.4

○ Set quota for this Workstation to: 0 minutes

● No specific quota time for this Workstation

Policy: * Global

□ Enable Password Override

2. Select the desired policy from the **Policy** drop-down list.

Note

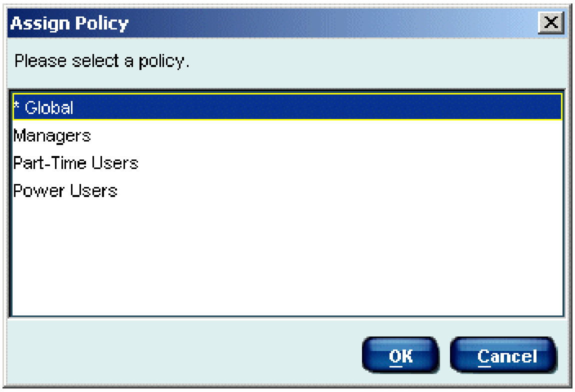
Alternatively, right-click the client name in the navigation tree, and then select **Assign Policy**.

3. Click **Save Changes** above the navigation tree.

Assigning a policy to multiple clients

To assign a single policy to multiple users, groups, workstations, or networks at the same time:

1. To select multiple users, press the **Ctrl** key while clicking each group name. To select a range of users, press the **Shift** key while clicking the first and last users in the range.
2. Right-click one of the selected clients, and then select **Assign Policy**. The Assign Policy dialog box appears.
3. Select the policy to assign, and then click **OK**.



4. Click **Save Changes** above the navigation tree.

Viewing assigned policies

To view a list of all clients assigned a particular policy:

1. Right-click the policy name in the navigation tree.
2. Select **View Assigned Clients**. The Assigned Clients dialog box lists the clients assigned that policy.
3. Click **OK**.

Distributing policies to multiple servers

If you have multiple Policy Servers, it may be convenient to configure server settings and filtering policies in one location, and then replicate the configuration to other Policy Servers. The Websense central policy distribution feature lets you distribute configuration data this way.

✓ **Note**

If only 1 Policy Server is added to Websense Manager, central policy distribution commands are temporarily disabled in all locations.

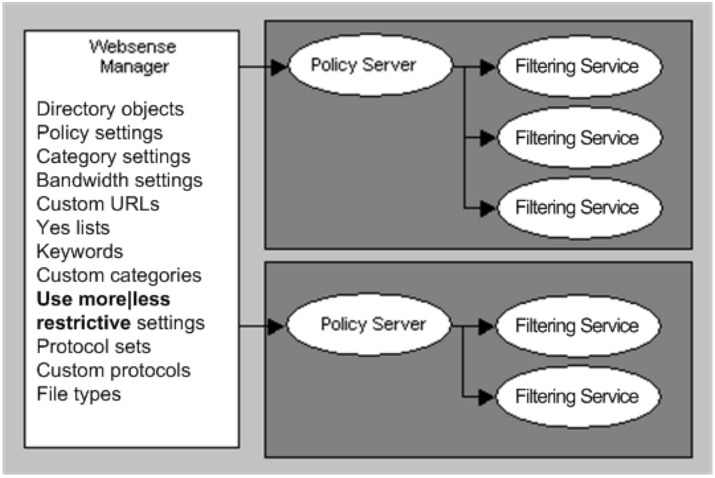
If you are running Websense Enterprise Corporate Edition, your options for distributing central data are more flexible. For more information, see *Central Configuration Distribution*, page 235.

Central policy distribution offers several advantages in managing multiple locations. This feature lets you:

- Implement filtering settings across locations in your organization.
- Manage and configure filtering policies in 1 office or location, and then share these policies with remote offices.
- Have local administrators maintain policies to be used at their locations via a remote connection to your main server.

The more information various locations share, the more convenient central policy distribution can be. If various locations do *not* share a directory service, see *Directory services and policy distribution*, page 309.

Policy settings from the central Policy Server are distributed to other Policy Servers, and consequently to all Filtering Services in your network.



Multiple Policy Servers

Multiple Filtering Services can share a single Policy Server. In this case, all Filtering Services share all policy and configuration settings by default. This scenario is established during installation.

Note

Each Filtering Service must be configured to communicate with a Policy Server. For installation instructions, see the installation guide.

Once you distribute policies, a distribution profile is stored locally in Websense Manager. The next time you distribute settings, you can use the same distribution profile or specify changes.

When you distribute from the central Policy Server to additional Policy Servers, the following policy configuration data is pushed to the other servers:

- Directory objects (users, groups, workstations, networks) defined in Websense Manager
- Policies and policy settings
- Category sets and their settings
- Bandwidth-based filtering settings (for category sets or protocol sets)
- Custom URLs
- Yes lists
- Keywords
- Custom categories
- **Use more|less restrictive blocking** settings
- Protocol sets
- Custom protocols
- Custom file types
- Global filtering settings (Settings dialog box/**Common Filtering**)

This data is *not* distributed between Policy Servers:

- Directory service settings
- Websense passwords saved in Policy Server
- Master Database settings and download times
- Subscription keys
- Network Agent configuration
- DC Agent and user identification settings
- Alerting settings
- Log Server settings
- Default bandwidth values
- Real-Time Analyzer settings
- Block message URLs (these can point to relative server locations, and should not move)
- Websense categories, file types and protocols from the Master Database

Directory services and policy distribution

Use the central policy distribution feature when:

a. Your network does not include a directory service, so you do not have filtering policies assigned to particular directory objects.

b. Your network includes a directory service that is shared between all locations. You might have filtering policies assigned to particular directory objects.

c. Your network includes a directory service, but various locations do *not* share directory service information. You might have filtering policies assigned to particular directory objects.

