



ADMINISTRATOR'S GUIDE

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

v6.2

©1996–2006, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published April 14, 2006

Printed in the United States of America 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

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

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

Trademarks

Websense 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

Copyright (c) 1999 - 2006 NetGroup, Politecnico di Torino (Italy).

Copyright (c) 2006 CACE Technologies, Davis (California).

All rights reserved.

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

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

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

Table of Contents

Chapter 1: Introduction	13
Overview	14
Filtering Defaults.....	15
Subscriptions.....	17
Websense Editions.....	20
Contact Information Web Page	20
Getting Started	21
Quick Start to Managing Internet Access	21
Websense Manager Interface.....	23
Customizing Websense	28
Chapter 2: Websense Components	31
Filtering	32
Policy Server	32
Filtering Service.....	33
Network Agent.....	33
Websense Master Database	33
Websense Manager	34
Websense Usage Monitor	34
Remote Filtering Service	34
Remote Filtering Client.....	35
User Identification	35
User Service	35
DC Agent.....	35
Logon Agent	36
RADIUS Agent.....	36
eDirectory Agent.....	36
Reporting.....	37
Websense Enterprise® Reporter.....	37
Websense Enterprise Real-Time Analyzer™	38

Chapter 3: Filtering Basics	39
Filtering Order	39
Ensuring Subscription Compliance	39
Determining the Policy	40
When Multiple Group Policies Apply	41
Filtering the Site	42
Multiple Policy Server Environment.....	47
Continue	48
Quotas	49
Quota Time and Applets	53
Password Override	53
Remote Filtering	53
Block Messages.....	54
Customized Block Messages	56
Customizing the Default Block Messages	59
Creating an Alternate Block Message	64
Filtering and the Websense Master Database.....	65
Database Downloads	65
Setting the Download Schedule	67
Resumable Downloads	69
Categories and Protocols in the Master Database.....	69
Websense Security Protocol Groups	71
New Categories and Protocols	71
Websense Real-Time Security Updates	72
Special Events	74
Adding Your Own Sites	74
Premium Groups	74
Matching Sites in the Master Database	76
URL Matching.....	76
URL Pattern Matching	76
IP Address Matching	77
Virtual Host Recognition.....	78
CGI Requests.....	78
Logging and Reporting	79
Risk Classes	81

Chapter 4: Network Agent	83
Installation	85
Initial Configuration	85
NICs on the Network Agent Machine	85
Configuring the Agent.....	88
Global Settings	89
Local Settings	93
Network Interface Card (NIC) Settings	95
Filtering Internet Content.....	99
Managing HTTP Traffic	100
Managing Protocols and Internet Applications	101
Blocking Ports, IP Addresses and Signatures	101
Protocol Usage	102
Measuring Network Bandwidth.....	102
Filtering Protocols	104
Filtering Internet Sites.....	104
Chapter 5: Clients	105
Adding Directory Objects	107
Adding Workstations	113
Adding Networks	114
Deleting Clients	115
Password Override.....	115
Enabling Password Override	116
Changing the Password	117
Disabling Password Override	117
Quota Time	118
Default Quota Time	118
Quota Time Allocated to Specific Clients	119
Filtering Remote Clients.....	120
How Remote Filtering Works.....	121
Virtual Private Network (VPN) Connections	121
How Websense Identifies Remote Users	122
Manual Authentication and Remote Clients.....	122
Chapter 6: User Identification	123

Directory Services.....	124
Transparent Identification	125
Combining Transparent Identification Agents	126
Transparent Identification and Remote Connections	128
Remote Transparent Identification with DC Agent	128
Remote Transparent Identification with RADIUS Agent.....	128
The Websense DC Agent	129
Installing DC Agent	131
Configuring User Service to Communicate with DC Agent	135
The Websense Logon Agent	142
Configuring Filtering Service to Communicate with Logon Agent .	143
Troubleshooting DC Agent or Logon Agent.....	148
Windows Services (or Service Control Manager).....	148
Windows Event Viewer	148
Websense Log	149
Websense Technical Support and the Websense ConsoleClient .	149
The Websense RADIUS Agent.....	150
Processing RADIUS Traffic.....	151
Installing RADIUS Agent	152
Configuring the RADIUS Environment	152
Configure RADIUS Agent and Filtering Service	154
Configuring RADIUS Agent to Ignore Certain User Names	159
Configure the RADIUS Client	160
Configure the RADIUS Server.....	161
Starting and Stopping RADIUS Agent.....	165
Starting in Console Mode	165
Starting in Service Mode (Windows)	166
Starting in Daemon Mode (Linux/Solaris).....	166
Stopping RADIUS Agent	166
Command Attributes	167
Troubleshooting RADIUS Agent	168
The Websense eDirectory Agent.....	169
Configuring the eDirectory Environment	171
Configure Novell eDirectory	171
Determine the eDirectory Agent Protocol.....	172
Configure eDirectory Agent and Filtering Service	173

Configuring eDirectory Agent to Ignore Certain User Names..	177
Configuring a Multiple-Replica Environment.....	178
Starting and Stopping eDirectory Agent	179
Starting in Console Mode	179
Starting in Service Mode (Windows).....	179
Starting in Daemon Mode (Linux/Solaris).....	179
Stopping eDirectory Agent.....	180
Troubleshooting eDirectory Agent.....	181
Configuring Different Settings for an Agent Instance	182
.ini Parameter to Field Name Correspondences	185
Directory Service Access	187
Windows NTLM-based Directory.....	187
Windows 2000/2003 Environment.....	188
LDAP-based Directory.....	192
Active Directory.....	193
Sun Java System Directory Server.....	198
Novell eDirectory	202
Custom Object Class Types	205
Manual Authentication.....	208
Enabling Websense Manual Authentication	208
Chapter 7: Server Administration	211
Adding a Server	212
Logging On to a Server.....	213
Changing the Policy Server Password	214
Configuring a Server	215
Stopping or Starting Websense Services.....	217
Windows	217
Solaris or Linux.....	218
Configuring Download Via Proxy	218
Removing a Server	220
Saving the Configuration.....	221
Backing Up the Configuration File	221
Restoring the Configuration File	222
Changing an IP Address	222
Network Agent.....	223

Policy Server	224
Integrated products and plug-ins.....	226
Alerting.....	227
Flood Control.....	228
Setting Up Alerting	229
Disabling Alerting	236
Administrative Auditing	237
Distributed Administration and Reporting	241
Removing Websense.....	242
Chapter 8: Distributed Administration	245
Overview: Setting Up Distributed Administration	246
Managing Roles.....	247
Administrator Roles.....	247
Managed Clients	249
Working with Roles.....	250
Creating a Role	252
Assigning an Administrative Role.....	254
Adding Clients to an Administrative Role	255
Removing an Administrator from a Role	257
Session Management	258
Lockouts.....	260
Defining Filtering Restrictions	261
Creating a Web Filter Lock.....	263
Central Configuration Distribution.....	269
Policy Server Relationships	270
Changing the Central Policy Server	270
Distributing Configuration Settings.....	271
Multiple Policy Servers with a Single Log Server	273
Chapter 9: Setting Up Web Filtering	277
Filtering Policies.....	277
The Global Policy	279
Sample Policies.....	279
Custom Policies	280
Adding a Policy.....	280

Editing a Policy	281
Assigning Policies to Clients.....	283
Assigning a Policy to a Single Client	284
Assigning a Policy to Multiple Clients	285
Viewing Assigned Policies	286
Distributing Policies to Multiple Servers	287
Directory Services and Policy Distribution	290
Single Log Server Environment.....	290
Distributing Policies	291
Printing Policies to a File	293
Deleting a Policy.....	295
Managing Sites	296
Category Sets/Yes Lists	296
File Types	297
Permanent Category Sets	303
Yes Lists	303
Adding a Yes List.....	308
Applying a Yes List to Clients	311
Adding a Category Set.....	313
Editing a Category Set.....	314
Copying a Category Set.....	317
Deleting a Category Set.....	317
Custom URLs	319
Custom-permitting Sites	320
Using Custom URLs for Sites With Multiple Addresses	323
Recategorizing URLs.....	324
Deleting Custom URLs	328
Adding a Custom Category.....	328
Editing a Category	330
Deleting a Custom Category.....	330
Keywords.....	331
Setting Up Keyword Blocking	332
Adding Keywords.....	333
Deleting Keywords.....	336
Managing Protocols	337
Defining Protocols	338
Port Blocking	340
How Protocols Are Filtered.....	341

TCP and UDP Support	341
Block Messages	342
Displaying Protocol Block Messages in Windows	343
Protocol Filtering Options	344
Instant Messaging Attachment Manager	346
Bandwidth Management	347
Bandwidth Limits	348
Protocols and User Identification	350
Permanent Protocol Sets	351
Customizing Protocols and Protocol Sets	351
Creating a Custom Protocol	352
Editing a Custom Protocol	355
Removing a Protocol	355
Adding to a Websense Protocol Definition	356
Adding a Protocol Set	357
Editing a Protocol Set	357
Configuring Protocol-based Filtering	359
Chapter 10: Troubleshooting	363
The Master Database does not download	364
Subscription Key	364
Internet Access	365
Firewall Restrictions	366
Restriction Application	366
Master Database download does not occur at the time specified ..	367
I made a mistake during installation	367
Where can I find download and error messages?	367
Windows NT	367
Windows 200x	367
Solaris or Linux	367
I forgot my Policy Server password	368
I cannot log on to Policy Server via Websense Manager	368
Sites in the Information Technology category are being blocked ..	368
Online Help shows a blank frame when viewed in Netscape 6.x ..	369
Keywords are not being blocked	369
Sites in blocked categories are not always being blocked	370
Custom or yes list URLs are not being filtered as expected	370
A Websense block message does not appear for a blocked file ...	371

Windows	371
Solaris or Linux.....	372
A blank white page displays instead of the block message.....	373
A “Page not found” error appears instead of a block message	373
A protocol block message does not appear in Windows	373
A protocol block message appears instead of a block page	374
Protocol block messages do not appear as expected	374
Some protocol requests are not being logged.....	374
A user cannot access a protocol or application as expected.....	375
An FTP protocol request is not blocked as expected	375
Two log records are generated for a single request	375
Websense is not filtering based on a directory object policy	376
Directory objects are incorrectly filtered by the Global policy	379
Remote users are not being filtered correctly.....	380
RADIUS Agent does not start.....	380
eDirectory Agent mis-counts eDirectory Server connections	381
Quota, continue, or password override doesn’t work as expected	381
Manager does not display distributed policy information	382
Distributed policy configuration data is lost	382
An authentication error appears during policy distribution.....	382
Filtering does not occur after an IP address change	383
User authentication fails in an English operating system set for an Asian locale	383
RTA does not report information immediately after restarting	384
An alert appears stating that RTA cannot contact Policy Server ...	384
Chapter 11: Practical Applications	385
Scenario 1: Monitoring Access Trends	386
Scenario 2: Permitting Travel Sites.....	387
Scenario 3: Deferring News and Media Sites	390
Add a Category Set	390
Edit the Policy	391
Scenario 4: Assigning a Different Policy	394
Add Directory Objects.....	394
Create a New Policy	396
Assign a Policy	397

Scenario 5: Using Yes Lists and Password Override	398
Add a Workstation	398
Set Up a Yes List	398
Assign Password Override Privileges	399
Scenario 6: Blocking Keywords	400
Scenario 7: Recategorized Custom URLs	402
Create a Custom Category	402
Add Recategorized Custom URLs	403
Scenario 8: Quotas	404
Configure Quota Session and Default Quota Time	405
Allocate Quota Time to Specific Clients	406
Scenario 9: Filtering Video and Audio Internet Media.....	407
Block File Types.....	407
Block a Protocol	408
Appendix A: Technical Support	409
Before Contacting Websense Technical Support	409
Websense Technical Support Services	409
Premium Support.....	410
Support Options.....	410
Web Portal	410
Email Questions	411
Telephone Assistance	411
Customer Care	412
Improving Documentation.....	412
Index.....	413

Introduction

Thank you for choosing Websense software, the system managing employee computing resources worldwide. 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 guide is for use with:

- ◆ 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 is an invaluable tool in minimizing employee downtime caused by 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 also 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 modules can greatly enhance your organization's regulation of employee desktop software and hardware. See your *Websense Enterprise Client Policy Manager Administrator's Guide* for details on obtaining and installing these modules.

Websense, Inc. strongly recommends that users be informed of your policies concerning internet access, and that Websense software has been installed as a tool for monitoring activity and/or enforcing the policies.

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

Overview

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

Each Websense component performs a particular function. See [Chapter 2 Websense Components](#) for component descriptions.

Websense Enterprise Reporter, along with its associated Log Server, is a separate program included with Websense software. After installation, Log Server records internet activity in your network. Reporter then allows you to generate a wide variety of reports and charts depicting your network's internet usage trends. These 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. Please install or upgrade Reporter as appropriate in order to generate reports.

Websense Enterprise Explorer is an optional reporting component that also uses the Websense Log Server. Explorer provides a sophisticated, browser-based view of internet usage. See your Websense Enterprise Reporting documentation for more information about Explorer.

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

RTA lets you drill down into internet access reports, and allows you to view internet usage trends for your network. You can also use the information from RTA reports to help you fine-tune your internet usage policies.

Using Reporter, Explorer and RTA, you can view and analyze internet usage data in your network in any number of ways. See your Reporting Tools documentation for information.

Filtering Defaults

For your convenience, the **Global** policy begins filtering according to its default settings immediately following download of the Websense Master Database.

Websense software automatically installs predefined settings for filtering internet protocols and applications, and uses these until configured otherwise. See *Managing Protocols*, [page 337](#) for information about protocol filtering, and about filtering internet content based on bandwidth usage within your network.

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



NOTE

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

The **Global** policy blocks categories that are commonly considered unacceptable, and grants full or limited access to others. Use Websense Manager to modify the **Global** policy so it is suitable for the largest number of users in your organization. See [page 279](#) for more information on the **Global** policy.

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

Websense software lets you create customized policies to define varying levels of access for users. Each policy defines which URL categories and protocols are permitted, blocked, or limited at particular times during the week. See *Editing a Category Set*, [page 314](#) for category filtering settings. See *Editing a Protocol Set*, [page 357](#) for protocol filtering settings.

A yes list (see [Yes Lists, page 303](#)) 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 is appropriate to the work requirements.

When a user attempts to access an internet site, your integration product receives the request and sends it to the Websense Filtering Service (see [page 33](#)). Filtering Service identifies the policy assigned to the requestor and consults its comprehensive Master Database of URLs. 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 alerting the user that the requested site is blocked, and identifies the category under which it is blocked.

Alternatively, you can block by default all sites that are not listed in the Master Database. See your installation guide for details.

Internet content transmitted by particular network or application protocols is handled in much the same way. See [Chapter 3 Filtering Basics](#) for details on Websense filtering precedence. See [Managing Protocols, page 337](#) for information about protocol-based filtering.

In addition to full blocking, the **Limit by Quota** filtering option allows you to allocate time daily to employees for the purpose of surfing sites in categories you deem appropriate. Quotas give you control over how much time employees are spending on personal surfing and which sites they are accessing. For more information, see [Quotas, page 49](#).

For even further flexibility in filtering, you can configure customized lists of URLs to be filtered in particular ways for all users. [Custom URLs, page 319](#) provides details about this feature.

Subscriptions

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

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

The number of clients your subscription permits is displayed in Websense Manager after the first successful database download. See [Database Downloads](#), page 65 for information on entering your key and downloading the Master Database.

The total number of client machines to be 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.

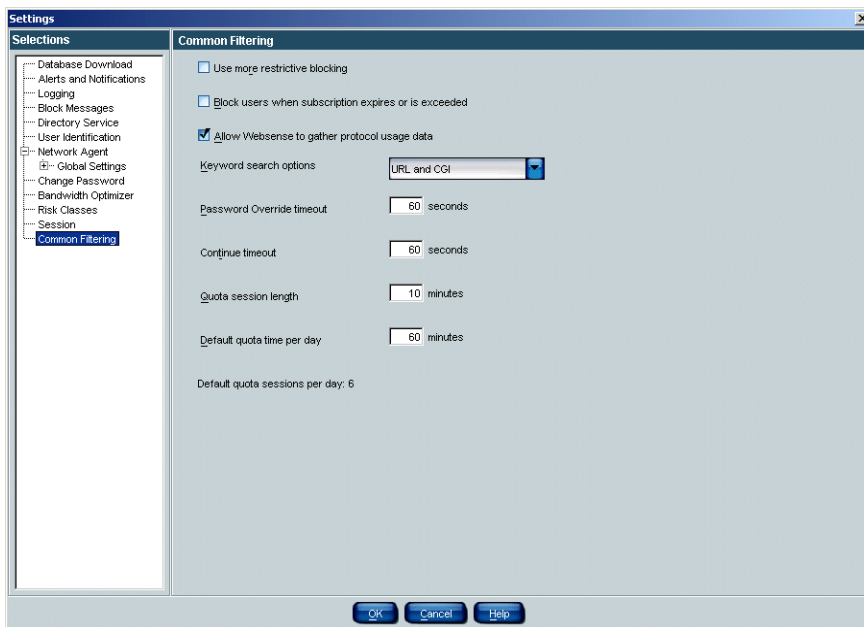
The subscription table is cleared each night. The first time a client makes an internet request after the table has been cleared, its IP address is entered in the table.

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** server setting (see the procedure that follows).

Likewise, when a subscription expires, all clients are either entirely blocked or unfiltered, depending on this global setting.

To determine filtering behavior when a subscription is exceeded:

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



Common Filtering settings

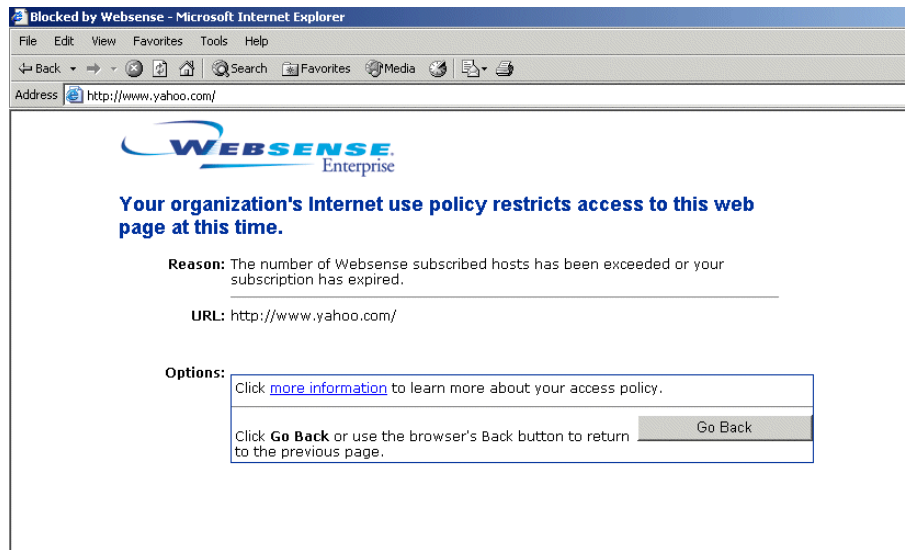
3. Check or uncheck **Block users when subscription expires or is exceeded**.

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, as well as any other clients already blocked from certain sites.

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.



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, it is possible to exceed the subscription. If this occurs, contact Websense, Inc. or your 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 229](#).

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 on Premium Groups, see [page 74](#).

Websense Editions

With the current release, there are six available 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 completed.

The page can be accessed manually in two ways:

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



Status bar in Websense Manager

View or update your Websense registration information as necessary.

Getting Started

To begin filtering internet requests, you must install Websense software, enter a valid subscription key, and download the Master Database. See your installation guide for instructions.

Chapter 2 Websense Components familiarized you with the Websense components and reporting tools. Then you can begin adding clients, and setting up filtering policies for managing those clients. *Chapter 11 Practical Applications* provides sample scenarios and tips for using these features.

Quick Start to Managing Internet Access

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



IMPORTANT

Initial, default filtering behavior is determined by your **Initial Filtering** selection during installation. If you selected **Yes**, Websense software employs the **Global** policy for all users by default. If you selected **No**, Websense software monitors and logs internet traffic, but permits all requests.