If scenario *c* applies, ensure that any directory objects associated with distributed policies exist at all destination locations. For more information, see *Distributing Policies*, page 310.

When you distribute policy data and Websense directory objects to multiple locations, any existing, local policies and objects are overwritten.

Single Log Server environment

Websense, Inc., does not support unique configuration of multiple Policy Servers with only 1 Log Server unless you are running Corporate Edition. If you need to maintain unique filtering settings on separate Policy Servers, Websense, Inc., recommends installing a separate Log Server for each Policy Server. This way, any custom settings (such as custom categories or custom URLs) are accurately reflected in report output for each server.

If you do not need to maintain unique settings for separate Policy Servers, use central policy distribution to ensure that a single Log Server receives accurate internet usage data for reporting.

Distributing Policies

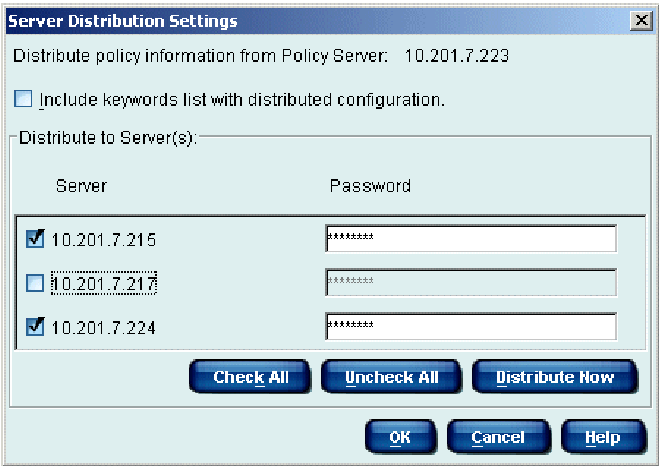
Configure settings to use in central policy distribution by all Policy Servers connected to Websense Manager, then specify distribution settings and distribute policies.

✓ **Note**

To avoid losing distributed data, ensure that Websense Manager is closed at all remote locations before you distribute data

1. If your organization uses separate directory services at different locations, do the following. (If all locations share the same directory service information, skip this step.)
   a. *Before* distributing policy data from the source location, ensure that directory objects associated with policies exist in the destination directory services. If necessary, have local administrators create directory objects and name them to match the directory objects at the source location.
   b. *After* distributing a policy for the first time, assign the policy to the local directory objects it should govern (see *Assigning policies to clients*, page 304). The policy does not take effect locally until you create the appropriate objects in the local directory service, and then assign the policy to those objects.

2. Select **Server** > **Distribution Settings**. The Server Distribution Settings dialog box appears.



Server Distribution Settings

Distribute policy information from Policy Server: 10.201.7.223

□ Include keywords list with distributed configuration.

Distribute to Server(s):

Server	Password
☑ 10.201.7.215	********
□ 10.201.7.217	********
☑ 10.201.7.224	********

3. Check the IP addresses of the destination Policy Servers.
4. For each Policy Server selected, enter the password.

Note

You must enter a valid password for each destination Policy Server. Distribution may fail for any server that does not have a valid password.

5. To distribute data, click **Distribute Now**, and then confirm distribution.

   Otherwise, click **OK** to exit the Server Distribution Settings dialog box, and then click **Save Changes** to save the selected distribution settings for future use.
6. Click **OK** to confirm distribution.

Printing policies to a file

Websense software lets you save your filtering policy configuration information to an external file. This retains a view-only copy of your policy configuration when you make changes. You can refer to the previous configuration later, and view all policy configuration details at a glance.