The **Global** policy is set to enforce the **Default Settings** category set and the **Default Settings** protocol set 24 hours a day, seven 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. See [page 49](#) for more information about quota time.

Premium Group categories are only available if purchased. See [Premium Groups, page 74](#) for information.

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. See [page 351](#) for instructions on customizing filtering options for protocol sets.

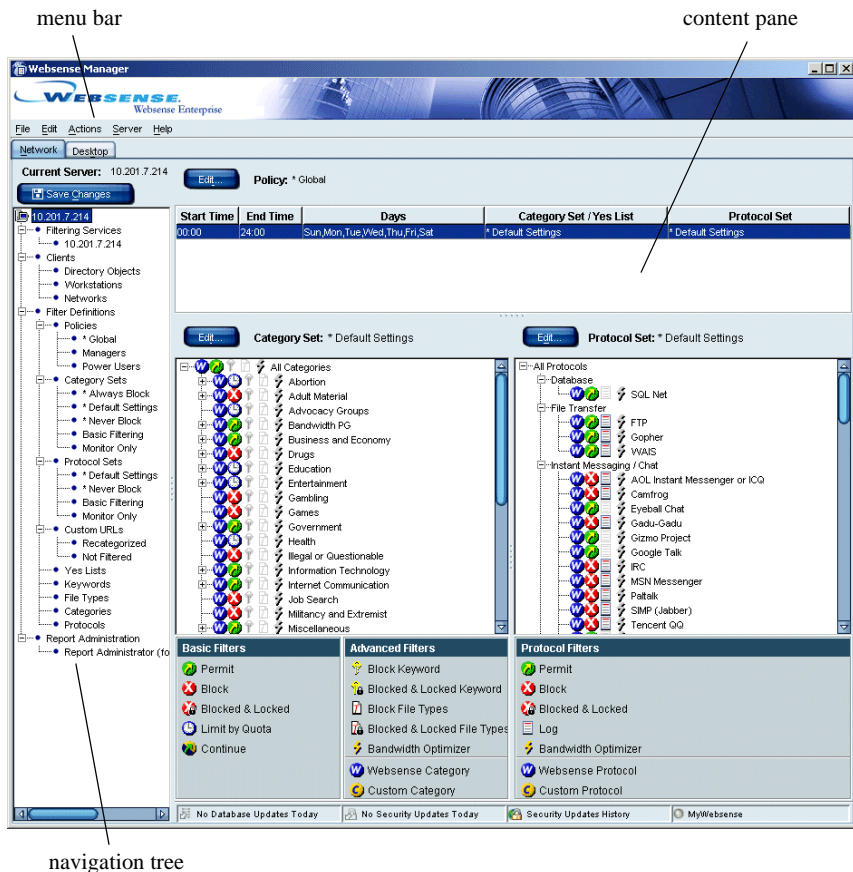
Use Websense Manager to modify the **Global** policy, or to create additional policies to meet the specific filtering needs of your organization. Instructions for modifying the **Global** policy are included under [Customizing Websense, page 28](#).

Websense Manager Interface

Websense Manager is the filtering configuration interface. This section familiarizes you with Websense Manager before you begin customizing filtering behavior (see *Customizing Websense*, page 28).

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

The Websense Manager window consists of a menu bar, navigation tree and content pane, as illustrated.



Websense Manager window

The main menu bar provides quick access to commonly-used Websense commands. Websense Manager offers shortcut menus for many functions. Right-click in the desired area and a shortcut menu displays related commands.

The **Save Changes** button sends changes made via Websense Manager to the Policy Server to which 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 this button.

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** in the **Settings** dialog box.

The **MyWebsense** button links to your personalized mywebsense.com page. See [Contact Information Web Page, page 20](#) for details about mywebsense.com.

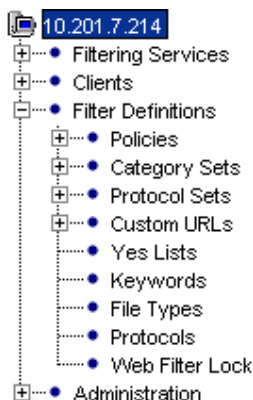
Context-Sensitive Help

Many dialog boxes have **Help** buttons. If you need assistance and a **Help** button is not available, click in the relevant area of the Websense Manager window and then press **F1**.

Navigation Tree

After Websense software has been installed and a Policy Server added, the Websense Manager navigation tree lists the Policy Servers available for configuration from this installation of Websense Manager. Once you log on to a Policy Server and enter the appropriate password (see [Logging On to a Server, page 213](#)), the navigation tree displays the topics for that server.

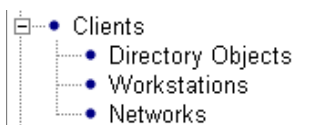
Click the plus symbol (+) beside a topic to display its child entries. For example, **Policies** can be expanded to show the individual policies that have been created for the associated Policy Server. Click one of these entries to display its details in the content pane.



Navigation tree

Topics in the navigation tree are:

- ◆ **Directory Objects, Workstations, Networks**, known collectively as “clients,” contain entries only after you add them via Websense Manager. You can add individual users and groups as defined in your directory service, as well as specific workstations. Collections of workstations, called networks, are identified as IP address ranges. See [Chapter 5 Clients](#) for information on working with clients.



Clients in navigation tree

- ◆ **Policies** are the basis of filtering. Each policy identifies which category set or yes list is enforced during particular time periods. A policy is assigned to all clients whose internet access should be filtered according to its restrictions.

Websense software comes with several sample policies (which you can edit), or you can create additional policies to meet your organization’s filtering requirements. By default, clients are filtered by the **Global** policy until another policy is assigned to them. See [Filtering Policies, page 277](#) for more information on policies.

- ◆ **Category Sets** are lists of all Websense categories, with a filtering setting designated for each category. Filtering settings include permit, block, limit by quota or file type, bandwidth-based limitations, and continue. Keyword blocking can be enabled in conjunction with any filtering settings. Category sets have descriptive names such as “Business Hours,” and are assigned to time periods within policies. See [Category Sets/Yes Lists, page 296](#) for more information on category sets.
- ◆ **Protocol Sets** are lists of all protocols with a filtering option designated for each. Filtering settings include permit, block, log, and bandwidth-based limitations. Protocol sets are assigned to time periods within policies. See [Managing Protocols, page 337](#) for more information.
- ◆ **Custom URLs/Recategorized** are sites to filter differently than their Master Database categories (including sites classified under **Miscellaneous/Uncategorized**). You can add a URL to any category. Websense software then filters the site according to the filtering setting for that category. See [Custom URLs, page 319](#) for more information.
- ◆ **Custom URLs/Not Filtered** are Master Database sites originally assigned to blocked categories but which you now permit users to access at any time.

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 two exceptions:

- if the **Always Block** category set is active
 - if a user is governed by a yes list. See [Custom URLs, page 319](#) for more information on permitted custom URLs.
- ◆ **Yes Lists** are 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 one client, yes lists take precedence over any other category set, including the **Always Block** category set. See [Yes Lists, page 303](#) for more information.

- ◆ **Keywords** let you further restrict filtering, blocking sites whose URLs contain certain words. Enter the keywords you want blocked for a category via the keywords editor. 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 331 for information on keywords.
- ◆ **File Types** are groupings of file extensions used for similar purposes. Websense software allows you to filter internet content based on file extension. For example, you can restrict access to particular types of files from sites within an otherwise-permitted category.
File type filtering is activated via policies. Websense, Inc. provides several predefined file types. You can modify these, or even create new file types to suit your needs. See [File Types](#), page 297 for more information.
- ◆ **Protocols** are Websense objects representing types of internet data transmitted via particular protocols or internet applications. You can 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. See [Managing Protocols](#), page 337 for more information about protocols.
- ◆ **Web Filter Lock** (*Corporate Edition only*) comprises key filtering restrictions to be applied to all clients. These restrictions limit 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. See [Chapter 8 Distributed Administration](#) for information.
- ◆ **Administration** (*Corporate Edition only*) is where administrative user objects are stored. 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. See [Chapter 8 Distributed Administration](#) for information.
Report Administration (*non-Corporate Edition only*) is where administrative user objects are stored. If you are not running Corporate Edition, you can still define roles and permissions for reporting purposes. See your Reporting documentation for information about using Websense Reporting Tools.

Customizing Websense

Follow these steps to configure Websense software to meet the filtering needs of your organization. This is an overview; you may need to consult the referenced sections for more details.



IMPORTANT

If you are running a Corporate Edition of Websense, the Distributed Administration and Reporting feature provides increased internet access management functionality. See [Chapter 8 Distributed Administration](#) for information on getting started with this feature.

1. If it is not already running, start Websense Manager (**Start > Programs > Websense > Websense Manager**).
2. If it is not already added, add Policy Server (see [Adding a Server](#), page 212).
3. Log on to Policy Server by right-clicking the server icon and choosing **Log On to Server**.
4. Enter the password that was established when first logging on to Policy Server.
5. If not done during installation, download the Master Database (see [Websense Master Database](#), page 33).
6. Configure the Websense Network Agent as appropriate for your network (see [Initial Configuration](#), page 85).
7. 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** to open the **Edit Policy** dialog box. See [Editing a Policy](#), page 281 for help with editing policies. Click **OK** when finished.
8. Expand **Category Sets** in the navigation tree, and then select **Default Settings**.
9. Click **Edit**, and then select the desired filtering options for each category. The filtering options you select will be enforced whenever the **Default Settings** category set is active. Click **OK** when finished. (For more information on category set editing, see [page 314](#).)

10. Expand **Protocol Sets** in the navigation tree, and then select **Default Settings**.
11. Click **Edit**, and then select the desired filtering settings for each protocol. The selected filtering settings will be enforced whenever the **Default Settings** protocol set is active. Click **OK** when finished. (For more information on editing protocol sets, see [page 357](#).)
12. Choose **Server > Settings**, and then make appropriate changes. Server configuration options are described on [page 215](#).
13. Click **OK** to save server configuration changes.
14. Click **Save Changes** above the navigation tree to update Policy Server.

After these basic steps are complete, you can begin adding category sets, protocol sets, policies, file types, custom URLs, and keywords as desired. You can also assign different policies to individual clients.

Websense Components

Understanding certain fundamental concepts and how they apply to internet filtering will help you use Websense most effectively. This chapter familiarizes you with:

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

This chapter also provides information about Websense Enterprise Reporter, a separate program included with your Websense subscription.

Filtering

Policy Server

Websense Policy Server is the component that stores server and policy configuration information. Policy Server communicates this data to Filtering Service, which filters internet requests. You can configure Policy Server settings via the user interface component, Websense Manager. Websense Manager is discussed on [page 34](#).

After installation, Policy Server automatically identifies any other Websense components. Policy Server continually tracks the location and status of other Websense services. For more information about Websense services and how to view or manually modify service status, see [Stopping or Starting Websense Services](#), [page 217](#).

If your network is large (10,000+ users), you may want to install and run multiple Policy Servers. You can replicate configuration settings from one 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 271](#) for information on distributing configuration data to multiple servers.
- ◆ *Non-Corporate Edition installations:* See [Distributing Policies to Multiple Servers](#), [page 287](#) for how to distribute policy information.

The Distributed Administration and Reporting feature, available with Corporate Editions of Websense, offers sophisticated management of multiple-server, multiple-site enterprises. See [Distributed Administration](#), [page 245](#) for information.

Filtering Service

Websense Filtering Service is the component that 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 [page 99](#)).

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.

You can view the status of Filtering Service or stop and start Websense services by following the steps on [page 217](#). You can configure several attributes of Filtering Service via the Websense Manager, discussed on [page 34](#).



NOTE

When Filtering Service is not running, filtering and logging of internet requests cannot occur. Detailed information about Websense logging and reporting is available in your *Websense Enterprise Reporting Administrator's Guide*.

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 be used to evaluate Websense internet filtering capabilities. See [Chapter 4 Network Agent](#) for functionality and configuration details.

Websense Master Database

The Websense Master Database is a collection of more than 15 million internet sites. Sites in the Master Database are categorized 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 also houses protocol definitions for use in filtering protocols. The updated list of protocols is available from:

<http://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, as needed. An up-to-date list of Websense categories is maintained on the Websense, Inc. website at:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php>

In addition to the standard categories provided in the Websense Master Database, you can optionally implement more advanced URL filtering using Websense Enterprise Premium Group categories. Premium groups and their categories are listed on the same web page.

Websense Manager

Websense Manager is the configuration interface. It can be installed 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 much more.

Once Websense software has been installed, you must configure Policy Server to communicate with Websense Manager by adding Policy Server. See [Chapter 3 Filtering Basics](#) for help getting up and running.

See [page 23](#) for an illustration of the Websense Manager interface.

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. See [Alerting, page 227](#) for more information.

Remote Filtering Service

The Websense Remote Filtering Server allows filtering of clients outside a network firewall. Your 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. See your installation guide for instructions on deploying Remote Filtering Client.

User Identification

User Service

Websense User Service communicates with your organization's directory service to convey user-related information to Policy Server and Filtering Service, for use in applying filtering policies. This information 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 [page 125](#)), User Service helps to interpret user logon session information. Specifically, 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 via Websense Manager (see [page 107](#)), User Service provides the list of objects residing in your directory service to Websense Manager, for use in configuring filtering policies.

There must be one instance of User Service for each Policy Server in your network. See [page 47](#) for information about using multiple Policy Servers.

For information about configuring directory service access and customizing directory service search filters, see [page 187](#).

DC Agent

The Websense DC Agent is an optional transparent user identification agent. The transparent identification feature allows Websense software to identify 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. DC Agent and transparent user identification are described on [page 125](#).

Logon Agent

The Websense Logon Agent is designed for unsurpassed accuracy in transparent user identification. Deploying the associated logon application to client machines in your network ensures that individual user logon sessions are captured and processed directly by Websense software. This enables the Websense Filtering Service to accurately filter internet access based on policies assigned to particular 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.

See [The Websense Logon Agent, page 142](#) for information about configuring and using Logon Agent.

RADIUS Agent

The Websense RADIUS Agent allows you to integrate your 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). You can then assign particular filtering policies to users or groups of users who access your network remotely.

See [The Websense RADIUS Agent, page 150](#) for information about installing and configuring RADIUS Agent and your RADIUS environment.

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. See [The Websense eDirectory Agent, page 169](#) for information about eDirectory Agent and making it work in your environment.

Reporting

Websense Enterprise® Reporter

Websense Enterprise Reporter is an optional application, included with Websense software, that generates tabular and graphical reports of your organization's internet use. These reports enable you to monitor internet access and fine-tune Websense software to meet your organization's employee internet management needs. Information regarding Reporter is provided in the separate Reporting documentation.

Log Server, which is installed with Reporter, stores internet requests that Websense processes. It records the following data:

- ◆ Source of a request
- ◆ Category or protocol association for 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 can also store information about number of bytes transferred.

Log Server must be running for you to generate reports with Reporter. In large organizations, Websense, Inc. recommends installing Log Server on a separate machine for better performance.

After installing Log Server, you must configure the Log Server location and port number. See [Logging and Reporting, page 79](#) for instructions.

Websense Enterprise Real-Time Analyzer™

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

RTA lets you drill down into internet access reports, and allows you to view and analyze internet usage trends for your network. You can also use RTA to verify the effectiveness of filtering in your organization. Use the information from RTA reports to help you fine-tune your internet usage policies.

RTA displays users' internet activity as it flows through Filtering Service. In order to use RTA, you must already have Policy Server, Filtering Service, a web server, and an internet browser installed. For details about managing access to RTA, see the *Websense Enterprise Reporting Administrator's Guide*. For information about using RTA, see the *Websense Enterprise Reporting User's Guide*.

This chapter familiarizes you with basic Websense filtering functionality. 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 can help you create more effective filtering policies.

For each request it receives, Websense software first verifies subscription compliance, and 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 in the following sections.

Ensuring Subscription Compliance

When Websense software receives a site request, it starts the filtering process by evaluating 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 17).

If the subscription is exceeded, you must renew or increase your subscription. To upgrade your Websense 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 down the list 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 restrictions in the **Global** policy. If the **Global** policy also has no active category set or protocol set at the time a request is made, Websense software filters according to the **Default Settings** category set and the **Default Settings** protocol set.



NOTE

This default filtering behavior applies if you selected **Yes** for **Initial Filtering** during installation. If you selected **No**, Websense software monitors and logs internet traffic, but permits all requests by default.

When Multiple Group Policies Apply

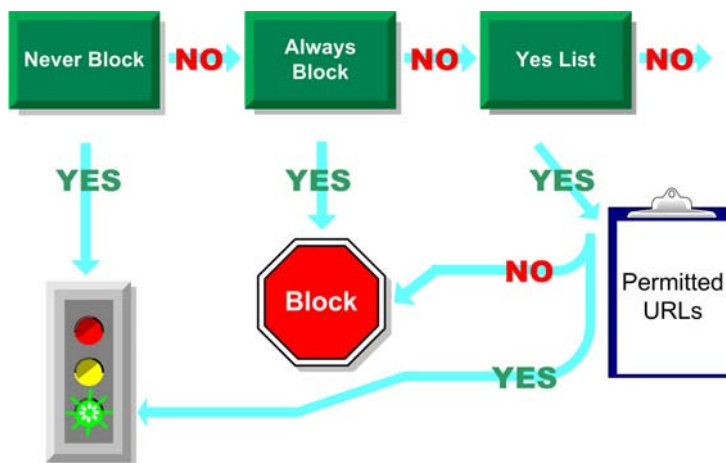
In some cases, a user belongs to more than one group and no user, workstation, or network policy applies. If this is true, Websense software checks the policies assigned to each of the user's groups. If all the groups have the same policy, Websense software filters the request according to that policy.

If one of the groups has a different policy than the others, Websense software filters the request according to the selection made in Websense Manager via **Server > Settings > Common Filtering**. If the **Use more restrictive blocking** option is checked, Websense software blocks the site if it is blocked by *any* of the policies assigned to those groups. If the option is left unchecked, Websense software permits the site if it is permitted by any of the policies assigned to those groups.

See *Yes Lists and Multiple Groups*, page 306 for more information about **Use more restrictive blocking**.

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

Filtering the Site



Determining global filtering options

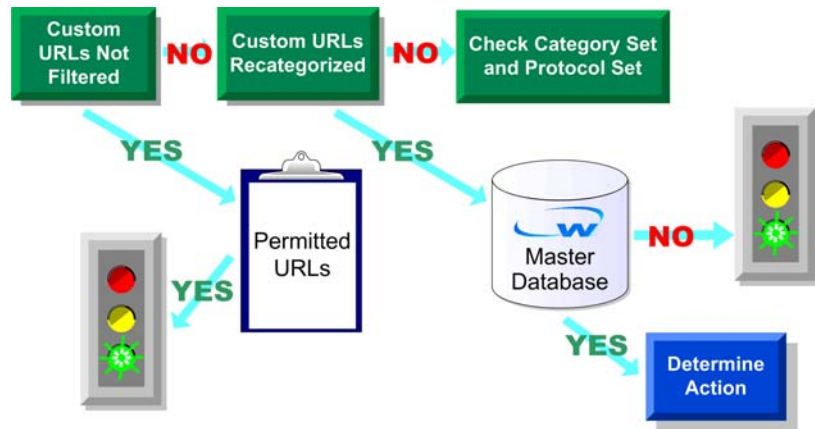
The Websense Filtering Service evaluates the policy's restrictions, in the following order, to determine whether the requested site should be permitted, blocked, or limited by quota.

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](#).



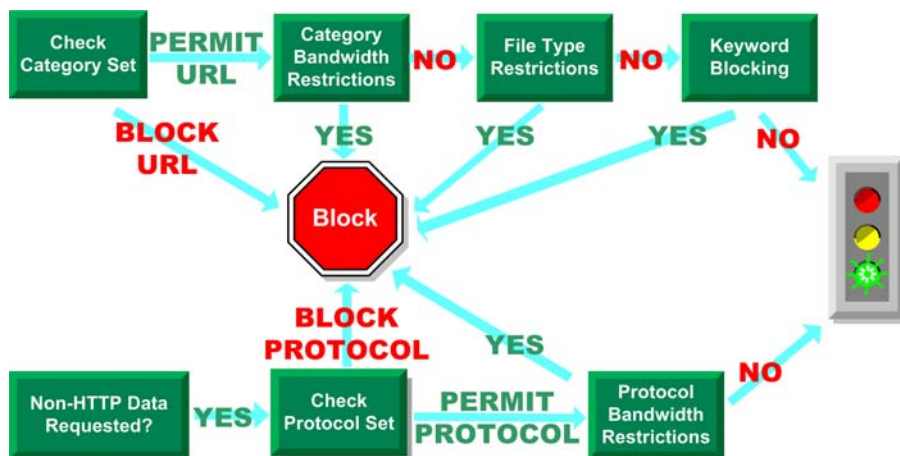
NOTE

Websense software filters URLs accessed from an internet search engine's cache just 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](#).

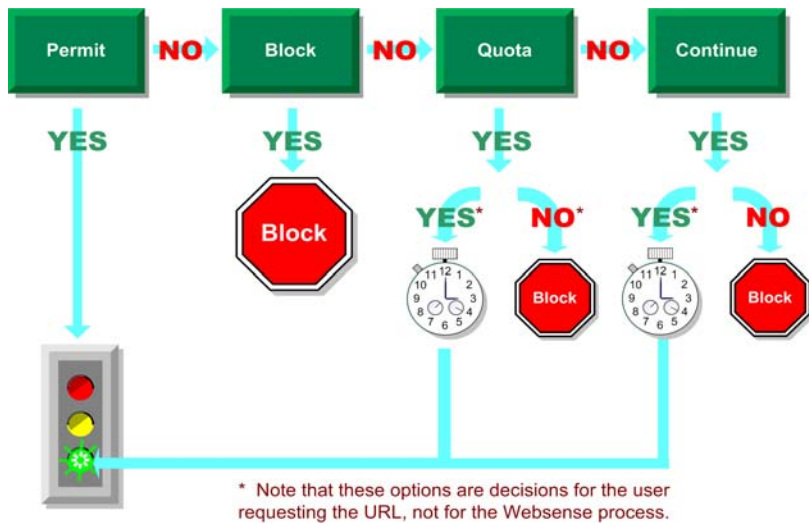


Checking the category set and protocol set

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, apply 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.

See [File Types, page 297](#) for more information about filtering based on file type.

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-related purposes.



User options for a request

Websense software proceeds through the list 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 the following 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, which is active in the **Global** policy. 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, you must perform 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 [page 119](#)).
- ◆ 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 269](#) for information about Policy Servers in a distributed environment.

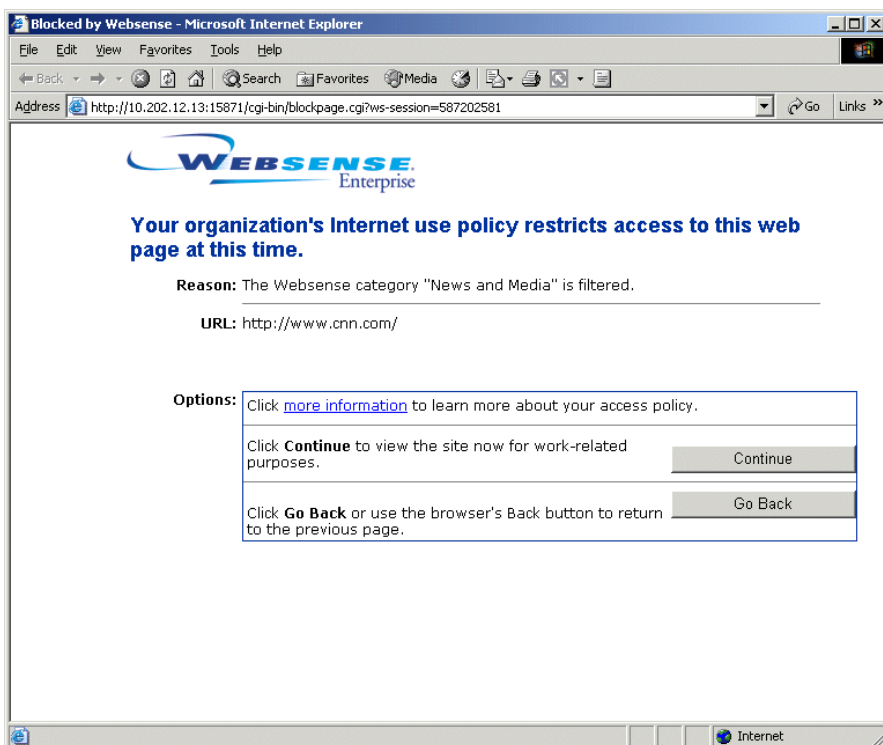
Continue

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



NOTE

In Websense versions 5.1 and earlier, the **Continue** option was associated with the **Defer to AfterWork** option.



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 edited via **Server > Settings**, under **Common Filtering**.

The Continue filtering option is activated at the category set level. See [Editing a Category Set, page 314](#) for information.

**NOTE**

The Continue filtering 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

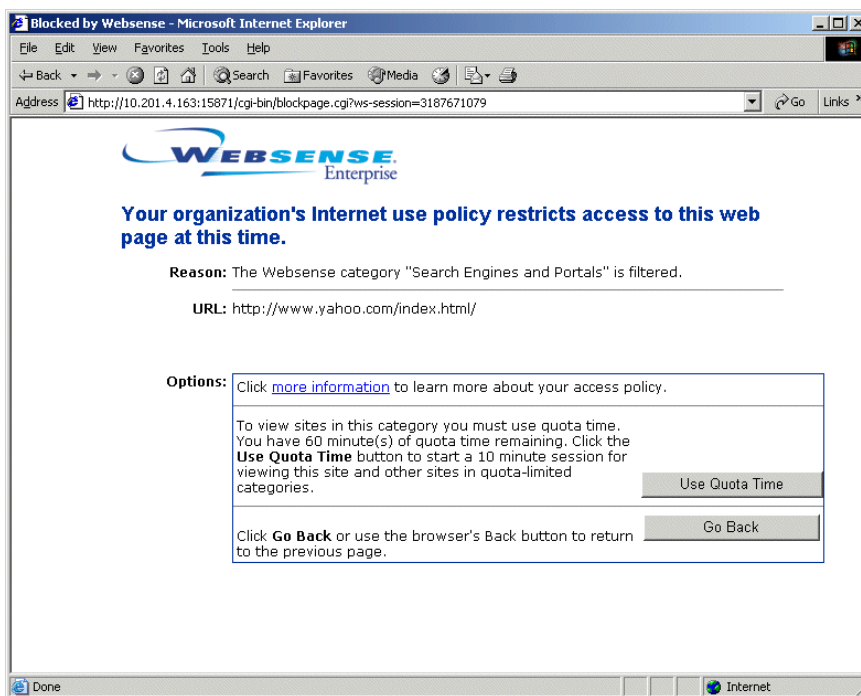
You can give employees access to sites in selected categories for a limited amount of time each day. Access is granted in configurable increments of time to sites in categories whose filtering setting is **Limit by Quota**. Quotas give you control over how much time your employees spend on personal surfing 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, you must 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.



Quota block page

Clicking the **Use Quota Time** button 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 *Quota Time Allocated to Specific Clients*, page 119 for instructions.

Once quota time has been 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:

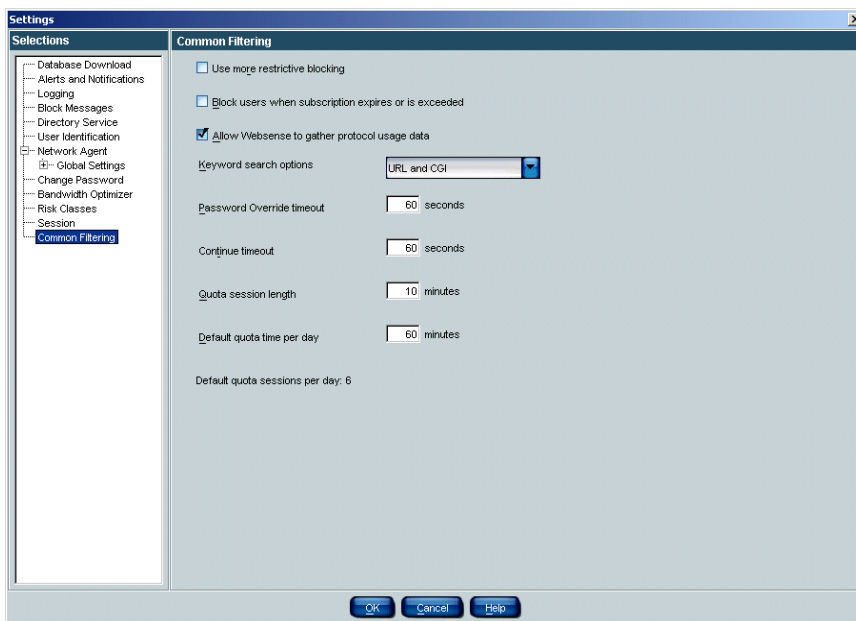
1. The user.
2. The workstation or network (range of IP addresses).
3. Groups of which the user is a member.

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, implement the following changes:

- ◆ When adding new category sets or editing existing ones, assign the **Limit by Quota** filtering setting to the appropriate categories. See [page 314](#) for instructions.
- ◆ 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 [page 281](#) for instructions).
- ◆ 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.



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 [page 119](#) for instructions.

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

The password override feature 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). When password override is activated for a user or workstation, the Websense block message includes a password field. If a valid password is entered, Websense software permits any blocked site for an allotted amount of time. See [page 115](#) for instructions on configuring password override.

Remote Filtering

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

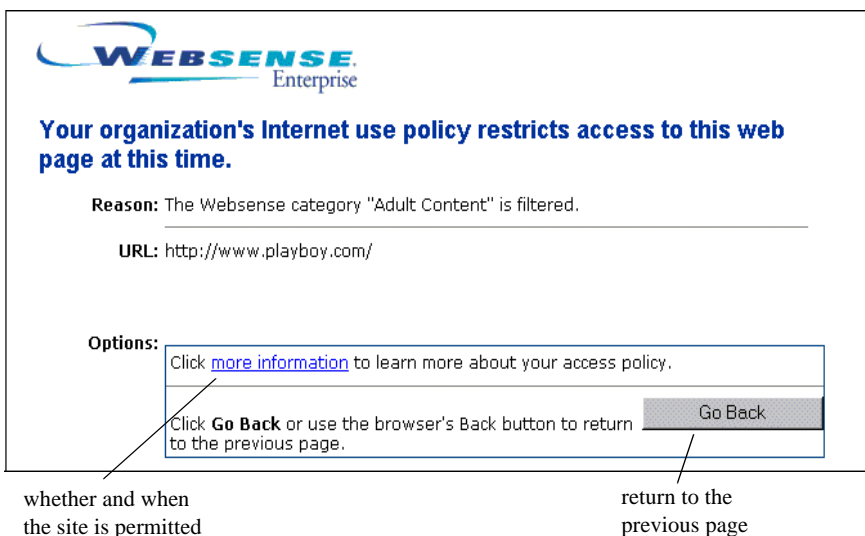
- ◆ Installing the Websense Remote Filtering Server and Remote Filtering Client according to the instructions in your installation guide.
- ◆ Ensuring that remote users can be successfully identified.

See *Filtering Remote Clients*, [page 120](#) for more information about Remote Filtering.

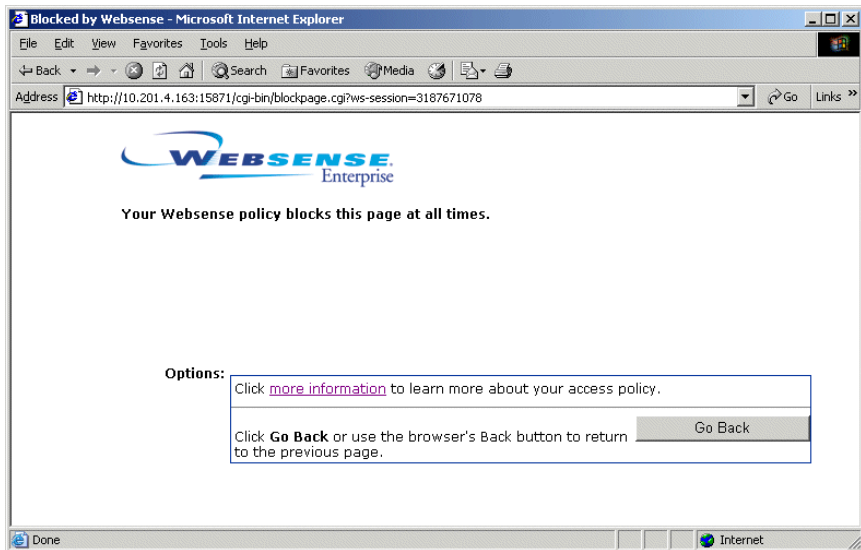
Block Messages

When Websense software blocks an internet site, it displays a block page in the client's browser. This page is comprised of two frames. By default, the top frame contains the block message, the requested URL, and the reason it was blocked.

The bottom frame always presents any options available to the user. For example, if the user has password override privileges, the bottom frame includes a password field. If the site is in a quota category, this frame presents quota information and options.



Default block message



more information page

Websense software provides default HTML files for the block pages. However, 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, you must set up the appropriate HTML files, and then configure Websense software to use them.

See *Customizing the Default Block Messages, page 59* for instructions on creating a new block message, customizing the default block message, and creating an alternate block message.

Customized Block Messages

Websense software provides the ability to modify certain portions of the default block messages, using a text editor. You can customize a block message in either of the following ways:

- ◆ Change the default message text displayed on an existing block message page.
- ◆ Create an entirely new block message page by choosing to display an alternate HTML file in the top message frame.



NOTE

If you are using Remote Filtering to manage clients outside the network firewall, you need to specify any new block page filenames in the **securewispproxy.ini** file (in the **\Websense\bin** directory by default). Contact Websense Technical Support for assistance.

When Websense software is first installed, block messages are stored in the Websense installation directory under **Websense\BlockPages\en\Default**. *Do not* modify any files in this directory. There is a separate directory provided for customized block message files: **Websense\BlockPages\en\Custom**. This directory is empty after initial installation.

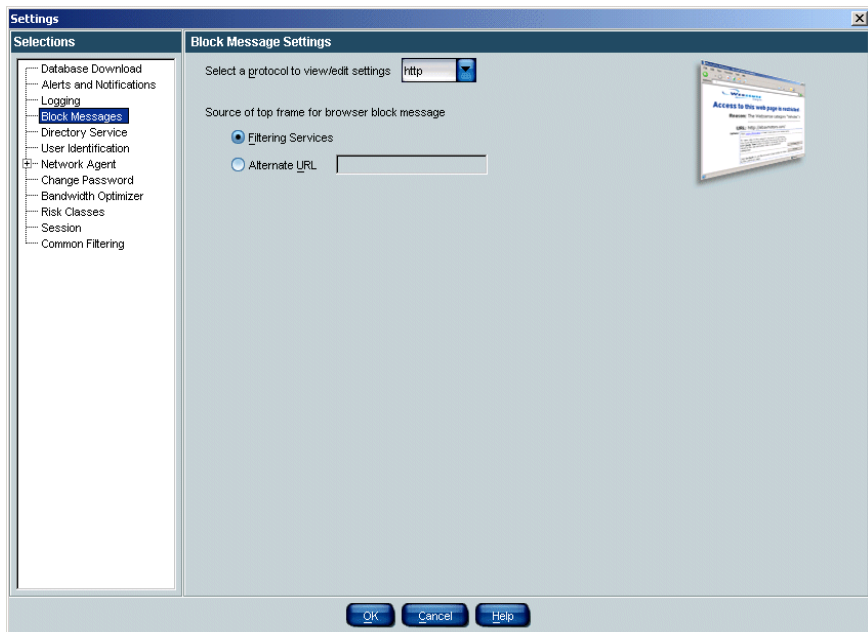
For example, to change the default block message text, you would *copy* the desired block message file from **Websense\BlockPages\en\Default** to **Websense\BlockPages\en\Custom**, and then use a text editor to modify the file as desired.



WARNING

Always use a plain text editor to edit block message files. Some HTML editors modify parts of the HTML code, which could corrupt the file and cause problems displaying a block message.

1. Create a new block page as desired by doing one of the following:
 - Customize the default message text by following the instructions in [Customizing the Default Block Messages](#), page 59.
 - Create an alternate HTML file to display in the top message frame, according to the instructions in [Creating an Alternate Block Message](#), page 64.
2. In Websense Manager, choose **Server > Settings**.
3. Select **Block Messages** at the left.



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 one of the following block message settings:

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 always 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 in the text box.

**NOTE**

Typically, alternate block messages are stored on an internal web server. If that cannot be done, store them on a web server that does not host a site in the Websense Master Database. Otherwise, the alternate block message will also be blocked whenever Websense software blocks its associated category.

7. Click **OK**.

Customizing the Default Block Messages

Websense Setup places the following default block message files into the **Websense\BlockPages\en\Default** directory:

- ◆ **block.html** – The text for the top frame of the block message. Indicates that access is restricted, the site that was requested and why it is restricted.
- ◆ **master.html** – The master frame that appears in the continue, quota and password override block messages.

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

This file invokes the following messages, which appear in the bottom frame of block messages as needed:

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.

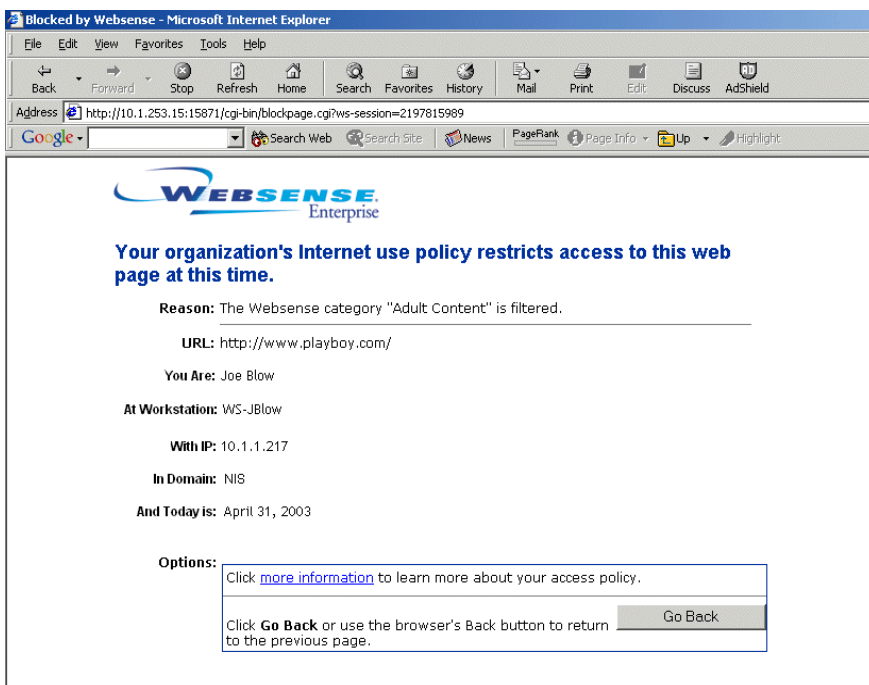
Websense software allows you to customize default block messages, maintaining filtering flexibility while presenting text more suitable to your organization.