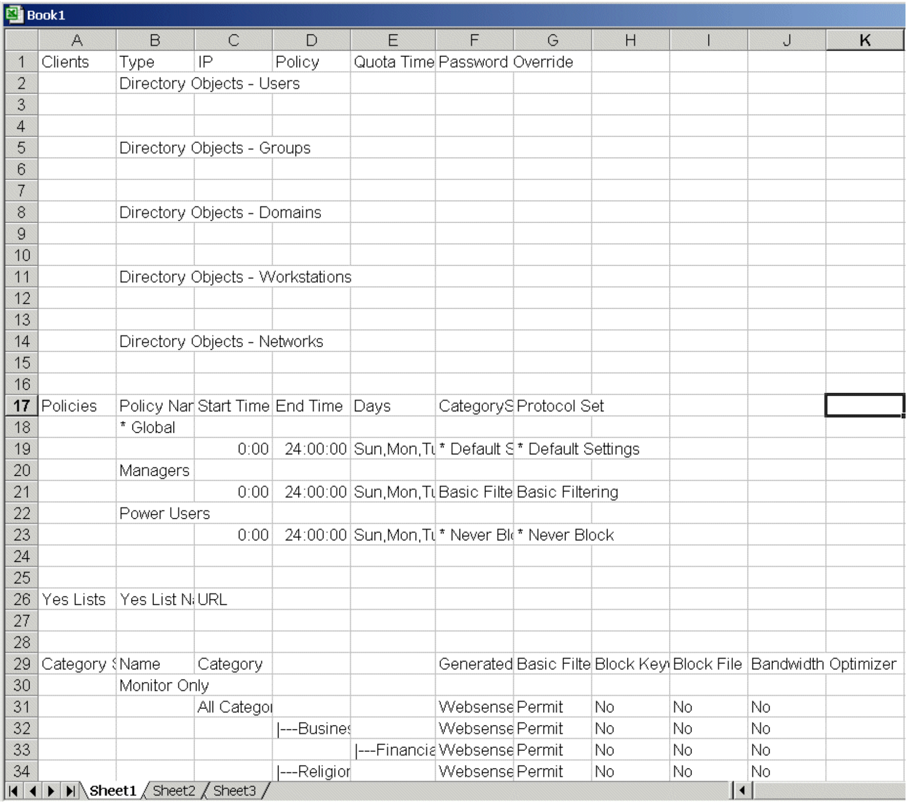
✓ **Note**

You cannot import exported policy configuration data back to Websense Manager. Policies must be configured manually, or using the central policy distribution feature.

Standard Websense users: See *Distributing policies to multiple servers*, page 306).

Corporate Edition users: See *Central Configuration Distribution*, page 235.

Configuration details are written to a text file. Paste the text output into another application, such as Microsoft Excel, for more sophisticated formatting.



Book1

	A	B	C	D	E	F	G	H	I	J	K
1	Clients	Type	IP	Policy	Quota Time	Password Override					
2		Directory Objects - Users									
3											
4											
5		Directory Objects - Groups									
6											
7											
8		Directory Objects - Domains									
9											
10											
11		Directory Objects - Workstations									
12											
13											
14		Directory Objects - Networks									
15											
16											
17	Policies	Policy Nar	Start Time	End Time	Days	CategoryS	Protocol Set				
18		* Global									
19			0:00	24:00:00	Sun,Mon,Tu	* Default S	* Default Settings				
20		Managers									
21			0:00	24:00:00	Sun,Mon,Tu	Basic Filte	Basic Filtering				
22		Power Users									
23			0:00	24:00:00	Sun,Mon,Tu	* Never Bl	* Never Block				
24											
25											
26	Yes Lists	Yes List N	URL								
27											
28											
29	Category S	Name	Category			Generated	Basic Filte	Block Key	Block File	Bandwidth Optimizer	
30		Monitor Only									
31			All Catego			Websense	Permit	No	No	No	
32				|---Busines		Websense	Permit	No	No	No	
33					|---Financia	Websense	Permit	No	No	No	
34				|---Religior		Websense	Permit	No	No	No	

Policy information exported to a file

1. Select **File** > **Print Policies to File**. The Save Policy to File dialog box appears.
2. Browse to the desired location, and specify an output filename.
3. Click **Save**.

CHAPTER 10 Troubleshooting

Following are previously-encountered problems and suggested solutions. Check this chapter before you contact Technical Support.

The Websense website features an extensive Knowledge Base. Search for topics by keyword or by reference number. Check the Top Ten FAQs for answers to commonly-asked questions. To access the Websense Knowledge Base, go to www.websense.com, and then navigate to Support & Knowledge Base.

Problems addressed in this chapter are:

Installation issues

I made a mistake during installation

Run the installation program again, choosing either **Modify** (Windows) or **Continue installation and overwrite current configuration settings** (Solaris or Linux).

I cannot enter my subscription key in Websense Manager

On Linux, if you attempt to enter your key in the Subscription Key field (via **Server > Settings > Database Download**), and the field does not accept characters, close the Settings dialog box, and then enter the key.

Database issues

The Master Database does not download

There are several possible reasons for difficulty receiving Master Database downloads.

Subscription Key

Verify that the subscription key is entered correctly and has not expired. Select **Server > Settings** > **Database Download**.

- Compare the key you received via email or in the Websense package to the key in the **Subscription key** field. The key must use the same capitalization as in your key document. Clicking **OK** in the Settings dialog box activates the key and enables database download.
- Check the date shown in the **Key expires** box. If this date has passed, contact Websense, Inc., to renew your subscription.

Internet access

The machine running Filtering Service must have access to HTTP, and must be able to receive incoming transmissions.

✓ **Note**

If you edit host files or routing tables in a firewall or internet router that restrict the URLs a Websense server can access, permit the following URLs to access database downloads and subscription data:

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
www.my.websense.com

First, determine whether Websense software is accessing the internet through a proxy server.

1. Select **Server** > **Settings** > **Database Download**.
2. On the Policy Server machine, open a web browser.
3. Set up the browser to access the internet with the same proxy settings as Policy Server.
4. Request the address:

   http://www.websense.com/global/en/downloads/

5. If you reach the site, the Websense logo appears, and you are redirected to the Websense home page. This means the Policy Servers proxy settings are correct, and Policy Server has HTTP access.

   If you cannot reach the download site, and the system requires proxy information, the proxy settings must be corrected.

   If no proxy information is required, use the `nslookup` command to ensure the Policy Server machine can resolve the download location to an IP address. For example:

   ```
   nslookup asia.download.websense.com
   ```

   If this does not return an IP address, set up the Websense machine to access a DNS server. Contact Websense Technical Support for assistance (see *Appendix A Technical Support*, page 337).

If Websense software must access the internet through an upstream firewall or proxy server that requires authentication, check that:

- The correct user name and password is entered under **Database Download** in the Settings dialog box. Verify spelling and capitalization.
- The firewall or proxy server is configured to accept clear text or basic authentication.

Firewall restrictions

If your firewall restricts internet access at the time Websense software normally downloads the database, or restricts the size of a file that can be transferred via HTTP, Websense software cannot download the database. Make appropriate changes on the firewall, or change the download times via **Server > Settings > Database Download**.

If you are running Websense software behind a Gauntlet firewall, check the Websense knowledge base for information about running Websense software behind a firewall. Go to www.websense.com, and then navigate to Support & Knowledge Base.

Restriction application

Some restriction applications, such as virus scanners or size-limiting applications, can interfere with database downloads. Disable the restrictions relating to the Policy Server machine and the Websense download location.

Master Database download does not occur at the time specified

The system date and time may not be set correctly on your machine. Websense software uses the system clock to determine the proper time for downloading the Master Database.

If the download is not occurring at all, see *The Master Database does not download*, page 316.

Filtering issues

Sites in the Information Technology category are being blocked

By default, Internet Explorer versions 4.0, 4.01, and 5.0 for Windows accept searches from the Address bar. If a user enters only a domain name in the Address bar (**websense** instead of **http://www.websense.com**, for example), Internet Explorer considers the entry a search request, not a site request. It displays the most likely site the user is looking for, along with a list of closely matching sites.

As a result, Websense software permits, blocks, or limits the request based on the status of the Information Technology/Search Engines and Portals category in the active policy—*not* on the category of the requested site. For Websense software to filter based on the category of the requested site, you must turn off searching from the Address bar:

1. From the **Tools** menu, select **Internet Options**.
2. Go to the **Advanced** tab.
3. In the **Search from the Address bar** area, select **Do not search from the Address bar**.
4. Click **OK**.

✓ **Note**

These steps apply to Internet Explorer versions 5 and 6.

Keywords are not being blocked

Possible reasons for this problem are:

- You may have **Disable keyword blocking** selected. To correct the problem:
    a. Select **Server** > **Settings.** The Settings dialog box appears.
    b. Select **Common Filtering** at the left.
    c. In the **Keyword search options** area, select an option other than **Disable keyword blocking**.

d. Click **OK.**

- If a site uses `post` to send data to your web server, Websense software does not recognize keyword filtering settings for that URL. If your integration product also does not recognize data sent via post, users can still access URLs containing blocked keywords.

  To check whether a website uses a `post` command, view the site's source from within your browser. If the source code contains a string like `<method=post>`, then `post` is used to load that site.

Sites in blocked categories are not always being blocked

If a site is in a category that is blocked by the active policy, but a user can still access the site, it may be because the site has a virtually hosting IP address. If a user enters the IP address instead of the URL, the site is accessible because the IP address registers as Miscellaneous/Uncategorized in the Websense Master Database.

To prevent access to blocked websites via virtually hosting IP addresses:

1. Select **Custom URLs/Recategorized** in the navigation tree.
2. Under **Choose a Category**, select **User-Defined**.
3. Under **Enter URLs for the highlighted category**, type:

   ```
   http://1
   http://2
   http://3
   http://4
   http://5
   http://6
   http://7
   http://8
   http://9
   ```

4. Click **Add URLs** at the bottom of the content pane.
5. Click **Save Changes** above the navigation tree.

If users enter IP addresses for sites in blocked categories, they cannot access those sites.

Custom or yes list URLs are not filtered as expected

If an HTTPS URL on a custom URL list is not filtered as expected, it may be because an integration product transforms the URL into a format that the Websense Filtering Service cannot recognize.

Non-proxy integration products translate URLs from domain format into IP format. For example, the URL https://<domain> is read as https://<IP address>:443. When this occurs, Filtering Service cannot match the URL received from the integration product with a custom URL or yes list, and does not filter the site appropriately.

To work around this problem, enter URLs using IP address format. This may involve adding multiple URLs for a single site, as there might be multiple IP addresses in a domain.

A user cannot access a protocol or application as expected

Dropped connections to messaging applications may be due to the user authentication configuration in your proxy server. If Microsoft Proxy Server or Microsoft ISA Server is in use in your network, check which authentication method is enabled.

If any method *other* than Anonymous Authentication is active, the proxy server attempts to identify data packets received when users request application connections. The proxy server fails to identify the data packet, and the connection is dropped. This potentially skews Websense protocol filtering activity.

An FTP protocol request is not blocked as expected

If Websense software is installed with Check Point® FireWall-1®, Websense software may not recognize and filter FTP internet requests as expected.

Check to see if *folder view* is enabled in the client's browser. When folder view is not enabled in the client's browser, FTP requests sent to the FireWall-1 proxy are sent to Websense software with an "http://" prefix. As a result, Websense software filters these requests as URL site requests, and not as protocol requests.

Websense is not filtering based on a directory object policy

If Websense software is filtering based on workstation or network policies, or on the **Global** policy, even after directory object policies were assigned, follow these suggestions. (Also see Websense Knowledge Base item 493.)

- If you did not add directory objects to Websense Manager, users are filtered by workstation or network policies (if created), or by the **Global** policy. For more information, see *Adding directory objects*, page 114.