For ease in customizing the content of your block messages, Websense software provides several variables for displaying information on the HTML 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)

Variable Name	Content Displayed
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)

An example of a block page that uses customized variables is shown:



Sample customized block message

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

```
<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
<code>ws_url</code>	Displays the requested URL
<code>ws_blockreason</code>	Displays why the site was blocked (i.e., which filtering setting is in effect)
<code>ws_pwoverridecgidata</code>	Populates an input field in the block page HTML code with information about use of the Password Override button
<code>ws_quota_cgidata</code>	Populates an input field in the block page HTML code with information about use of the Use Quota Time button
<code>ws_passwordoverrid_begin</code> , <code>ws_passwordoverrid_end</code>	Plays a role in telling Filtering Service whether to process a request using password override functionality
<code>ws_moreinfo</code>	Displays detailed information (shown after the more information link is clicked) about why the requested site was blocked
<code>ws_policyinfo</code>	Indicates which policy governs the requesting client
<code>ws_moreinfocgidata</code>	Sends data to Filtering Service about use of the more information link
<code>ws_quotatime</code>	Displays the amount of quota time remaining for the requesting client
<code>ws_quotaintervalttime</code>	Displays quota session length configured for the requesting client

Variable Name	Purpose
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
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 you want to customize to the **Websense\BlockPages\en\Custom** directory.

**IMPORTANT**

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**

Websense, Inc. does not recommend using an HTML editor to modify the block messages. Some HTML editors modify parts of the HTML code, which could corrupt the files and cause problems displaying the block messages.

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

DO NOT modify the tokens (enclosed by `$*` and `*$` symbols), or the general structure of the HTML code as it relates to tokens. These portions of the file 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 217 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 the **Websense\BlockPages\en\Default** directory.)
2. Restart Filtering Service (see [Stopping or Starting Websense Services](#), page 217).

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. This approach is often used to display corporate internet use policies, or to present a message that references that policy.

Alternate block messages are typically stored on an internal web server. If doing so 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 will be 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 in the **Websense\BlockPages\en\Default** directory to the **Websense\BlockPages\en\Custom** directory.
2. Open the **master.html** file using a text editor, such as Notepad or vi (not an HTML editor), and edit the following parameter, specifying the appropriate size.

```
<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.

3. If you are using Remote Filtering to manage clients outside the network firewall, specify any new block page filenames in the **securewisproxy.ini** file in the **Websense\bin** directory. Contact Websense Technical Support for assistance.

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

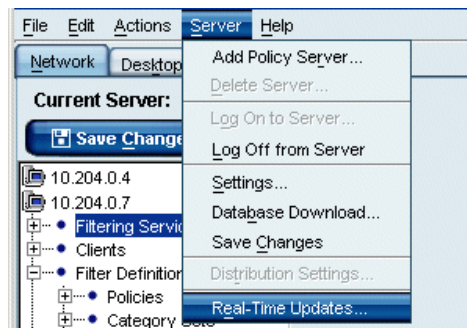
The Master Database can be downloaded in one of two ways:

- ◆ Enter your subscription key during installation, and choose to download the database automatically at that time.
- ◆ Enter your subscription key via **Server > Settings > Database Download** in Websense Manager. Filtering Service automatically contacts the database server and downloads the Master Database.

After the initial download, Websense software downloads changes to the Master Database according to the schedule you establish (see [page 67](#)). To download at any other time, choose **Server > Database Download** in Websense Manager.

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, choose **Server > Real-Time Updates**.



Real-Time Updates menu command

The status bar at the bottom of the Websense Manager window indicates when the Master Database is updated or when new information is available. By default, the status bar appears as shown.



Status bar in Websense Manager

Clicking the **MyWebsense** link at the right opens the MyWebsense web page (<http://www.mywebsense.com>).

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 *Configuring Download Via Proxy*, page 218 for instructions.

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.

For information about download status for subsequent Filtering Services, check the appropriate log, using these instructions.

- ◆ *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, choose **Start > Programs > Administrative Tools > Event Viewer**. From the **Log** menu, choose **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, choose **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 elect to be notified whenever a Websense Master Database download fails. See *Alerting*, page 227 for instructions.

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.

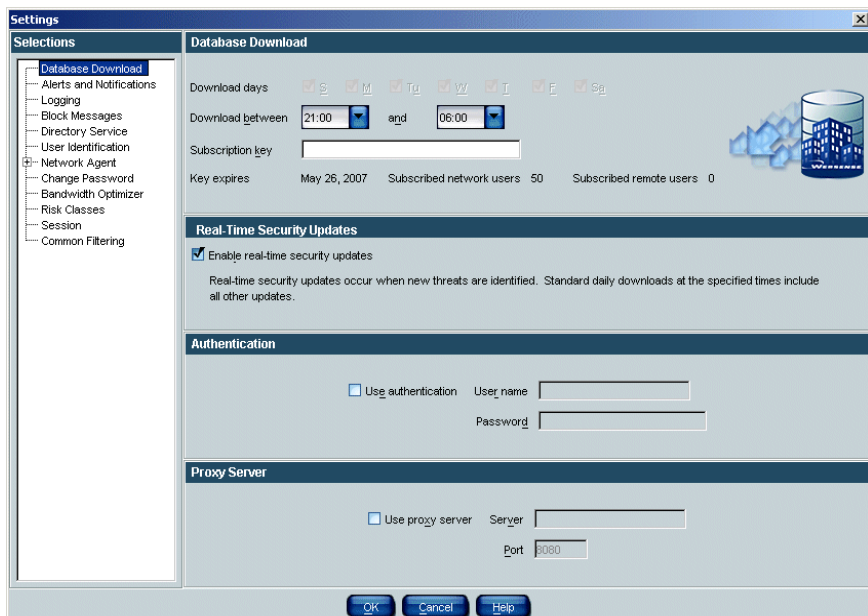


IMPORTANT

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

To change the schedule:

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



Download settings

3. Configure download behavior as desired.



NOTE

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

Available settings are:

- **Download days:** Check the days of the week to update your copy of the Master Database. Downloading daily ensures the fastest download time and the most up-to-date version of the Master Database.
- **Download between:** Select a start time and end time to define the period during which Websense software downloads the Master Database. Filtering Service selects a random time during this period to contact the Master Database server. If Filtering Service is unable to contact the server, it retries at intervals until the end time is reached. You can configure Websense software to notify you if download fails (see [Alerting](#), page 227).
- **Subscription key:** Enter your subscription key as it appears in the key document (the key is not case-sensitive). Websense software cannot download the Master Database until you enter a valid subscription key.
- **Key expires** and **Subscribed users:** These are display-only calculations based on your subscription key. You can block all sites or permit all sites if the subscription expires (see [Subscriptions](#), page 17). Contact Websense, Inc. to renew your subscription before the expiration date to avoid any loss of service. See [page 39](#) for more information.

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 will resume 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 will attempt 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 timeframe of the failed download, Filtering Service will still contact the database download server to attempt download again.



NOTE

You can click **Download All** at any time to resume a database download.

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 the basis for internet content filtering by protocol type.

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

Categories have been broken down to allow organizations better control in adjusting the level of access they want to give their users. In case of uncertainty, a collaborative decision is made as to whether a site is included, and in what category it is placed. Additionally, the Master database is checked regularly for accuracy and quality.

The categories used by Websense, Inc. have been 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:

<http://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:

<http://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:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php>

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

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

<http://www.websense.com/global/en/ProductsServices/MasterDatabase>.

Websense Security Protocol Groups

If you have *Websense Web Security Suite*, you automatically 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 about the Security Protocol Groups, go to:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php>

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. See *Alerting*, page 227 for information on setting up alerting.

Websense Real-Time Security Updates

The Websense Real-time Security Update feature is the optional 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. Automatically 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 74) and Websense Enterprise Client Policy Manager (see your Client Policy Manager documentation).

The Websense Filtering Service queries the database download server every five 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.

Special Events

The Websense Master Database contains a Special Events category, created especially for the purpose of controlling employee access to sites covering “hot” topics. Sites in the Special Events category are automatically added to the Master Database during scheduled download times. They are kept in the Special Events category 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.

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 319). Websense software then filters the sites you define as soon as you click the **Save Changes** button in Websense Manager.

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

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php>

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

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™ - primarily focuses on preventing cyberslacking.
- ◆ Websense Enterprise Bandwidth PG™ - primarily focuses on saving bandwidth.
- ◆ Websense Enterprise Security PG™ - focuses on internet sites containing malicious code, which can bypass virus-detection software programs.

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

<http://www.websense.com/global/en/ProductsServices/Modules/PremiumGroups.php>

There is an additional cost for Premium Groups. When purchased, they are delivered through the existing database download process. The filtering option for Premium Groups is set to **Permit** by default, and cannot be changed until purchased. Customers can report on all requests to these categories, but until purchased, display **[monitor only]** next to their names in category lists.

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:

<http://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.

<http://www.websense.com/products/index.cfm>

Protocol Domain Path

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

Following is an example of two URLs that share the same domain but fall into different categories.

<http://www.cnn.com/WORLD> (News and Media)

<http://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 adds flexibility to site filtering, allowing you to specify general patterns for Filtering Service to match, as opposed to specific URLs or strings.

See *Chapter 9 Setting Up Web Filtering* for instructions on creating custom URLs, yes lists or keywords.

**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%.

As of version 6.2, Websense software supports the common sets of Perl, Javascript and Posix regular expression libraries for URL pattern matching.

For further help on using regular expressions, see the following websites:

http://en.wikipedia.org/wiki/Regular_expression

<http://www.regular-expressions.info/>

<http://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

<http://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 will have 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 one 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 three 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. Uses for CGI scripts include search engine request forms and image maps that contain links to other internet sites. When a user enters a search engine request or clicks on an image map, the CGI script automatically generates a new URL request.

The following 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, called the CGI string, 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 previous example, 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>

To provide additional filtering for sites requested via CGI, you can block keywords in CGI strings appended to URLs (see *Keywords*, page 331).

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 in graphical or tabular format.

**NOTE**

Websense software sends log information that can only be read by the corresponding version of Websense Enterprise Reporter. Install or upgrade Reporter as appropriate in order to generate reports. See your Reporting documentation for instructions.

Log entries contain the following information:

- ◆ 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.

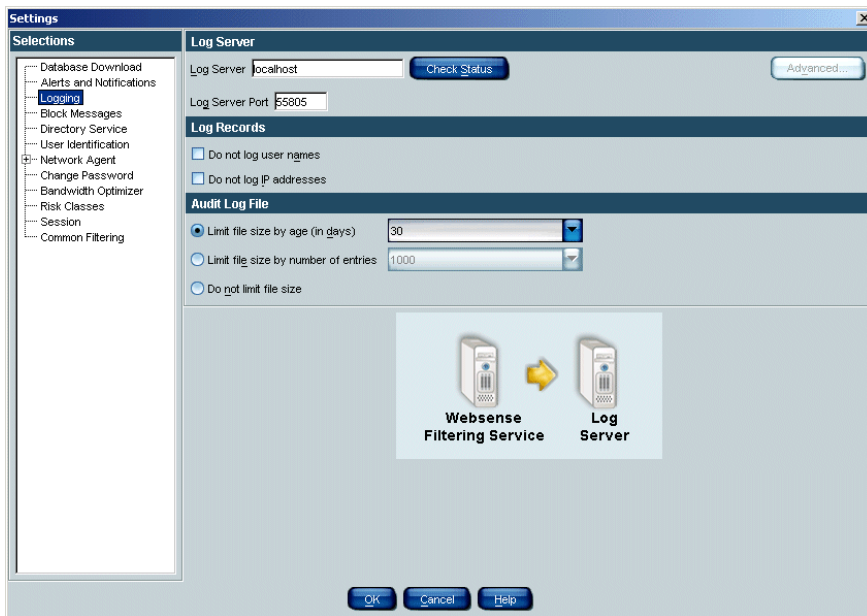
Although Log Server must be installed in the same network as other Websense components, most organizations run it on a separate machine to optimize performance.

**NOTE**

No logging can occur until Log Server is installed and the appropriate information is entered via **Server > Settings > Logging**.

To configure logging:

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Logging** at the left. The **Logging** settings are displayed.
3. Specify Log Server settings, as indicated.



Logging settings

- ◆ **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 left blank, logging will be disabled.



NOTE

Machine names containing certain 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, choose **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 that Websense software must use to communicate with Log Server. The default port is 55805.
- ◆ **Check Status:** Use this button to determine whether the Websense Filtering Service can successfully connect to the IP address and port specified for Log Server.
- ◆ **Do not log user names:** Check this box to omit user names from report output. This preserves anonymity in internet usage reporting.
- ◆ **Do not log IP addresses:** Check this box to omit IP addresses from report output.

Websense software is configured to log user internet activity.

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:

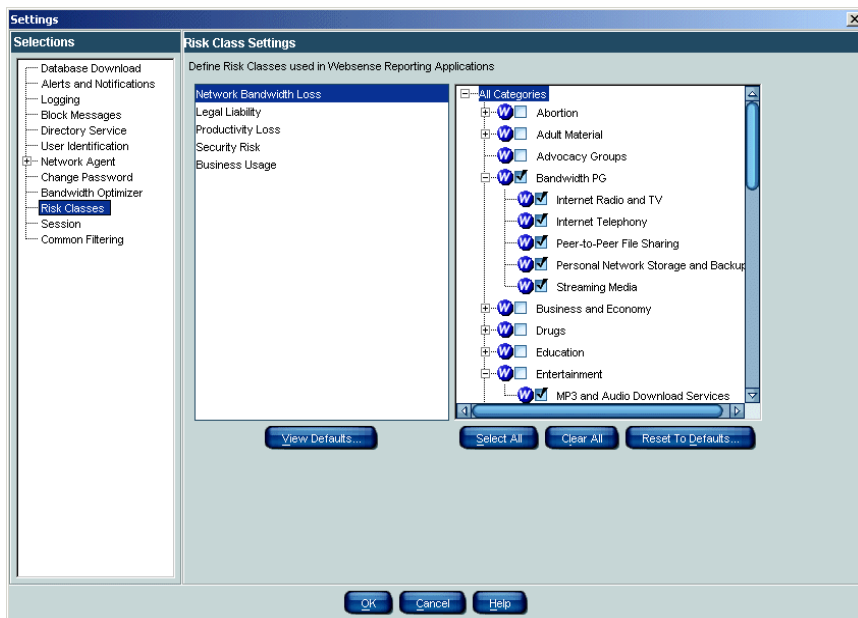
- ◆ **Network Bandwidth Loss**
- ◆ **Legal Liability**
- ◆ **Security Risk**
- ◆ **Productivity loss**
- ◆ **Business Usage**
- ◆ **Miscellaneous**

See the *Websense Enterprise Reporting User's Guide* for examples of internet usage reporting based on risk class.

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

To modify the predefined Websense risk classes:

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Risk Classes** at the left. The risk class settings are displayed.



Risk Classes settings

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 for the chosen risk class to those provided by the Websense software.
4. Click **OK**.

Your risk class modifications will be applied in reporting.

Network Agent

Network Agent enables several Websense functions, described in this chapter. In most cases, Network Agent operates behind-the-scenes to provide a complete internet filtering solution, according to configuration settings in Websense Manager. How Network Agent handles internet content is described in *Filtering Internet Content*, page 99.

Network Agent is involved in the following Websense functions:

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

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.

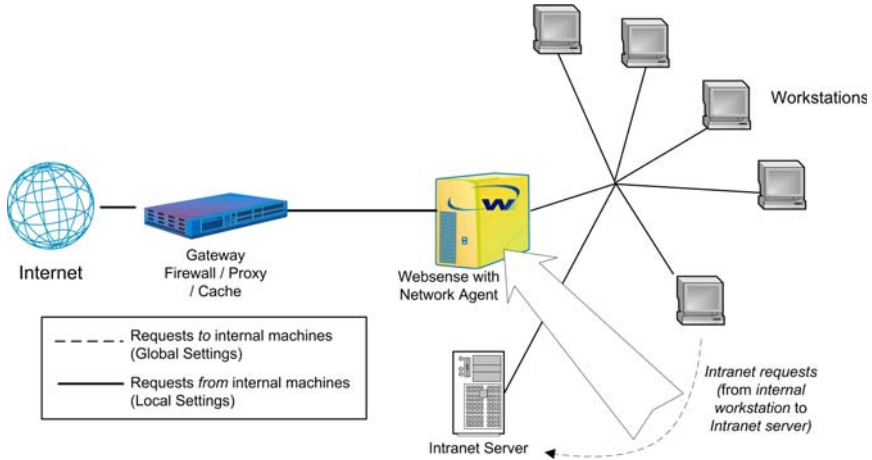
By default, Network Agent also provides bandwidth usage data to Policy Server, and filtering log data to Filtering Service.

Network Agent sees all traffic in your network. The Agent distinguishes two types of requests:

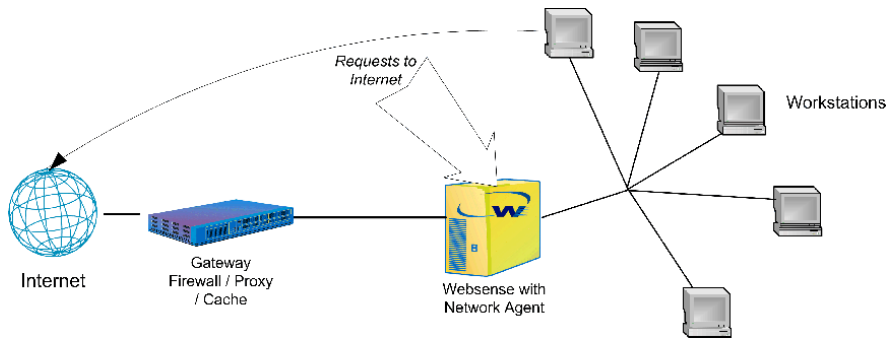
- ◆ requests sent from internal machines to internal machines (hits to an intranet server, for example)
- ◆ requests sent from internal machines to external machines such as web servers (user internet requests, for example)

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

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 and/or destinations.



Monitoring requests to internal machines



Monitoring requests from internal machines

Configure global and local settings for Network Agent via Websense Manager. Configuration instructions begin on [page 85](#).

Installation

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

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

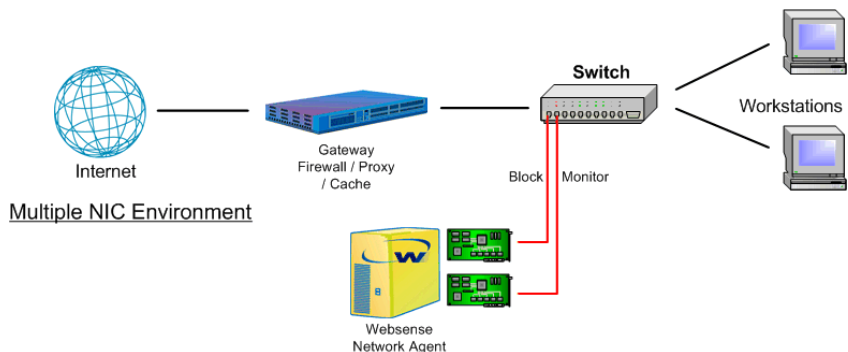
<http://www.websense.com/global/en/SupportAndKB/ProductDocumentation/?Section=All>

Initial Configuration

After you have installed Network Agent, you need to 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

You can have one or more instances of Network Agent monitoring traffic. Each Network Agent instance must use at least one designated network interface card (NIC). You might also have Network Agent on a machine with multiple NICs. In the example shown, Network Agent uses one NIC for monitoring traffic, and another to send blocking information to client machines.



Network Agent on a dual-NIC machine

Generally, the number of NICs required by the Network Agent machine depends on:

- ◆ The hardware resource configuration of the Network Agent machine;
- ◆ The type of device (switch or hub) to which Network Agent is connected.



IMPORTANT

The number of NICs required can depend on a variety of factors, such as the software running on client machines, and how filtering policies are configured. See the *Websense Enterprise Deployment Guide* for recommendations on where to place Network Agent and how to ensure it best captures your network traffic.

The NICs Network Agent uses for monitoring must be able to see all traffic outbound from your network. Typically, this means the Network Agent machine is connected to the device closest to the internet gateway.

If this device is a switch, it must support port spanning (also known as port mirroring or switch mirroring). This means ports on the switch are mirrored so traffic on monitored ports is simultaneously sent to the monitoring port to which Network Agent is connected.

Websense, Inc. strongly recommends using a switch that supports bi-directional spanning. If such a switch is used, Network Agent can function successfully with a single NIC performing both monitoring and blocking. If the switch does not support bi-directional spanning, Network Agent must use separate NICs for monitoring and blocking.

If this device is a dumb hub (which distributes traffic from the up-linked port to all other ports), Network Agent requires only one NIC for both monitoring and blocking.

Initially, you select which NIC Network Agent uses during installation. You can change a NIC associated with Network Agent - for example, if your network includes multiple Network Agents and/or multiple Filtering Services.