- If your integration product is Microsoft ISA Server, check that the Web Proxy Service was restarted if the authentication method was changed.
- If you are using nested groups in Windows Active Directory, policies assigned to a parent group are applied to users belonging to a sub-group, and not directly to the parent group. For information on user and group hierarchies, see your directory service documentation.
- If you installed Websense DC Agent on a Windows system to enable Websense transparent identification:
    - A standard Windows 200x service can contact a domain controller periodically with a user name made up of the workstation name followed by a dollar sign (wkstn$). If this happens, the Websense DC Agent service must be run with the administrative account rather than with the local system account. To change accounts: Select **Start > Programs > Administrative Tools > Services** (*Windows 2000*). Right-click **Websense DC Agent**, and then select **Properties**. Change **local** to **administrator**.
    - DC Agent or User Service may have been installed as a service using the Guest account, equivalent to an anonymous user to the domain controller. If the domain controller has been set not to give the list of directory objects to an anonymous user, DC Agent is not allowed to download the list if it is running as a Guest.

      On the machine running the domain controller:

      a. Create a user account such as **Websense**. You can use an existing account, but a Websense account is preferable so the password can be set not to expire. No special privileges are required.

         Set the password never to expire. This account only provides a security context for accessing directory objects.

         Save the user name and password you establish for this account, as it must be entered in Step f.

      b. Open the Windows Services dialog box on each Websense DC Agent machine.
Windows NT/2003: Select **Start > Settings > Control Panel**, and then double-click **Services**.
Windows 2000: Select **Start** > **Programs** > **Administrative Tools** > **Services**.

      c. Select the **Websense DC Agent** entry, and then click **Stop**.

      d. Double-click the **Websense DC Agent** entry.

e. On the **Log On** tab, select the **This account** option.

f. Enter the user name of the Websense DC Agent account created in Step a. For example: **DomainName\websense**.

g. Enter and confirm the Windows password for this account.

h. Click **OK** to close the dialog box.

i. Select the **Websense DC Agent** entry in the Services dialog box, and then click **Start**.

j. Repeat this procedure for the Websense User Service.

- The User Service cache may be outdated. User Service caches user-name-to-IP-address mappings for 3 hours. To refresh the cache, click **Save Changes** in Websense Manager.

◆ If the user being filtered incorrectly is on a machine running Windows XP SP2, the problem could be due to the Windows Internet Connection Firewall (ICF), included and enabled by default in Windows XP SP2. For more information about the Windows ICF, see Microsoft Knowledge Base Article #320855.

For DC Agent or Logon Agent to get user logon information from a machine running Windows XP SP2:

1. From the Windows **Start** menu on the client machine, select **Settings** > **Control Panel** > **Security Center** > **Windows Firewall**.
2. Go to the **Exceptions** tab.
3. Check **File and Printer Sharing**.
4. Click **OK** to close the ICF window, and then close any other open windows.

◆ If you installed Websense DC Agent on a Linux machine, you must establish a user name and password with administrative privileges. This is typically done at installation time. If credentials were not entered during installation, complete these steps:

1. In Websense Manager, select **Settings** > **Directory Service**.
2. Select **Windows NT/Active Directory**. (Choose this selection even if you are not using Mixed Mode.)
3. Complete the requested fields on screen.

◆ If you deployed the Websense eDirectory Agent, a user may not be filtered properly if the user name is not being passed to eDirectory Agent.

This happens when a user does not log on to Novell eDirectory server, so eDirectory Agent cannot detect the logon. This can happen because:

- A user logs on to a domain that is not included in the default root context for eDirectory user logon sessions. This root context is specified during installation, and should match the root context specified for Novell eDirectory via **Server > Settings > Directory Service**.
- A user tries to bypass a logon prompt to circumvent Websense filtering.
- A user does not have an account set up in eDirectory server.

If a user does not log on to eDirectory server, user-specific policies cannot be applied to that user. Instead, the **Global** policy takes effect. If there are shared workstations in your network where users log on anonymously, set up a filtering policy for those particular workstations.

To determine whether eDirectory Agent is receiving a user name and identifying that user:

a. Activate eDirectory Agent logging, as described under *Troubleshooting eDirectory Agent*, page 174.

b. Open the log file you have specified in a text editor.

c. Search for an entry corresponding to the user who is not being filtered properly.

d. An entry like the following indicates that eDirectory Agent has identified a user:

```
WsUserData::WsUserData()
User: cn=Admin,o=novell (10.202.4.78)
WsUserData::~WsUserData()
```

In the example above, the user **Admin** logged on to eDirectory server, and was identified successfully.

e. If a user is being identified, but is still not being filtered as expected, check your policy configuration to verify that the appropriate policy is applied to that user, and that the user name in Websense Manager corresponds to the user name in Novell eDirectory.

If the user is *not* being identified, verify that:

- The user has a Novell eDirectory account.
- The user is logging on to a domain that is included in the default root context for eDirectory user logons.

- The user is not bypassing a logon prompt.

Directory objects are incorrectly filtered by the Global policy

This occurs because some network services require domain privileges to access data on the network. When the service contacts the domain controller, it does so as the domain user name under which the service is running. This causes the actual user to be misidentified.

Similar behavior occurs when a standard Windows 200x service contacts a domain controller periodically with a user name made up of the workstation name followed by a dollar sign (wkstn$). DC Agent interprets the service as a new user, for which no policy has been assigned.