If you do add a new NIC on the Network Agent machine, you must restart the Network Agent service, and then configure the new NIC via Websense Manager (according to the procedure in this section).

**NOTE**

If you are unsure whether the NIC used by Network Agent can see traffic in the appropriate network segment, use the Traffic Visibility Tool provided. To start the tool, choose **Start > Programs > Websense > Utilities > Traffic Visibility Tool**. For usage instructions, refer to the *Initial Setup* chapter of your installation guide.

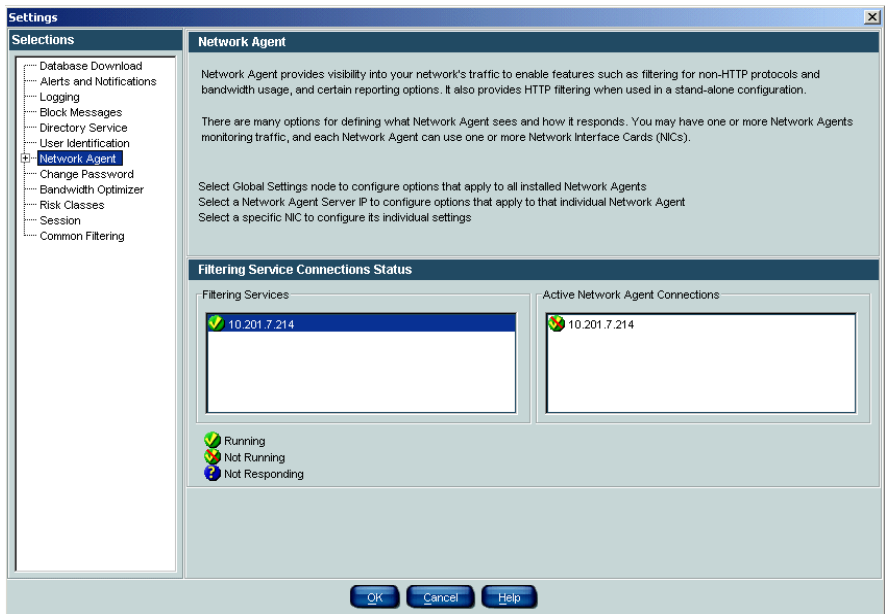
Configuring the Agent

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 one instance of Network Agent is connected.

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.

Modify Filtering Service connections via the Network Agent local settings (see *Local Settings*, page 93).



Main Network Agent settings panel

To configure Network Agent:

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

**IMPORTANT**

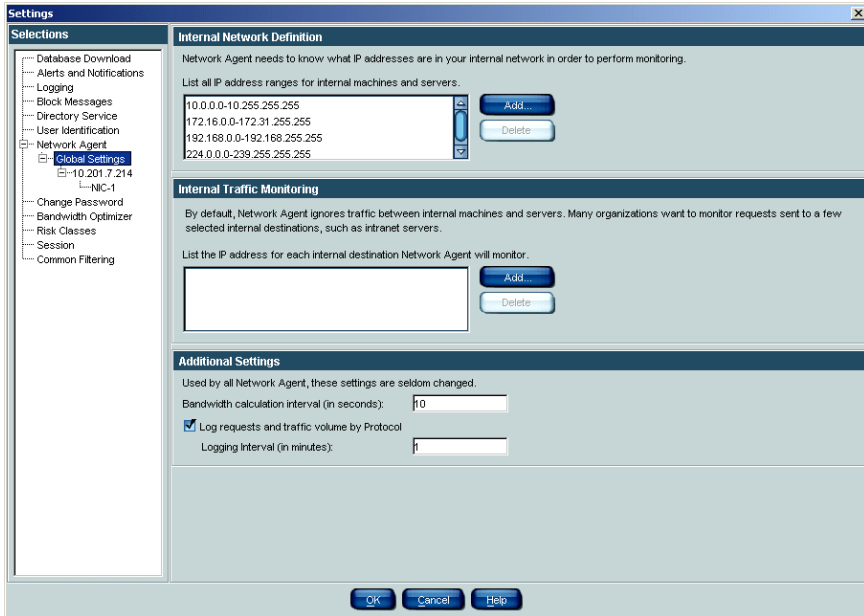
If at any time you change the IP address of a machine running Network Agent or any Websense component, be sure to follow the guidelines in [Changing an IP Address, page 222](#) to ensure uninterrupted filtering.

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, you must tell Network Agent to monitor the internal machines involved. (See [Instant Messaging Attachment Manager, page 346](#) for more information.)

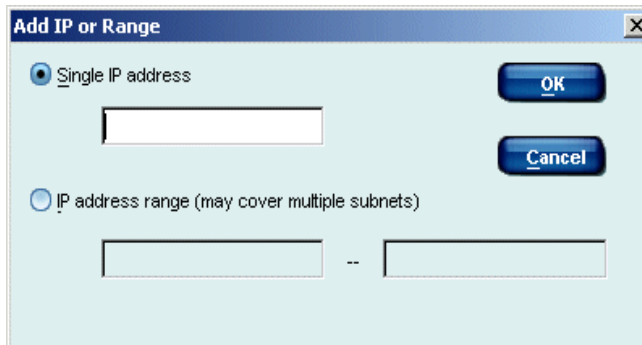


Network Agent global settings panel

- ◆ **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**.



ENTERING IP ADDRESS RANGES

An IP address range should span only one subnet or network segment. Ranges spanning multiple subnets may be problematic, because in many configurations Network Agent only sees internet traffic from machines in its own subnet. For example, 10.203.0.0 - 10.203.255.255 is a valid IP address range, while 10.1.2.3 - 255.255.255.255 (encompassing multiple subnets) is considered invalid.

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 will monitor 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 enter the IP addresses of the internal machines involved here. (See *Instant Messaging Attachment Manager*, page 346 for more information.)

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/or 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. See [page 347](#) for more information.
 - **Log requests and traffic volume by protocol:** Accept the default interval (**1** minute), or specify a different interval (at least 1 minute). *Uncheck* this box to prevent Network Agent from tracking protocol request data.

When this option is selected, Network Agent provides the number of requests by protocol, and traffic volume by protocol, to Log Server.

Local Settings

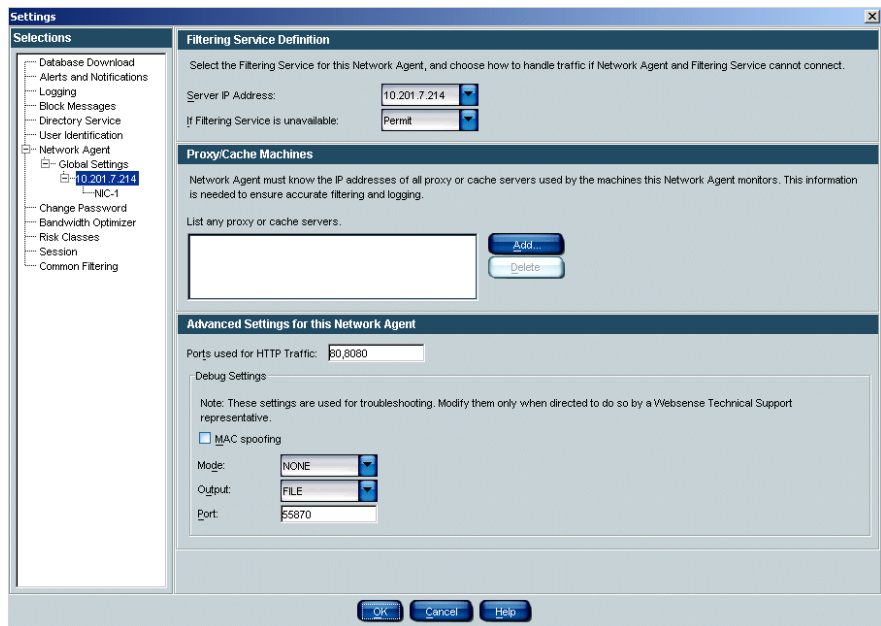
These determine the functions performed by each particular Network Agent. By default, Network Agent monitors requests from all internal machines it sees. Websense software filters internet content requested from these machines. Machine names are tracked in log data and Real-Time Analyzer output.

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, you must configure one at a time.



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.



IMPORTANT

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 user requests will not be filtered or logged.

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.



WEB SECURITY SUITE CUSTOMERS ONLY

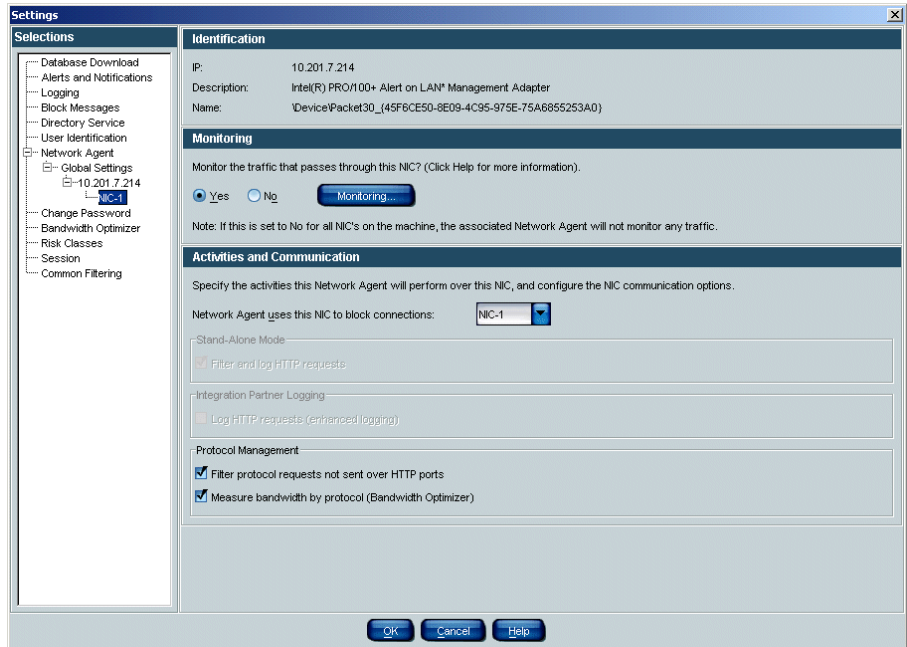
Network Agent is automatically configured to scan all ports for HTTP traffic. This protects against HTTP servers set up for spyware or phishing that use non-standard HTTP ports in order to avoid detection.

- ◆ **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.



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 one 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.



IMPORTANT

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 you want Network Agent to 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 (see [page 363](#)).

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 one 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, refer to 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 will perform 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. See [Managing HTTP Traffic, page 100](#) for details.

- **Log HTTP requests (enhanced logging):** Network Agent will log requests, but will 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.
 - Selecting **Filter protocol requests not sent over HTTP ports (Protocol Management)** activates the Protocol Management feature (see [Managing Protocols, page 337](#)).
 - Selecting **Measure bandwidth by protocol (Bandwidth Optimizer)** activates the Bandwidth Optimizer feature. Network Agent will use this NIC to track network bandwidth usage by each protocol or application (see [Bandwidth Management, page 347](#)).



IMPORTANT

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

Filtering Internet Content

Websense software enables you to block internet content that is:

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

This section provides an overview of enhanced internet filtering options provided by Network Agent. For instructions on configuring protocol-based filtering, see *Managing Protocols*, page 337.

Network Agent can be used in conjunction with a proxy server, firewall, or cache product that is integrated with Websense software. In a typical scenario, 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/block filtering options for HTTPS and FTP content.



FTP REQUESTS

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.

By default, Network Agent is set to filter internet content according to the **Global** policy. See your installation guide for Network Agent installation and setup instructions. See [Managing Protocols, page 337](#) for information on configuring how Network Agent monitors internet traffic.



NOTE

When Filtering Service is down, users are permitted 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 93](#)).

Managing HTTP Traffic

By default, Network Agent is configured to scan 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, choose **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**.



WEB SECURITY SUITE EDITIONS ONLY

Network Agent is configured automatically to scan 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 provides several existing protocol definitions; you can edit or create policies to enforce filtering of these protocols. For a complete list of protocols provided, see:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/>

If desired, you can create additional protocol definitions. However, protocol definitions are not used in filtering until you configure a policy to manage those protocols. See *Creating a Custom Protocol*, page 352 for information about adding protocol definitions to Websense software.

Network Agent also allows Websense software to manage usage of applications like AOL instant messaging and various media players.

For information about managing protocols, including instructions on configuring protocol definitions and protocol-based filtering, see *Managing Protocols*, page 337.

Blocking Ports, IP Addresses and Signatures

The filtering capability Network Agent provides allows Websense software to block internet content transmitted over particular ports or IP addresses, or marked by particular signatures, regardless of the nature of data being transmitted. For example, you can configure Websense software to block all content entering your network over port NN.

Protocol definitions are housed in Websense Manager. View which ports are assigned to a protocol, or create new port number or IP address assignments. For detailed instructions on viewing or changing port numbers for protocols, see *Managing Protocols*, page 337.

Protocol Usage

In order 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. will 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:

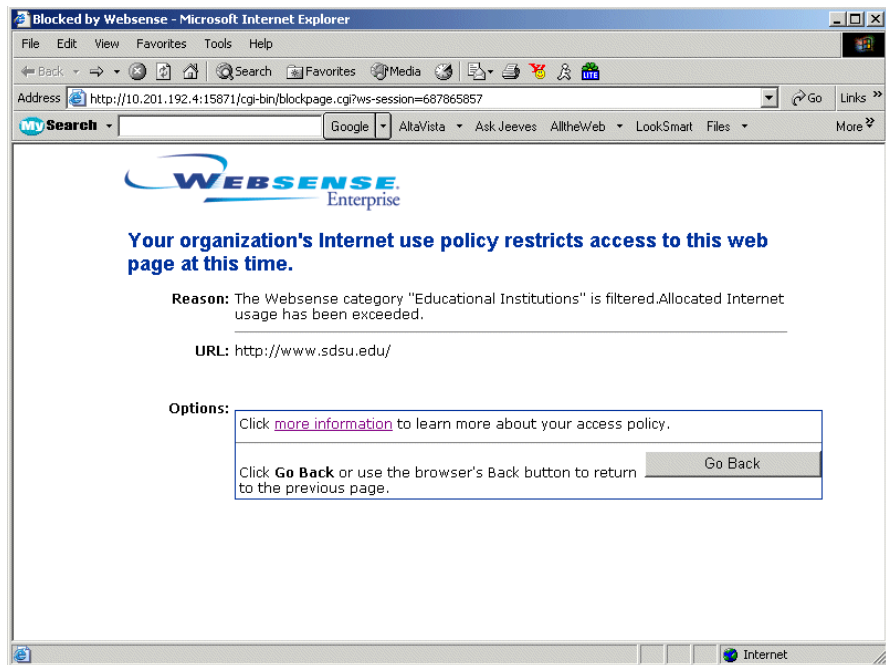
1. In Websense Manager, choose **Server > Settings**.
2. Go to the **Common Filtering** panel.
3. Uncheck **Allow Websense to gather protocol usage data**.

Measuring Network Bandwidth

Websense Enterprise® Bandwidth Optimizer is an optional feature available for purchase with Websense software. This feature provides the ability to limit internet access within your organization based on bandwidth availability. Network Agent is the component that enables “threshold” filtering, or filtering of particular types of internet content based on available network bandwidth.

Websense software can filter internet sites, protocols or applications based on bandwidth usage. Filtering policies let you limit access to sites, protocols or applications based on bandwidth limitations you specify.

When a request is blocked based on bandwidth limitations, the Websense block page displays this information in the **Reason** field, as shown.



Block page resulting from a bandwidth filtering restriction

The default limits for available network bandwidth serve as the basis for bandwidth-based filtering settings. You can use these default values, or you can change them according to your needs. For instructions on changing the default bandwidth limits, see [page 348](#).

When bandwidth limitations are activated, Network Agent sends network bandwidth data to Filtering Service at a predetermined interval by default. Websense, Inc. does not recommend changing this interval. The default interval ensures that Websense software accurately monitors bandwidth usage, and receives measurements that are closest to an average. (A longer measurement interval might result in some very high, and some very low measurements. With a shorter interval, bandwidth “peaks” caused by application startup could create falsely high overall bandwidth usage measurements.)

Filtering Protocols

You can block content provided by a particular protocol based on total network bandwidth usage, or bandwidth usage associated with that protocol. For example, you can 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.

See [page 357](#) for instructions on setting bandwidth limitations for protocols. See [Filtering Policies, page 277](#) for how to configure a policy to filter particular protocols.

Filtering Internet Sites

You can filter internet content based on bandwidth usage associated with the URL categories governed by a filtering policy. For example, you could have a policy that blocks the sites in its category set if total network bandwidth usage exceeds 50% of available network bandwidth.

Alternatively, you can apply bandwidth limitations to a URL category based on overall network HTTP bandwidth usage. For example, you could 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.

See [Editing a Category Set, page 314](#) for more information about filtering HTTP internet requests based on bandwidth usage.



NOTE

When bandwidth-based filtering options are activated, 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.

Initially, Websense software either filters or monitors all clients in the same manner, depending on the **Initial Filtering** setting established during installation (see your installation guide). If you selected **Filter Internet traffic based on a predefined policy**, Filtering Service applies the **Global** policy to all clients. If you selected **Monitor Internet traffic only**, Filtering Service only logs clients' requests, but does not filter 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 283). The Websense Policy Server enforces only one policy per internet request.

When multiple policies apply, such as when separate policies have been assigned to the user and the machine being used, Policy Server uses the following criteria to determine which policy to enforce:

1. Apply the policy assigned to the specific user making the request, if one exists. If that policy has no category set scheduled at the time of the request, the next applicable policy is enforced.
2. If there is no user-specific policy, or the policy has no active category set at the time of the request, Policy Server looks 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, Policy Server looks for a policy assigned to any group to which the user belongs. (If the user belongs to more than one group, see [page 41](#) for information about what happens when multiple group policies apply.)
4. If no group-specific policy is found, or the policy has no category set assigned at the time of the request, the **Global** policy is enforced by default.
5. If no category set or protocol set is scheduled in the **Global** policy at the time of the request, the **Default Settings** category set or protocol set is automatically enforced.

Adding Directory Objects

Add directory objects to Websense Manager when you want to assign them distinct filtering policies. Any user who is *not* added is filtered by the policy for the group he or she belongs to (if the group has been added), a workstation or network policy (if applicable), or the **Global** policy. In order 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.

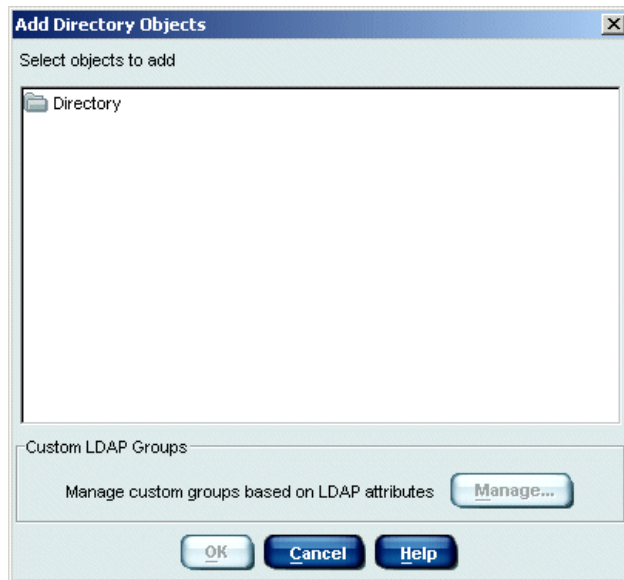


NOTE

If you plan to change to a different directory service, implement that change before adding directory objects. Otherwise, directory objects will have to be re-added after the change.