To correct this problem, DC Agent can be configured to ignore any logon of the form workstation$. Add the following entry to the `transid.ini` file and then restart the DC Agent service:

```
IgnoreDollarSign=true
```

Remote users are not being filtered correctly

If remote users are not being filtered, or are not being filtered by particular policies assigned to them, check the RADIUS Agent logs for the message **Error receiving from server: 10060** (Windows) or **Error receiving from server: 0** (Linux/Solaris).

This usually occurs when the RADIUS server does not recognize RADIUS Agent as a client (source of RADIUS requests). Ensure that your RADIUS server is configured properly (see *Configuring the RADIUS environment*, page 150).

You can use RADIUS Agent's built-in diagnostic tool to troubleshoot filtering problems (see *Troubleshooting RADIUS Agent*, page 161).

If you have implemented the Remote Filtering feature (see *Filtering remote clients*, page 126), remote users cannot be filtered if the Remote Filtering Client cannot communicate with the Remote Filtering Server within the network.

For instructions on setting up Remote Filtering, see the installation guide.

Quota, continue, or password override doesn’t work as expected

If a user gets a block message when accessing a website using quota time, password override, or the continue option, the following may apply:

- An internet transaction is interrupted. For example, a user is filling out an internet purchase form during a quota session, the quota session expires. The user submits the form, but since the quota time has expired, Network Agent intercepts the request and presents the user with a block page. The request is still sent out, and is processed by the external web server.

  Meanwhile, the user starts another quota session to complete the form, re-sending the same request to the external server. The server returns an error because it has received duplicate requests.
- You have a load-balancing configuration where multiple Policy Servers may govern a single user at certain times. In this situation, quota, continue, and password override features may not function properly. For more information, see *Multiple Policy Server environment*, page 42.

Filtering does not occur after an IP address change

This can occur because Policy Server does not recognize an IP address change. For more information, see *Changing an IP address*, page 195.

Try the following:

1. Use the `ping` command to verify that machines affected by the IP address change can communicate.
2. Ensure that all Websense services are running.
3. If filtering is still non-functional, check the `secureid` parameter in the `websense.ini` file for all Websense components affected by the IP address change. By default, this parameter is set to 1 (enabled). If you have disabled `secureid` (set it to 0), the automatic IP update broadcast system may fail.

If you need to change an IP address, ensure that `secureid` is enabled while you are making the change. If this requires editing `websense.ini`, first stop the Websense Policy Server and Websense Filtering Service (see *Stopping or starting Websense services*, page 191). You can disable `secureid` again after making the change.

Block messages

A Websense block message does not appear for a blocked file

If a block message does not appear for a blocked file type, the block message may be called but not visible to the user. For example, when a downloadable file is contained within an internal frame, the block message sent to that frame is not visible because the frame size is zero.

This is only a display problem; a user cannot access or download the blocked file. If Filtering Service is installed on a multi-homed machine, identify Filtering Service in your network.

Windows

- Enter the IP address of the machine running Filtering Service as a resource record in your DNS server. See the DNS server documentation.
- *If you do not have internal DNS:* Add an entry to the `EIMserver.ini` file.

  a. Open the Windows Services dialog box.

     Windows NT/2003: Select **Start** > **Settings** > **Control Panel**, and then double-click **Services**.

     Windows 2000: Select **Start** > **Programs** > **Administrative Tools** > **Services**.

  b. Select **Websense Filtering Service** from the list, and then click **Stop**.

  c. Click **Close** to exit the **Services** dialog box.

  d. Go to the Websense installation directory.

  e. Open the `EIMserver.ini` file in a text editor.

  f. In the `[WebsenseServer]` area, enter on a blank line:

     ```
     BlockMsgServerName = <IP address>
     ```

     where *<IP address>* is the IP address of the machine running Filtering Service.

  g. Save the file.

  h. Open the Services dialog box.

  i. Select **Websense Filtering Service** from the list, and then click **Start**.

  j. Click **Close** to exit the Services dialog box.

Solaris or Linux

- Enter the IP address of the machine running Filtering Service as a resource record in your DNS server. For instructions, see the DNS server documentation.
- *If you do not have internal DNS:* Add an entry to the `EIMserver.ini` file.

  a. Go to the Websense installation directory on the machine running Filtering Service.

  b. Stop the Websense Filtering Service using the command:

  ```
  ./WebsenseAdmin stop
  ```

  c. Open the `EIMserver.ini` file in a text editor.

  d. In the *`[WebsenseServer]`* area, enter on a blank line:

  ```
  BlockMsgServerName = <IP address>
  ```

  where <*IP address*> is the IP address of the machine running Filtering Service.

  e. Save the file.

  f. Start Filtering Service (see *Stopping or starting Websense services*, page 191).

A blank white page displays instead of the block message

Possible reasons are:

- When the Advertisements category is blocked, Websense software sometimes interprets a request for a graphic file as an advertisement request, and displays a blank image instead of a block message (the normal method for blocking advertisements). If the requested URL ends in .gif or similar, have the user reenter the URL, leaving off the *.gif portion.
- Some older browsers may not detect the encoding of block pages. To enable proper character detection, configure your browser to display the appropriate character set (UTF-8 for French, German, Italian, Spanish, Brazilian Portuguese, Simplified Chinese, Traditional Chinese, or Korean; and Shift_JIS for Japanese). For more information, see the Netscape or Microsoft Internet Explorer documentation.

A “Page not found” error appears instead of a block message

If an HTTP 404 error or a proxy-generated error page appears on a client machine instead of the expected Websense block page, the client’s browser might be configured to use an external proxy. In most browsers, there is a setting that enables use of an external proxy. Verify that the browser is not set to use an *external* proxy.

A protocol block message does not appear in Windows

In Windows 200x, the Messenger service must be running on both the client and Websense server machines for the protocol block message to display to a client, even if the protocol request was blocked normally. Check the Services dialog box to see if the Messenger service is running.

The Websense User Service must be installed on a Windows machine in order for protocol block messages to display properly. For more information, see the installation guide.

A protocol block message appears instead of a block page

If your integration product doesn't send HTTPS information to Websense software, or if Websense software is running in stand-alone mode, Network Agent may interpret an HTTPS site request that is blocked via category settings as a protocol request. As a result, a protocol block message is displayed. The HTTPS request is also logged as a protocol request.

Protocol block messages do not appear as expected

- Protocol block messages may not reach client machines if Network Agent is installed on a machine with multiple network interface cards (NICs), and a NIC is monitoring a network segment separate from Filtering Service. Ensure that the Filtering Service machine has NetBIOS and Server Message Block protocol access to client machines, and that port 15871 is not blocked.
- A protocol block message may be slightly delayed, or appear on an internal machine where the requested protocol data originated (instead of on the client machine), when Network Agent is configured to monitor requests *to* internal machines.

Logs, status messages, and alerts

I am looking for download and error messages

Windows 200x

Check the Windows Application Event log for listings about database download or other error and status messages. Access the log via **Start > Programs > Administrative Tools > Event Viewer**. Click **Application log**.

Solaris or Linux

Websense software creates `Websense.log` in the `\Websense\` directory when there are errors to record. This log records error messages and messages pertaining to database downloads.

Some protocol requests are not being logged

A few protocols, such as those used by ICQ and AOL, prompt users to log onto a server having one IP address, and then send a different identifying IP address and port number to the client for messaging purposes. In this case, all messages sent and received may not be monitored and logged by the Websense Network Agent, because the messaging server is unknown at the time messages are exchanged.

As a result, the number of requests logged may not match the number of requests actually sent. This affects output in Real-Time Analyzer and Reporter.

Two log records are generated for a single request

This can occur if Windows QoS Packet Scheduler is installed on the same machine as the Websense Network Agent. In this case, Network Agent logs 2 requests for each single HTTP or protocol request made from the Websense Network Agent machine. (This duplication does not occur with requests made by client machines within your network.)

To fix the problem, disable Windows QoS Packet Scheduler on the Network Agent machine.

This problem will *not* occur if you use Network Agent for all logging purposes. For how to enable full logging, see the installation guide.

Onscreen alerts are truncated with the Samba client on Linux

When Samba client version 3.x is in use, and the active DOS character set is CP850, onscreen alerts sent to Windows client machines can be truncated.

To eliminate truncation of alert message text, change the character set used by Samba. To do this, edit the file `smb.conf`, locate the `[global]` section, and set `dos charset` equal to `UTF-8`. Save the file.

For more information about alerting, see *Alerting*, page 199.

Policy Server

I forgot my Policy Server password

If you forget your Policy Server password, call Websense Technical Support for assistance (see *Websense Technical Services Support Center*, page 337).

I cannot log on to Policy Server via Websense Manager

Websense Manager might be looking for an outdated IP address for Policy Server. If you have changed the IP address of the Policy Server machine, remove the old Server from Websense Manager, add the Server with its new IP address, and then log on to the server again (see *Adding a server*, page 186).

If Websense Manager has been stopped via the `kill` (Linux/Solaris) or **End Task** (Windows) commands, restart the Websense Policy Server to log on to Policy Server again (see *Stopping or starting Websense services*, page 191). Alternatively, wait for the current Policy Server session to time out (see *Session management*, page 228).

Corporate Edition users: If an administrator cannot log on to Policy Server after Websense Manager has exited suddenly, restart the Websense Policy Server service (see *Stopping or starting Websense services*, page 191), and then log on again. Policy Server remembers who was previously logged on.

Policy distribution

Manager does not display distributed policy information

This can occur when you are viewing multiple Policy Servers at the same time. If data is distributed from one Policy Server to another while both servers are open concurrently, Websense Manager may not display updates for the second Policy Server.

To correct this problem, ensure that you are logged in to the second Policy Server. This may require logging back on to the server.

Distributed policy configuration data is lost

Multiple administrators may be using Websense Manager simultaneously. In Websense versions *earlier than v6.1*, distributed configuration changes can be lost when one administrator distributes Policy Server data while another administrator is connected to Websense Manager. If the second administrator uses the **Save Changes** button to save additional changes, this action overrides data distribution.

To reinstate distributed changes, have the second administrator close and then re-open Websense Manager. Then, redistribute the data.

An authentication error appears during policy distribution

If you see an *authentication failure* error during policy distribution, the destination server password may be missing.

To verify that there is a password specified for policy distribution, select **Server** > **Distribution Settings**. Verify that an appropriate password is entered for each destination Policy Server. Then, try again to distribute policy data.