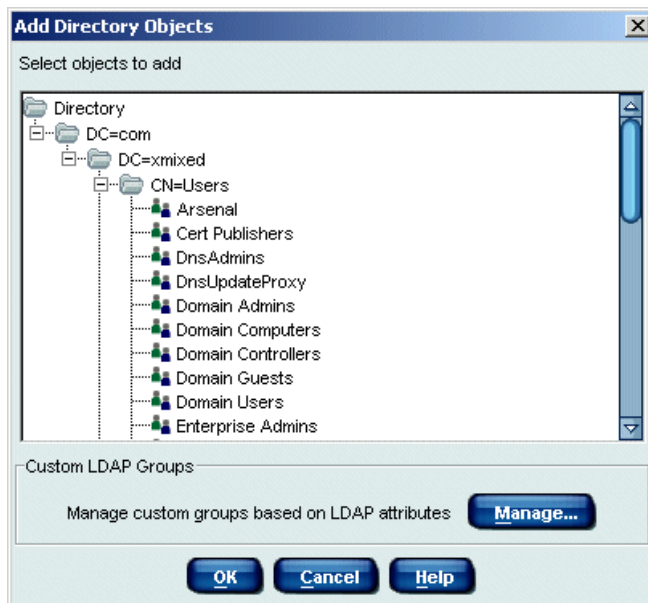
To add a directory object, follow these steps.

1. Right-click in the Websense Manager navigation tree, and then choose **Add Directory Objects**.
2. The **Add Directory Objects** dialog box appears.



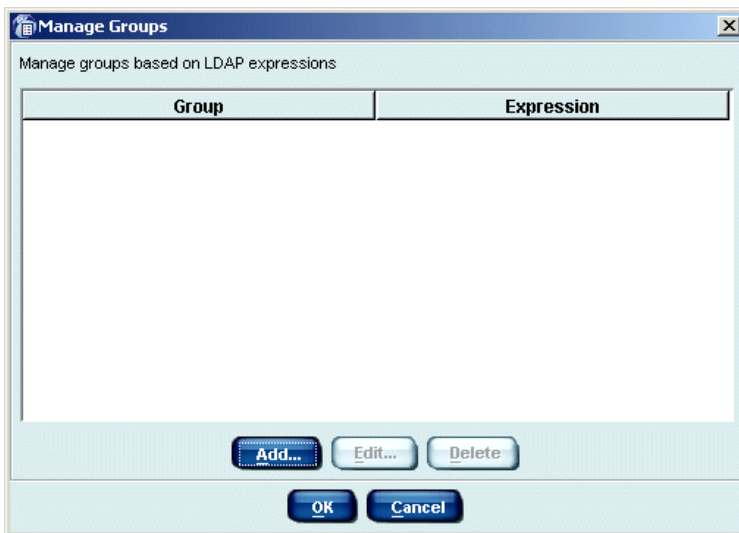
Add Directory Objects dialog box

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 dialog box

5. Select the object to be added 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](#).

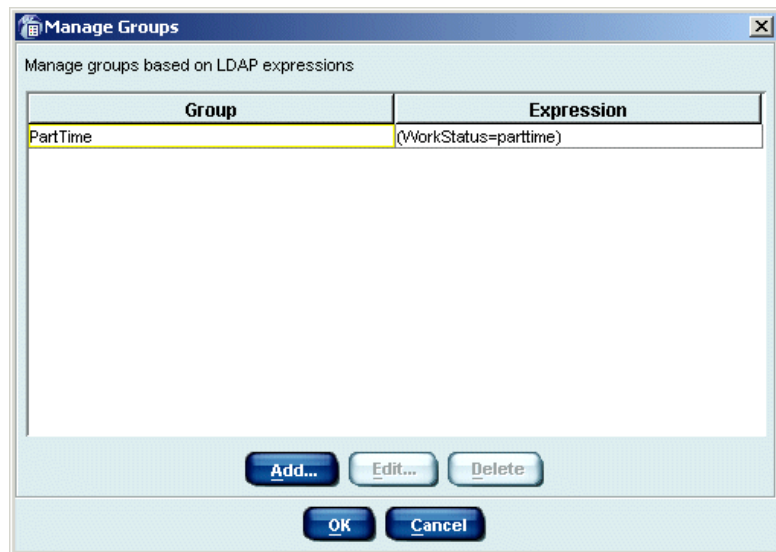


Manage Custom LDAP Groups dialog box

- 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.
- Enter a name for the group. Group names are case-sensitive.
- Enter the expression that defines this group in your directory service. For example:

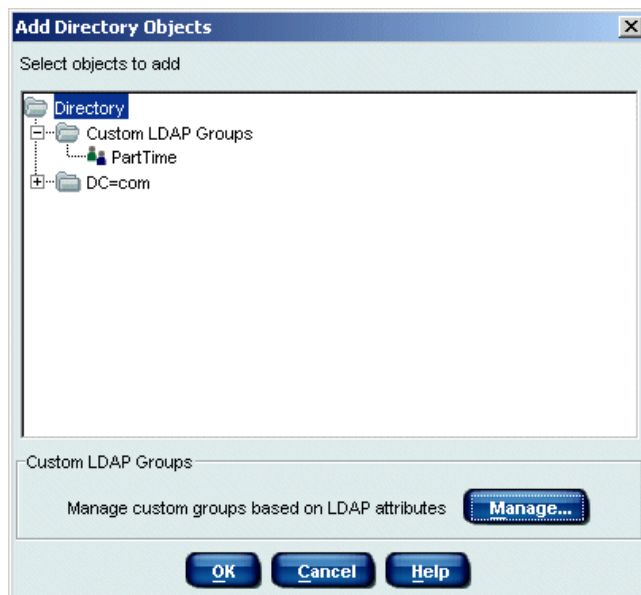
```
(WorkStatus=parttime)
```

where `WorkStatus` is a user attribute that indicates employment status, and `parttime` is a value indicating that the user is a part-time employee.
- Click **OK**. The new group appears in the **Manage Custom LDAP Groups** dialog box, next to its defining expression.



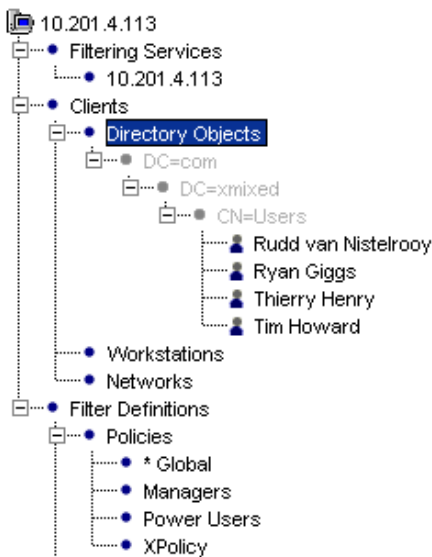
Manage Custom LDAP Groups dialog box with new group specified

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 you have finished adding user and group objects to Websense Manager, click **OK**.
13. To view users in the navigation tree, expand **Directory**, then the user's domain/context.



Users in the navigation tree

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



NOTE

For Websense software to properly filter internet requests from specific users, you may need to enable Websense manual authentication so that if Websense software is not able to identify users transparently, it can prompt users for directory authentication. See [Directory Service Access](#), page 187 to make this determination.

Requests continue to be filtered by the **Global** policy until another policy is assigned.

To assign a new policy to a user or group, select the user or group in the navigation tree, and then select a policy from the policy list. See [page 283](#) for details on assigning policies.

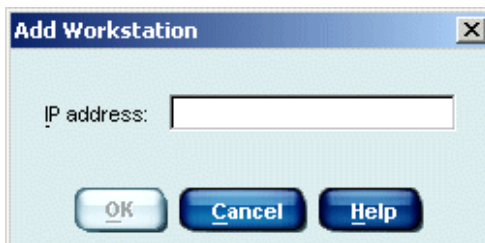
You can grant users password override privileges to allow them access to sites that would otherwise be blocked. For password override options, see [page 115](#).

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 more than one person during the day.

Workstations are identified by IP address.

1. Right-click in the Websense Manager navigation tree, and then choose **Add Workstation**.
2. The **Add Workstation** dialog box appears.
3. Enter the **IP address** of the workstation you want to add. (To add multiple workstations at once, click **Cancel** and then choose **Add Network**. See the next section for details.)



Add Workstation dialog box

4. Click **OK**. The IP address of the workstation appears in the navigation tree under **Workstations**.
5. The workstation continues to be filtered by the **Global** policy until another policy is assigned to it. You can assign a different policy at any time by selecting its IP address under **Workstations** in the navigation tree, and then selecting a different policy from the list (see [page 283](#)).

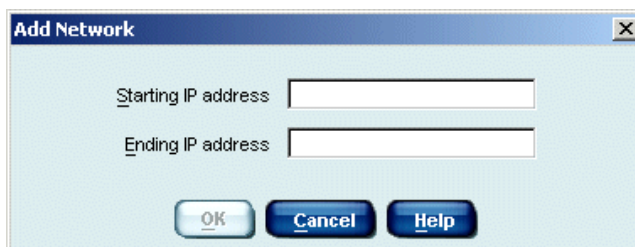
6. Click **Save Changes** above the navigation tree.

Once a workstation is added, you can assign password override privileges to it, and give the password to the appropriate users. This enables authorized users to access sites that would otherwise be blocked on that workstation. See [page 115](#) for details.

Adding Networks

Networks allow you to 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 choose **Add Network**.
2. The **Add Network** dialog box appears.
3. Enter the **Starting IP address** and **Ending IP address** of the workstations you want to add as a network.



Add Network dialog box

4. Click **OK**. The network appears in the navigation tree under **Clients > Networks**.
5. The network is filtered by the **Global** policy until another policy is assigned to it. To assign a different policy at any time, select its IP address under **Networks** in the navigation tree, and then select a different policy from the list (see [page 283](#)).
6. Click **Save Changes** above the navigation tree.

Deleting Clients

If a directory object, workstation, or network becomes obsolete, you can delete it from Websense Manager. This removes the client from the navigation tree, and removes any related policy assignments.

1. Right-click the appropriate client in the navigation tree.
2. Choose **Delete** from the shortcut menu.
3. Click **Yes** when prompted to confirm the delete request.

If you remove a client that still exists on the network, it will revert to being filtered by the **Global** policy.

Password Override

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

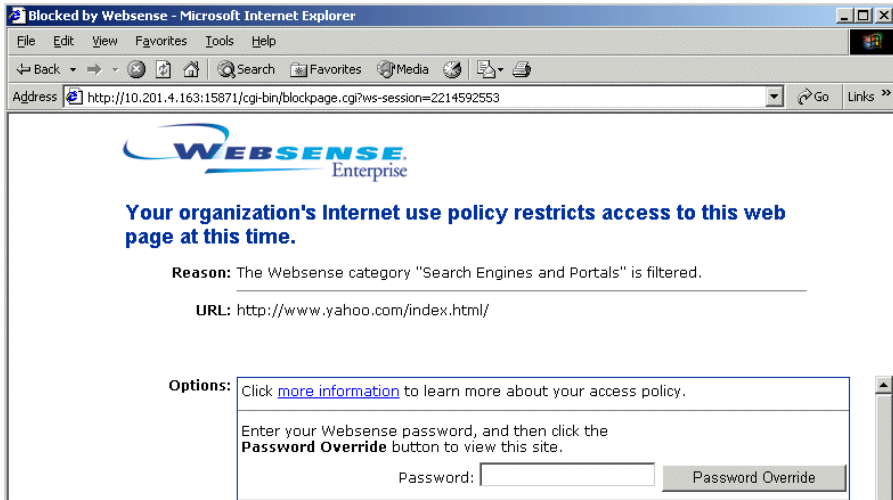
When password override is activated, the Websense block message includes a password field. If a valid password is entered, Websense software permits free access to any blocked site for a limited amount of time.



NOTE

Password override can be used when clients (users, groups, workstations, and networks) 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 a Websense block page, as shown.



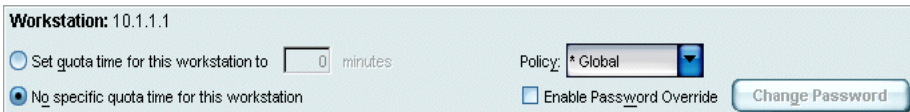
Block page allowing password override

Enabling Password Override

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

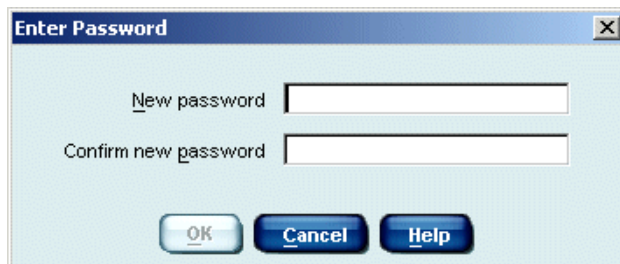
When the override period expires, the password must be entered again for access to additional blocked sites.

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.



Client information

4. Check **Enable Password Override**. The **Enter Password** dialog box appears.



Enter Password dialog box

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 the **Change Password** button in the content pane. The **Enter Password** dialog box appears.
3. Enter a new password for this directory object, workstation, or network. Confirm the spelling by entering it again in the **Confirm new password** field.
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

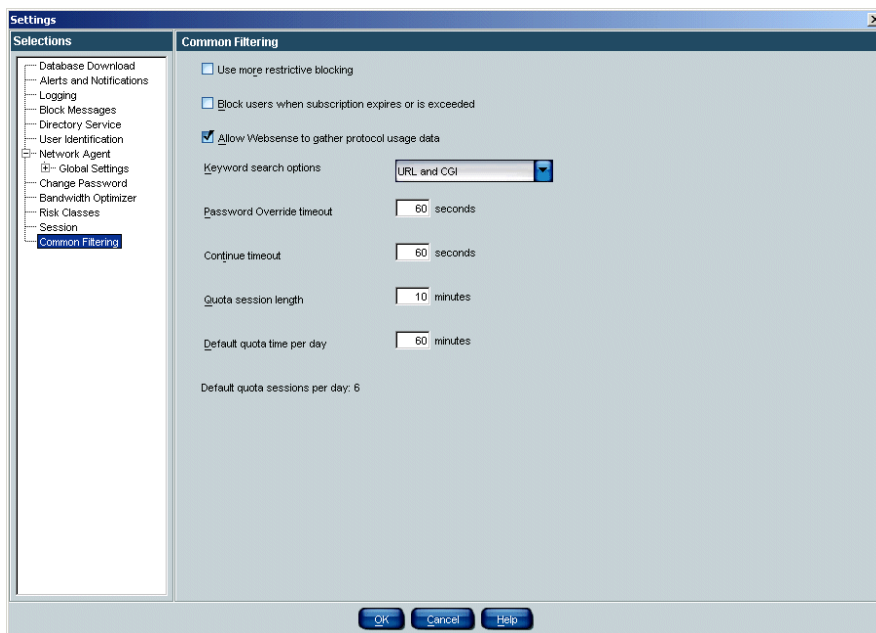
Quota time can be allocated to employees in two different ways:

- ◆ 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. In Websense Manager, choose **Server > Settings** to open the **Settings** dialog box.
2. Select **Common Filtering** at the left.



Common Filtering settings

3. For **Quota session length**, enter the desired number of minutes for a quota session. (Ten minutes is the default time period, and allows employees a short amount of time to take care of personal business.)

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 quota time period.
5. Click **OK**.

Quota Time Allocated to Specific Clients

Quota time can be allocated to individual clients by following these instructions.

1. Add to Websense Manager the user, group, workstation, or network to which you want to allocate quota time by following the instructions on [page 107](#).



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 you want to allocate quota time. The settings for the selected client appear in the content pane.
3. Select **Set quota time for this user to...minutes**.
4. Enter the desired number of minutes (0-240) of quota time.

Client information

5. Click **Save Changes** above the navigation tree.
6. Change the filtering option on selected categories to **Limit by Quota**, if you have not already done so. See [page 314](#) for instructions.

The selected clients are allocated a unique amount of quota time.

Filtering Remote Clients

Using the Remote Filtering feature, you can 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. Your installation guide provides instructions for installing these components.



NOTE

Install only one primary Remote Filtering Server instance per Filtering Service. See the *Websense Enterprise Deployment Guide* for information about this and other setup requirements.

For remote clients, Websense software filters HTTP traffic only. The Websense Remote Filtering Server automatically 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.



IMPORTANT

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 85](#) for Network Agent configuration instructions.

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 [Bandwidth Management, page 347](#)).

If you have implemented Remote Filtering and are using customized Websense block pages, you need to specify any new block page filenames in the **securewispproxy.ini** file (in the **/Websense/bin** directory by default). Contact Websense Technical Support for assistance. See [Customized Block Messages, page 56](#) for information on customizing block pages.

Virtual Private Network (VPN) Connections

If your organization's 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 will not be 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. See your Reporting documentation for more information about Delegated Reporting.

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 will 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 will be applied to the remote user.

For more information about transparent identification of users, see [Transparent Identification](#), page 125.

Manual Authentication and Remote Clients

Manual authentication (see [Manual Authentication](#), page 208) is supported for remote clients. If the **Prompt user for directory authentication** setting (**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.

User Identification

Policy-based filtering allows you to define individual filtering plans for different members of your organization. In any environment, you can 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 allows you to 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.

To filter internet requests based on policies assigned to directory objects, Websense software must be able to identify a user making a request, given the IP address where the request originated. There are various ways to do this.

- ◆ Websense software receives user identification information from your integrated product if it offers an authentication method. See your installation guide for whether your integration product supports authentication.
- ◆ Websense software can identify the user transparently, if your network uses a directory service and you implement the Websense transparent identification feature. See [Transparent Identification](#), page 125 for more information.
- ◆ Websense software can prompt the user for identification, if the information cannot be obtained otherwise. See [Manual Authentication](#), page 208 for more information.

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).

It is generally recommended to install 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, you can 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 have the Websense User Service running on Windows, Linux, or Solaris.

See [Directory Service Access, page 187](#) for details on configuring Websense software to communicate with your directory service.

Transparent Identification

Websense transparent identification allows Websense software to filter internet requests from users in your directory service, without prompting users to manually authenticate by logging on to the browser.

Websense, Inc. currently provides four optional components for identifying users transparently in various environments. All of these 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 optional components can be used alone, or combined, with certain limitations. Limitations are 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. The Websense DC Agent is installed on a Windows Server in the network. DC Agent should *not* need to reside in any particular domain.
- ◆ **Websense Logon Agent:** Designed for use with Windows client machines. Identifies users as they log on to Windows domains. The 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:** Designed specifically for use with Novell eDirectory. Authenticates users against user accounts in Novell eDirectory.

Your installation guide includes instructions for installing each agent. Please see the appropriate section in this chapter for instructions on configuring a transparent identification agent to identify users.



NETCACHE USERS

For transparent identification to work, NetCache must send user names to Websense software in WinNT, LDAP, or RADIUS format.

Websense software can be configured to prompt users to manually authenticate if it cannot obtain the user information it needs 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 various other reasons. In this situation, you can configure Websense software to prompt users for identification so that they can be filtered by their individual object policies. See [Manual Authentication, page 208](#) for more information.

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

Combining Transparent Identification Agents

Websense, Inc. supports certain combinations of transparent identification agents within the same network, or on the same machine. Generally, it is recommended to run one agent of a particular type on one machine. If your network configuration requires multiple agents, it is best to install them on separate machines. However, you can configure Websense software to work with multiple agents on a single machine in some cases.

Supported combinations for Websense versions 5.2 and later are listed here.

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.

Combination	Same machine?	Same network?	Configuration required
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 one 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.
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 one 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 installed and set up 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. See [Filtering Remote Clients](#), page 120 for details about remote filtering.

If remote filtering is not implemented, there are still two ways Websense software can identify remote users, described next.

Remote Transparent Identification with DC Agent

The same requirements apply as with local users: The Websense DC Agent must be installed on a Windows machine. Users should also 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, it is recommended to use Websense manual authentication (see [page 208](#)).

Remote Transparent Identification with RADIUS Agent

If you are using a RADIUS server to authenticate users logging on from remote locations, the Websense RADIUS Agent can transparently identify these users so you can apply filtering policies based on users or groups. See [The Websense RADIUS Agent](#), page 150 for details on installing and configuring RADIUS Agent.

The Websense DC Agent

The Websense DC Agent can detect users in a Windows network running NetBIOS, WINS or DNS networking services.

DC Agent must be installed on a Windows Server in the network. If Policy Server is installed on a Solaris or Linux machine, but your directory service is Windows-based, install DC Agent on a separate machine running Windows Server.

DC Agent must run using administrative privileges for the domain it occupies. See [Installing DC Agent, page 131](#) for details about setting up DC Agent to use administrative privileges.



MICROSOFT PROXY/ISA USERS

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 certain internet applications.

Instructions for installing and configuring the Websense DC Agent are given in this section. Once DC Agent is installed, you need to configure Websense software to communicate with it.

Once installed, 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 Websense server components as needed. 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 three hours. You can refresh the cache by clicking the **Save Changes** button in Websense Manager. If a user is not filtered as expected, it could be because the User Service cache needs to be refreshed.

To enable transparent identification with DC Agent:

1. Install DC Agent on a Windows Server by following the instructions in the next section.
2. Configure Policy Server to allow User Service to communicate with DC Agent by following the instructions for [Configuring User Service to Communicate with DC Agent](#), page 135.
3. Add the directory objects you want to filter individually via Websense Manager by following the instructions under [Adding Directory Objects](#), page 107.

Websense software can prompt users for identification in the event User Service is not able to obtain information from a DC Agent. See [Manual Authentication](#), page 208.

Installing DC Agent

DC Agent can either be installed along with other Websense components on the same machine, or it can be installed on a different Windows Server.

If your network is large (10,000+ users), you may benefit from installing DC Agent on multiple machines. This way, you will have ample space for DC Agent files that are continually populated with user information.

If you installed Policy Server on a Windows machine, you were prompted to install the Websense DC Agent. If you did not install it along with Policy Server, you can install DC Agent separately, either on the Policy Server machine (Windows), or on a separate Windows Server machine. To do so, follow these steps.

1. Log on to the installation machine with **domain** administrator privileges. The domain administrators group you are using must be a member of the **Administrators** group on the current machine.



IMPORTANT

DC Agent must have administrator privileges on the network to retrieve user logon information from the domain controller. If you cannot install these components with such privileges, configure administrator privileges for these services after installation via the properties for Windows services. See *Websense is not filtering based on a directory object policy*, page 376 for details.

2. Download the setup file containing the Websense installer from <http://www.websense.com/global/en/Downloads/>, or copy it from the Websense CD to your local drive.

3. Double-click on the download file to extract the compressed installer files.
Instructions for extracting the setup program are displayed.
4. Click **Browse** to select a destination folder, or type in a path.
If the path you enter does not exist, the installer creates it for you.
5. Click **Extract** to begin decompressing the files.



IMPORTANT

Do not extract the installer files to a folder on your desktop. This may prevent the Real-Time Analyzer from receiving the IP address of the Policy Server machine. Accept the default location of `C:\Temp` or select another appropriate folder.

If Websense installation files already exist in that location, you can overwrite the existing files.

Setup.exe runs automatically after the files are decompressed.

6. Click **Next** on the welcome screen and follow the instructions through the subscription agreement.
7. Select **Websense Enterprise**, and then click **Next**.
8. Select **Custom**, and then click **Next**.
9. Select **DC Agent** from the list of components, and then click **Next**.
If the installation machine is multihomed, a list of enabled network interface cards appears.

10. Select the card you want Websense software to use to communicate, and then click **Next**.



IMPORTANT

The configuration port (55806) in this dialog box is the default port number used to install Policy Server. If you installed Policy Server using a different port number, enter that port in this dialog box.

11. Enter the IP address of the Policy Server machine and the port number if different from the default, and then click **Next**.

Setup asks for a user name and password with administrative privileges on the domain. If you install DC Agent without providing access to directory information, DC Agent will be unable to identify users transparently.

12. Enter the domain and user name, followed by the network password for an account with domain privileges, and then click **Next**.
13. Accept the default path (C:\Program Files\Websense), or click **Browse** to locate another installation folder and then click **Next** to continue.

The installer assesses the resources of the installation machine. If the machine has inadequate disk space or memory, separate warnings are displayed.

A summary list shows the installation path, download file size, installation size, and the components you have selected.

14. Click **Next** to start the installation.

Setup downloads the appropriate installer files. Installation begins automatically when the necessary files have been downloaded.

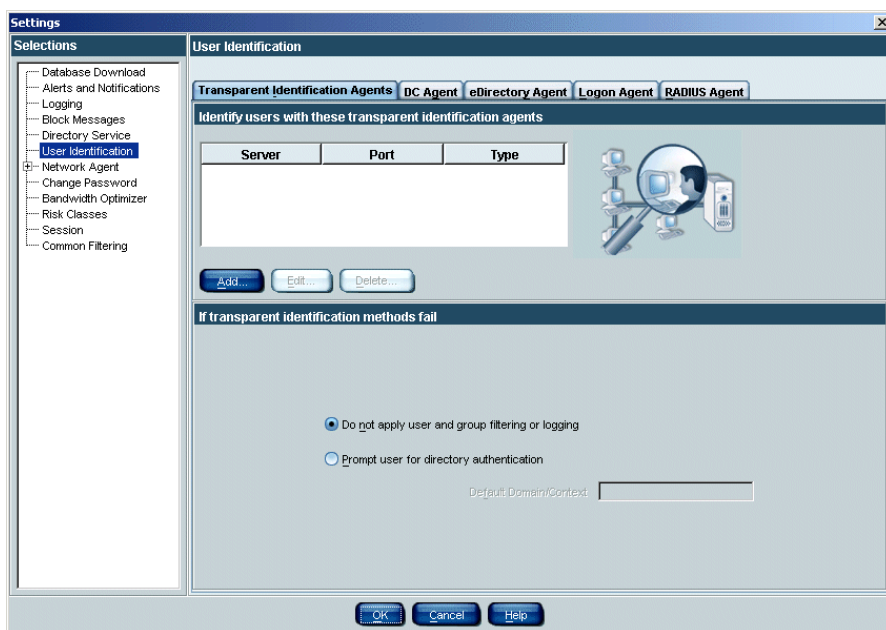
A message is displayed advising you that the procedure was successful.

15. Click **Next** to continue.
16. Select a restart option and click **Finish** to exit the installer.
17. Configure User Service to communicate with DC Agent by following the instructions in the next section.

Configuring User Service to Communicate with DC Agent

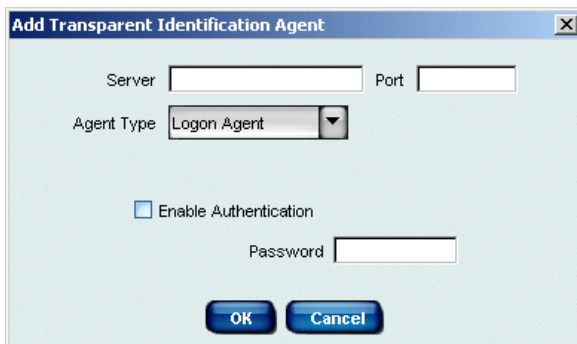
When you installed the Websense DC Agent, Websense software was automatically configured to communicate with DC Agent. However, it is recommended to verify your configuration.

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



User Identification settings

6. If this is a new agent instance that does not appear in the list, add the agent as follows.
 - a. Click the **Add** button. The **Add Transparent Identification Agent** dialog box appears.



Add Transparent Identification Agent dialog box

- b. Enter the following information.
 - **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 will communicate. The default is 30600.
 - c. For **Agent Type**, select **DC Agent** from the drop-down list.

8. Under **DC Agent Settings**, specify the following information:
 - **TCP Port:** Specify the port over which DC Agent connects to the Websense User Service. Normally, it is recommended 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 ConsoleClient troubleshooting tool listens for data from DC Agent.
9. To establish an authenticated connection between User Service and DC Agent, check **Enable Authentication**.
10. 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.

11. Under **Domain Controller Settings**, 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. 10 seconds (default) is typically an ideal interval.
 - **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 by adding the case-sensitive parameter `EntryLifetime=[N]` to the **transid.ini** file. See [Configuring Different Settings for an Agent Instance](#), page 182 for instructions on editing this file.

12. Under **Workstation Settings**, check **Enable workstation polling** if you want 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. It is generally recommended to accept the default interval (15 minutes). 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 user map accuracy.
 - **User Entry Timeout:** Specify how often DC Agent refreshes its user map. It is recommended to accept the default value (1 hour). Increasing this interval may result in missed logons. 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, as 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.
13. 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 the **Websense/bin** directory (Solaris or Linux).

14. Click **OK** to save the changes and close the **Settings** dialog box.

15. To configure DC Agent to ignore logon names that are not associated with actual users, do this step.

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** in order 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.

Follow these instructions to set up a list of user names, or user name/workstation pairs, for the Websense DC Agent to ignore.

- a. Stop the DC Agent service, using the **Services** applet accessible via **Control Panel** (*Windows NT*) or **Administrative Tools** (*Windows 200x*).
- b. Go to the `\Websense\bin\` directory, and locate the text file named **ignore.txt**.
- c. Open the file in a text editor.
- d. Add to this file two types of entries, according to your needs.

User names: Type a one-line entry for each user name to be ignored. Websense software will ignore user names listed this way, regardless of the associated workstation.

User name/workstation pairs: Type two words per line, separated by a comma, for each user name/workstation pair to be ignored. Websense software will ignore a user name only if it comes from the corresponding workstation.

In the following example:

```
johnsmith  
admin,WKSTA-NAME
```

The user name **johnsmith** will be ignored for ALL workstations. The user name **admin** will only be ignored if it came from workstation **WKSTA-NAME**.

- e. Save and close the file when all entries are complete.
- f. Restart the DC Agent service.



NOTE

Occasionally, when you create a new Windows workgroup, all machines are temporarily included in the new workgroup. This problem resolves itself after a few minutes. Try refreshing the view in Windows Explorer. If this problem recurs frequently, see Websense Knowledge Base article #919 for additional information.

- 16. Add the directory objects you want to filter individually by following the instructions in *Chapter 5 Clients*.

The Websense Logon Agent

The 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. The associated logon application must be deployed to client machines from a central location, such as the Websense Filtering Service machine.

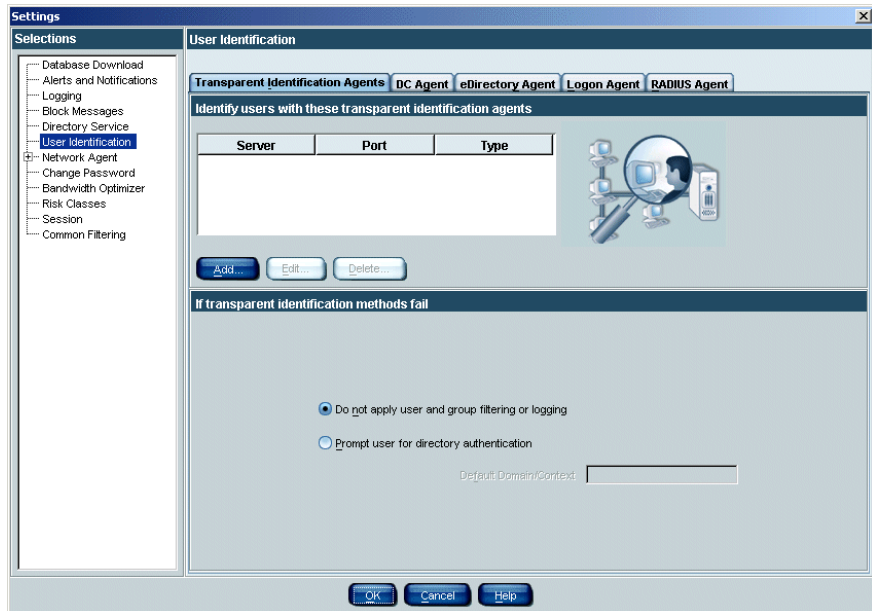
See your installation guide for instructions on installing the Logon Agent and its associated logon application. After installation, configure the Agent to communicate with client machines and with the Websense Filtering Service, as described here.

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.

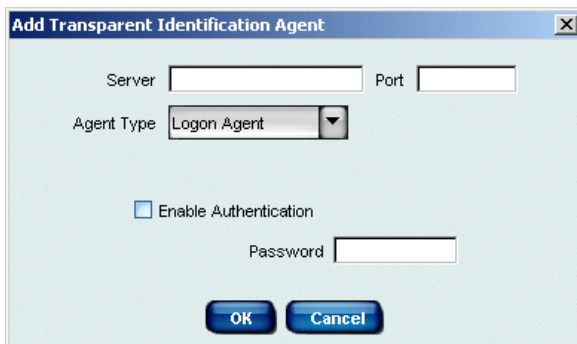
When you installed the Websense Logon Agent, Websense software was automatically configured to communicate with Logon Agent. However, it is recommended to verify your Logon Agent configuration, as follows.

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



User Identification settings

6. 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.



Add Transparent Identification Agent dialog box

- b. Enter the following information:
 - **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 will communicate. The default is 30602.
- c. For **Agent Type**, select **Logon Agent** from the drop-down list.

- 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**.
7. Go to the **Logon Agent** tab. The Logon Agent settings are displayed.

The screenshot shows the 'User Identification' dialog box with the 'Logon Agent' tab selected. The settings are as follows:

- Logon Agent Settings:**
 - TCP Port: 30602
 - Diagnostic Port: 30603
 - Enable Authentication:
 - Password: [Empty field]
- HTTP Settings:**
 - HTTP Server Port: 15880
 - Maximum Connections (HTTP): 200
- Timeout Settings:**
 - Query Interval (persistent mode): 15 minutes
 - Entry Lifetime (non-persistent mode): 24 hours

Buttons at the bottom: OK, Cancel, Help.

Logon Agent User Identification settings

8. Under **Logon Agent Settings**, specify the following information:
 - **TCP Port:** Specify the port over which Logon Agent connects to the Websense Filtering Service. Normally, it is recommended to accept 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.
9. To establish an authenticated connection between Filtering Service and Logon Agent, check **Enable Authentication**.

10. If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
11. **Under HTTP Settings**, specify the following:
 - **HTTP Server Port**: Specify the port over which the logon application connects to Logon Agent.
 - **Maximum HTTP Connections**: Specify 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. Keep in mind that increasing the number can increase network traffic.
12. **Under Logon Application Settings**, specify the following:
 - **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 at any time, the change will 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.

13. Click **OK**.



NOTE

If Websense software is not able to connect to Logon Agent, it logs a message in the Application Event Log (Windows), or in the **Websense.log** file in the **/Websense/bin/** directory (Solaris or Linux).

14. Click **OK** to save the changes and close the **Settings** dialog box.

Add the directory objects you want to filter individually by following the instructions in [Chapter 5 Clients](#).

Troubleshooting DC Agent or Logon Agent

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

First, check the topics in *Chapter 10 Troubleshooting* for possible solutions. If user identification problems occur, it is recommended that you check all network connections, and then check the Windows Event Viewer and/or the Websense Log for related error messages. If you are unable to identify a user identification problem, Websense Technical support can assist you.



NOTE

To troubleshoot any problems with RADIUS Agent or eDirectory Agent, it is recommended to use their built-in diagnostic capabilities. See the appropriate section in this chapter for instructions.

Windows Services (or Service Control Manager)

Transparent identification agents, User Service, and Filtering Service run as Windows services, so they 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: Choose **Start > Programs > Administrative Tools > Event Viewer**. From the **Log** menu, choose **Application**.

Windows 2000/2003: Choose **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 the Websense 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 be used to gather data that may reveal the cause.

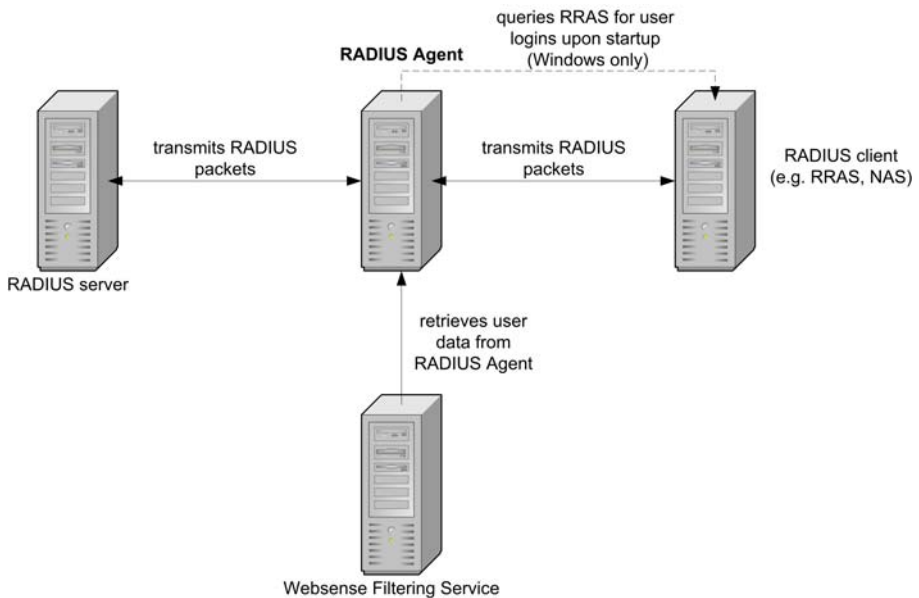
The transparent identification agents store user name-to-IP address correspondences to a “user map” in local memory. Analyzing the user name associations an agent has recorded can help determine whether users and workstations are being identified correctly.

See *Websense Technical Support Services*, [page 409](#) for Websense Technical Support contact information.

The Websense RADIUS Agent

The Websense RADIUS Agent allows you to integrate your Websense filtering policies with authentication provided by a RADIUS server. The 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).

The 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 automatically integrates with your existing Websense components. However, RADIUS Agent, your RADIUS server and your RADIUS client must be configured appropriately. See [Configuring the RADIUS Environment](#), page 152 for details.

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. Optimally, 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 can glean 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, the Websense RADIUS Agent captures and processes all RADIUS protocol packets of the following 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.

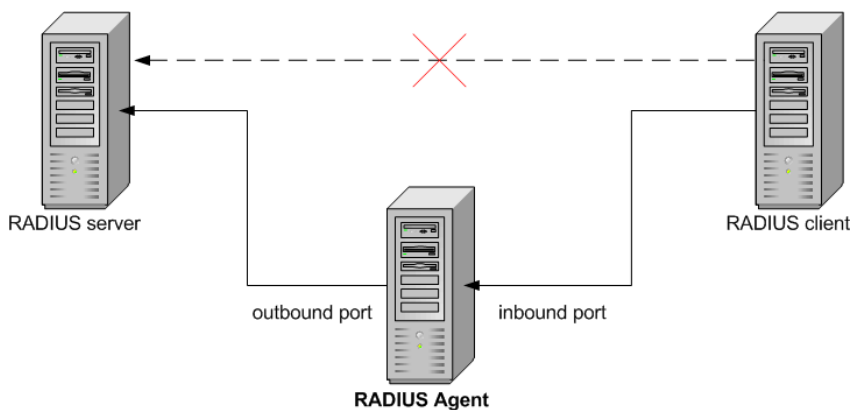
Installing RADIUS Agent

Using RADIUS Agent to identify remote users requires that you have both a RADIUS server and a RADIUS client installed in your network. The RADIUS client can be a server such as a Network Attached Storage (NAS) server, or a remote access server.

For instructions on installing RADIUS Agent, see your installation guide.

Configuring the RADIUS Environment

The Websense RADIUS Agent serves as a proxy between a RADIUS client and a RADIUS server. The following 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, do the following to configure your environment for RADIUS Agent.

- ◆ Configure the 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. It is recommended 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. Please refer to your RADIUS server documentation for instructions on configuring a proxy. If you have multiple RADIUS servers, each server must be configured separately.

**LUCENT RADIUS SERVER AND MICROSOFT RRAS**

Lucent RADIUS Server must be configured to use Password Authentication Protocol (PAP), and the RRAS server must be configured to accept only PAP requests. For instructions, please consult your respective product documentation.

Perform the following configuration procedures to set up your RADIUS environment.

Configure RADIUS Agent and Filtering Service

The Websense Filtering Service must be able to communicate with RADIUS Agent. When you installed the Websense RADIUS Agent, Websense software was automatically configured to communicate with RADIUS Agent. However, it is recommended to verify your RADIUS Agent configuration.