General issues

RADIUS Agent does not start

If RADIUS Agent does not start, check your RADIUS Agent logs for the message **Cannot bind to port: 10048** (Windows) or **Cannot bind to port: 98** (Linux/Solaris).

Typically, another application (for example, a second instance of RADIUS Agent, or the RADIUS server) is currently running on the RADIUS Agent machine and using the same port RADIUS Agent is defined to use. Ensure that each RADIUS application on the RADIUS Agent machine uses a different port.

eDirectory Agent mis-counts eDirectory Server connections

If eDirectory Agent is monitoring more than 1000 users in your network, but shows only 1000 connections to the Novell eDirectory server, it may be due to a limitation with the Windows API that conveys information from the eDirectory server to the Websense eDirectory Agent. This is unlikely, and affects a minority of users.

To work around this limitation, add a parameter to the `wsedir.ini` file that counts server connections accurately (*Windows only*):

1. Stop the Websense eDirectory Agent service.
2. Go to the Websense installation directory.
3. Open the `wsedir.ini` file in a text editor.
4. Enter on a blank line:

   ```
   MaxConnNumber = <NNNN>
   ```

   where <*NNNN*> is the maximum number of possible connections to the Novell eDirectory server. For example, if your network has 1,950 users, you may want to enter 2000 as the maximum number.
5. Save the file.
6. Restart the **Websense eDirectory Agent** service.

User authentication fails in an English operating system set for an Asian locale

In a Windows operating system installed in English and set to an Asian locale (Japanese, Chinese, or Korean), Websense software cannot authenticate users unless the Policy Server locale is set to the appropriate language. The user is prompted to log on manually (which will fail), or is filtered by the **Global** policy, depending on your Websense configuration.

The same is true for DC Agent, which cannot detect Asian language domains unless restarted by a user whose locale is set appropriately. In this case, users cannot be authenticated, and the **Global** policy is applied.

To set a service to the proper locale:

1. Stop the service in the Services dialog box (see *Stopping or starting Websense services*, page 191).
2. Right-click the service name, and then select **Properties**.
3. *(Windows 200x)* Go to the **Log On** tab.
4. Select **This account**, and then enter a logon ID and password that have the proper locale. Locales for logon IDs are set at the domain level in your network.
5. Click **OK** to verify your logon ID.
6. Restart the service.

RTA does not report information immediately after restarting

When RTA restarts, it registers with Policy Server, causing Filtering Service to re-connect. This reconnection can result in a loss of data over the brief period of time during which Filtering Service cannot send data to RTA.

An alert appears stating that RTA cannot contact Policy Server

Check whether Filtering Service and Policy Server are running. Real-Time Analyzer (RTA) relies on these components for operations. RTA cannot start until Policy Server is running.

APPENDIX A

Technical Support

Websense, Inc., is committed to providing excellent service worldwide. Our goal is to provide professional assistance in the use of our software wherever you are located.

Websense Technical Services Support Center

Technical information about Websense products is available 24 hours a day on the internet at:

www.websense.com/global/en/SupportAndKB/

This site contains the latest release information, a Knowledge Base, product documentation, and other information.

Premium support

Websense, Inc., offers 2 premium fee-based support options: Priority One 24x7 Support and Platinum Support. These options are available to United States customers only.

Priority One 24x7 Support offers a toll-free number and extended 24x7 service to customers.

Platinum Support is our most comprehensive support and education offering. It includes the advantages of Priority One 24x7 Support as well as a dedicated support team, highest priority service, and educational opportunities.

For information about Priority One 24x7 and Platinum Support services, please visit our website at:

www.websense.com/global/en/ProductsServices/Services/

For additional information, please contact our Sales Department at **800.723.1166** or **+1 858.320.8000**, or send an email to **sales@websense.com**.

Support options

Websense Technical Support can be requested 24 hours a day.

Web Portal

You can submit support tickets through the Web Portal 24 hours a day. The response time during business hours is approximately 4 hours. Response to after-hours requests will occur the next business day. Support tickets can be submitted at:

www.websense.com/global/en/SupportAndKB/CreateRequest/

Telephone assistance

Before you call a Websense Technical Support representative, please be ready with the following:

- Websense subscription key
- Access to Websense Manager
- Access to the machine running Filtering Service, the Websense Reporter server, and the database server (MSDE or SQL)
- Permission to access the Websense Log Database
- Familiarity with your network's architecture, or access to a person who has this knowledge
- Specifications of the machines running Filtering Service and Websense Manager
- A list of other applications running on the Filtering Service machine

For severe problems, additional information may be needed.

Standard telephone assistance is available during normal business hours Monday through Friday at the following numbers:

- San Diego, California, USA: **+1 858.458.2940**
- London, England: **+44 (0) 1932 796244**

Customers in Japan should contact their distributor for the most rapid service.

Customer Care

Contact Customer Care for assistance with:

- General concerns
- Subscription key questions or issues
- Follow-up on telephone support issues
- General service requests

A Customer Care representative can be reached at:

- Customer Care U.S. in San Diego, California: **866.355.0690** (from the U.S.only) or **+1 858.320.9777**, or **customercare@websense.com**
- Customer Care International in Dublin, Ireland: **+353 (0) 1 6319360** or **intcustcare@websense.com**

Improving documentation

Websense, Inc., understands the value of high quality, accurate documentation. If you have any suggestions for improving the documentation, contact us at **DocFeedback@websense.com**. We appreciate your input.

Index