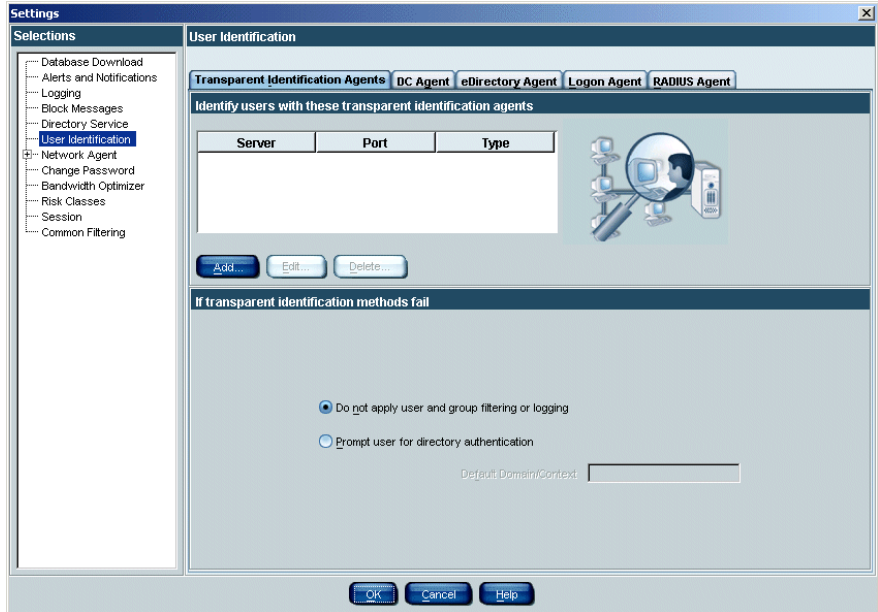
NOTE

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. The procedure below includes specifying the necessary IP address.

To configure RADIUS Agent:

1. Open Websense Manager.
2. Right-click the Policy Server icon, and then choose **Log On to Server**.
3. Enter the password for this Policy Server, and then click **OK**.
4. Choose **Server > Settings**. The **Settings** dialog box appears.

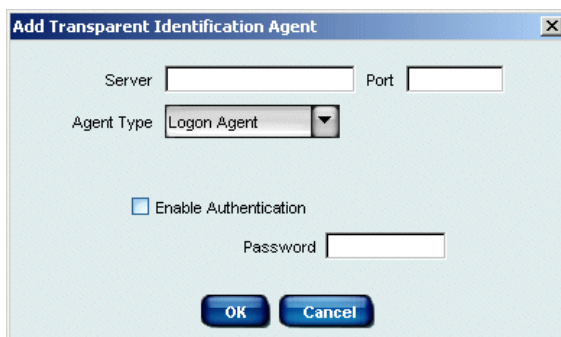
5. Select **User Identification** at the left.
Installed agents appear in a list under **Identify users with these transparent identification agents**.



User Identification settings

6. *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.



Add Transparent Identification Agent dialog box

- 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 automatically specified for this purpose during installation.

If you need to use a different port number, please contact Technical Support for assistance.

- d. For **Agent Type**, select **RADIUS Agent** from the drop-down list.
- 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**.
7. Go to the **RADIUS Agent** tab. 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. See [Configuring Different Settings for an Agent Instance](#), page 182 for information.

User Identification

Transparent Identification Agents
DC Agent
eDirectory Agent
Logon Agent
RADIUS Agent

RADIUS Agent Settings

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

TCP Port *
 Enable Authentication *
Password *

Diagnostic Port *

RADIUS Server Settings

RADIUS server *
User Entry Timeout hours

RRAS Machine (Windows Only) *

Authentication Ports

From RADIUS Agent to RADIUS server *

From RADIUS clients to RADIUS Agent *

Accounting Ports

From RADIUS Agent to RADIUS server *

From RADIUS clients to RADIUS Agent *

RADIUS Agent User Identification settings

8. Specify the ports RADIUS Agent uses:
 - **TCP Port:** Specify the port over which RADIUS Agent connects to the Websense User Service. Normally, it is recommended to accept the default port (30800).
 - **Diagnostic Port:** Accept the default port for RADIUS Agent diagnostic activities (30801). This is the port over which the RADIUS Agent troubleshooting tool listens for data from RADIUS Agent.
9. To establish an authenticated connection between User Service and RADIUS Agent, check **Enable Authentication**.
10. If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
11. Specify the following information:
 - **RADIUS Server:** Enter 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, enter the IP address of the machine running RRAS. Websense software queries this machine for user logon sessions.
 - **User Entry Timeout:** Specify the interval at which RADIUS Agent refreshes its user map. It is recommended to accept the default query value (24 hours).
 - **Authentication ports:** Specify the ports over which RADIUS Agent sends and receives authentication requests.
 - **Accounting ports:** Specify the ports over which RADIUS Agent sends and receives accounting requests.
12. Click **OK**.
13. Click **OK** to save the addition and close the **Settings** dialog box.

Filtering Service, User Service and RADIUS Agent are configured to communicate.

Configuring RADIUS Agent to Ignore Certain User Names

You can configure RADIUS 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** in order 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 Websense RADIUS Agent service (see [page 165](#)).
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 one-line entry for each user name to be ignored. Websense software will ignore user names listed this way, regardless of the associated workstation. Do not use wildcard characters, such as “*”.

In the following example:

```
johnsmith  
aperez, enggroup1
```

The user name **johnsmith** will be ignored for ALL workstations. The user name **aperez** will be ignored only for the domain **enggroup1**.

5. Save and close the file when all entries are complete.
6. Restart the Websense RADIUS Agent service.

RADIUS Agent will ignore the user names you have specified, and Websense software will not consider these names in filtering.

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 for this purpose during configuration of RADIUS Agent (see [page 154](#)).
- ◆ 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 for this purpose during configuration of RADIUS Agent (see [page 154](#)).

The procedure for configuring your RADIUS client differs depending on the type of client used. Please refer to your RADIUS client documentation for instructions.



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 your RADIUS client documentation for instructions.

Configure the RADIUS Server

To enable proper communication between the 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. See your RADIUS server documentation for instructions on modifying the client list. See *Example: Configuring a Client*, page 162 for an example.
- ◆ 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.

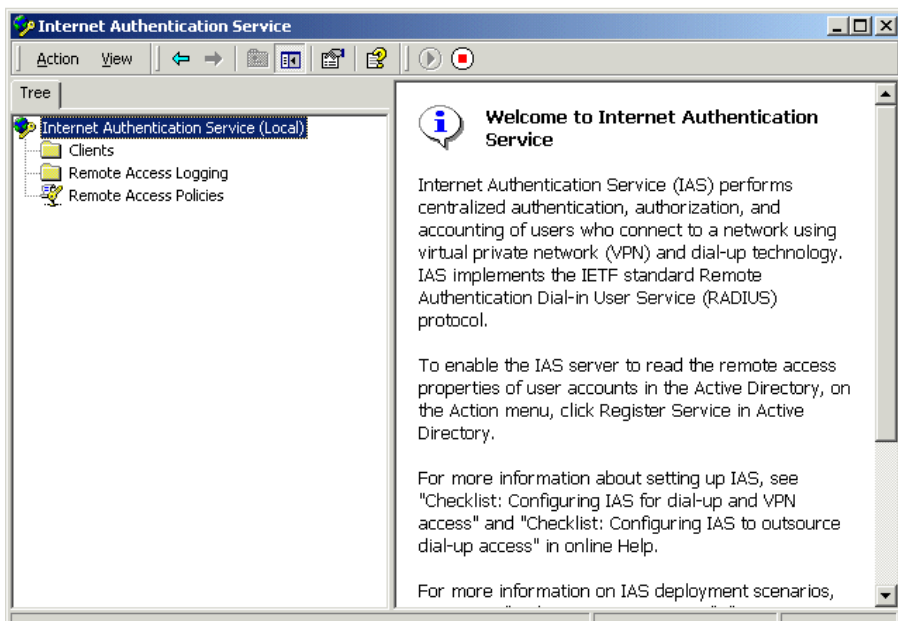
Configuring a shared secret for RADIUS clients and the RADIUS server provides secure transmission of RADIUS messages. Typically, the shared secret is a common text string. See your RADIUS server documentation for instructions on configuring shared secrets.

As an example, the procedure for configuring a VPN client for use with Microsoft Internet Authentication Service (IAS) as the RADIUS server follows. This procedure applies specifically to a Microsoft IAS environment. However, the procedure is similar to configuring any RADIUS client.

Example: Configuring a Client

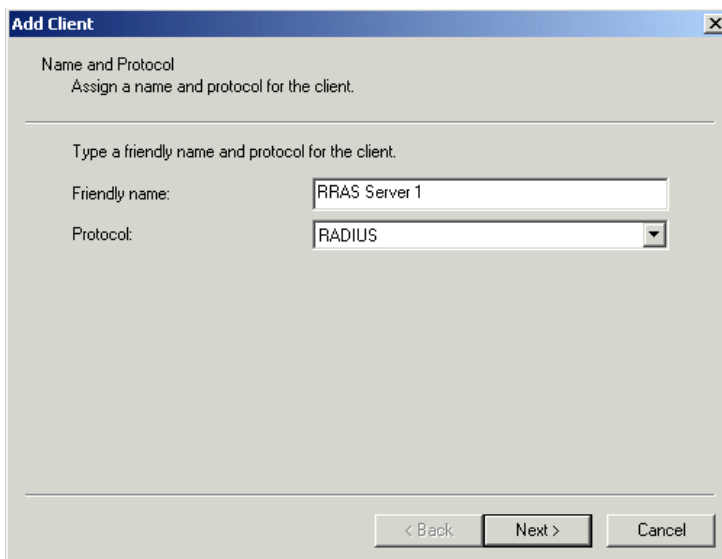
To configure a VPN client for use with Microsoft IAS:

1. Open the Internet Authentication Service console.



Internet Authentication Service console

2. In the navigation tree, right-click **Clients**, and then choose **New Client**. The **Add Client** dialog box appears.

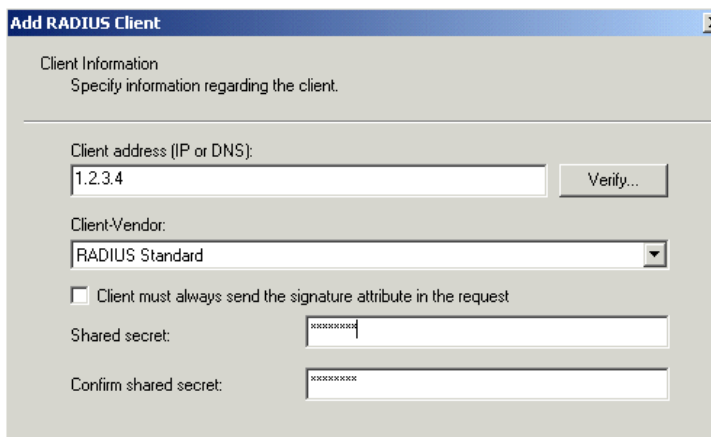


The **Add Client** dialog box is titled "Add Client" and contains the following elements:

- Name and Protocol**: Assign a name and protocol for the client.
- Type a friendly name and protocol for the client.**
- Friendly name:** Text input field containing "RRAS Server 1".
- Protocol:** Drop-down menu showing "RADIUS".
- Navigation buttons:** "< Back", "Next >", and "Cancel".

Add Client dialog box

3. In the **Friendly name** field, enter a unique name by which you can recognize the client.
4. For **Protocol**, select RADIUS from the drop-down list.
5. Click **Next**. The **Add RADIUS Client** dialog box appears.



The **Add RADIUS Client** dialog box is titled "Add RADIUS Client" and contains the following elements:

- Client Information**: Specify information regarding the client.
- Client address (IP or DNS):** Text input field containing "1.2.3.4" and a "Verify..." button.
- Client-Vendor:** Drop-down menu showing "RADIUS Standard".
- Client must always send the signature attribute in the request
- Shared secret:** Password input field with masked characters.
- Confirm shared secret:** Password input field with masked characters.

Add RADIUS Client dialog box

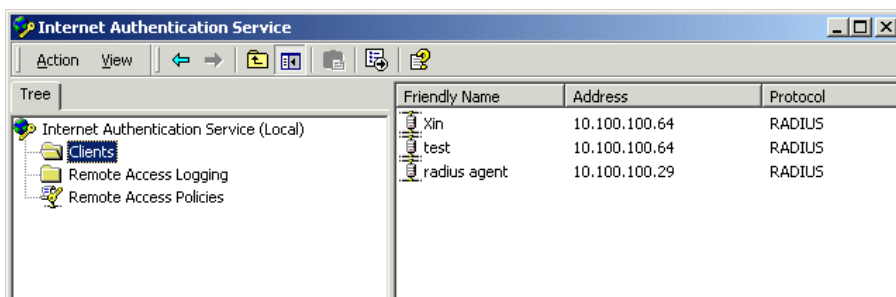
6. For **Client address (IP or DNS)**, enter the IP address of the client machine.

7. For **Client-Vendor**, select **RADIUS Standard** from the drop-down list.
8. For **Shared secret**, enter the text string you have defined as a shared secret between your RADIUS server and RADIUS client. Confirm the shared secret by typing it again.
9. Click **Finish**.

You have added your RADIUS client to the Microsoft IAS RADIUS server.

**NOTE**

A single IAS can support multiple clients. To add another client, repeat [Step 2](#) through [Step 9](#) above. Added clients appear under **Clients** in the navigation tree of the Internet Authentication Service console window.



Clients added to Internet Authentication Service

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.

<http://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 your RADIUS server documentation for instructions.

Starting and Stopping RADIUS Agent

After you have installed RADIUS Agent, follow the appropriate steps below to start it. Your method of starting the Agent depends on the installation method used (see *Installing RADIUS Agent*, page 152).

Starting in Console Mode

To start the Agent in console mode (as an application), do the following.

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 a description of each command attribute, see *Command Attributes*, page 167.

Starting in Service Mode (Windows)

Follow these steps to start the RADIUS Agent service.



IMPORTANT

Do not start the RADIUS Agent service while the RADIUS server is down.

1. Open the Windows **Services** dialog box: Choose **Start > Programs > Administrative Tools**, and then double-click **Services**.
2. Right-click **Websense RADIUS Agent**, and then choose **Start**.

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 a description of each command attribute, see [Command Attributes](#), page 167.

Stopping RADIUS Agent

Use the methods shown 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 choose **Stop**.

Linux/Solaris:

1. At the prompt, type the following:

```
WebsenseAdmin stop
```



NOTE

This command stops any Websense services running on this machine.

2. Press **Enter**.

The Websense RADIUS Agent service is stopped.

Command Attributes

The table below describes the available command attributes for RADIUS Agent.



NOTE

On Linux/Solaris, Websense, Inc. recommends using the script provided to start or stop the Websense RADIUS Agent (`wsRADIUSAgent start | stop`), instead of the `-r` and `-s` command parameters.

Parameter	Description
<code>-i</code>	Installs the RADIUS Agent service/daemon.
<code>-r</code>	Runs the RADIUS Agent service/daemon.
<code>-s</code>	Stops the RADIUS Agent service/daemon.
<code>-c</code>	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.
<code>-v</code>	Displays the version number of RADIUS Agent.
<code>-?</code> <code>-h</code> <code>-help</code> <code><no option></code>	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. You can enable debugging, indicate a level of detail for log messages, and choose a location for log output.

Follow these steps to activate RADIUS Agent logging and debugging.

1. Stop the RADIUS Agent service (see *Starting and Stopping RADIUS Agent*, page 165).
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 165).

If remote users are not being identified and/or filtered as expected, the likely cause is communication problems between RADIUS Agent and your RADIUS server. Checking your RADIUS Agent logs for errors can help you determine the specific cause of the problem.

For help with problems running RADIUS Agent or identifying remote users, please see *Troubleshooting*, page 363, or refer to the Websense Knowledge Base at <http://www.websense.com/global/en/SupportAndKB/>.

The Websense eDirectory Agent

The 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 automatically integrates with your existing Websense components. However, some minimal configuration required to ensure that eDirectory Agent and Novell eDirectory are communicating properly. See *Configuring the eDirectory Environment*, page 171 for details.

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. The 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 the Websense User Service, eDirectory Agent supplies this information to the Websense Filtering Service.



NOTE

From a Novell Client running Windows, multiple users can log on to one Novell eDirectory server. This associates one 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.

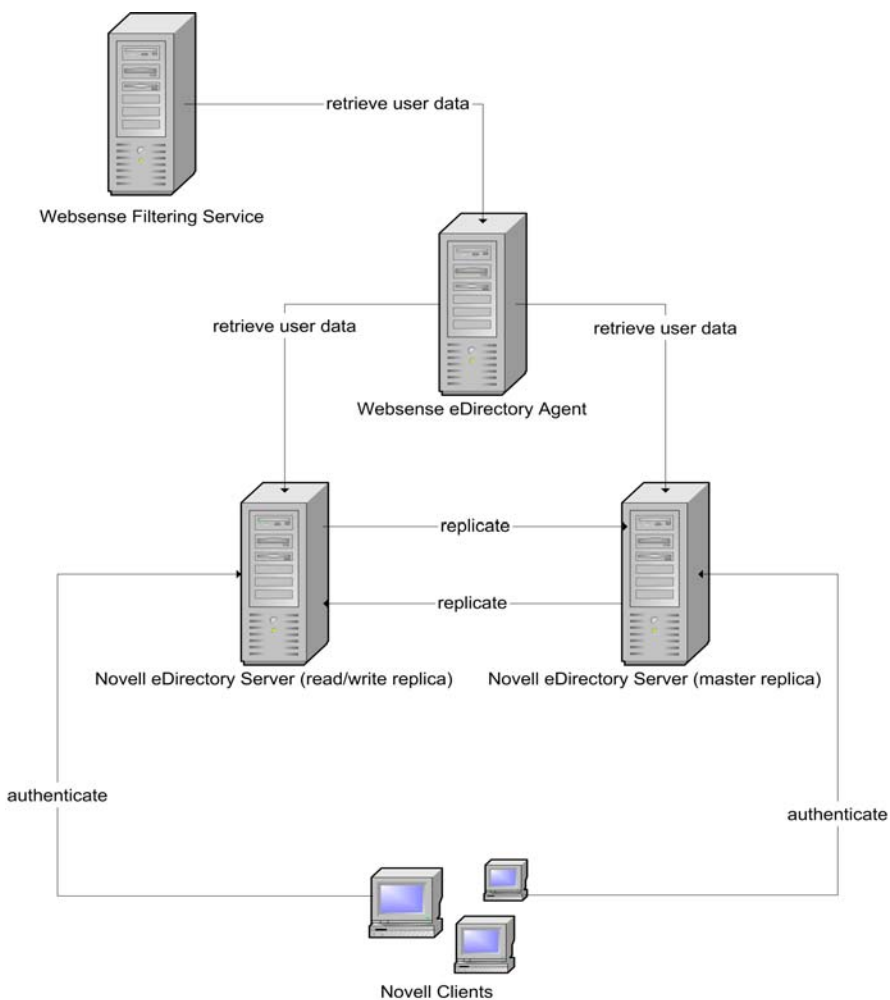
One instance of the Websense eDirectory Agent can support one Novell eDirectory master, plus any number of Novell eDirectory “replicas.”

Following is an illustration of how eDirectory Agent works in conjunction with a Novell eDirectory master and replica.



NOTE

Websense, Inc. does not currently support using the Websense eDirectory Agent together with the Websense DC Agent.



eDirectory Agent working with eDirectory master and replica

Configuring the eDirectory Environment

The Websense eDirectory Agent queries Novell eDirectory for user logon session information at a given interval. You must specify certain network parameters for the Websense eDirectory Agent to get user logon information from Novell eDirectory.

After installing the Websense eDirectory Agent, do the following to configure the Agent.

Configure Novell eDirectory

The location of Novell eDirectory is specified during installation of the Websense eDirectory Agent. If you are using multiple Novell eDirectory replicas, ensure that you have specified the server where each replica is running. If you did not already specify multiple servers during installation, please follow the instructions under [Configuring a Multiple-Replica Environment](#), page 178.



CISCO CONTENT ENGINE USERS

If you have integrated Cisco Content Engine v5.3.1.5 or higher with Websense software, do the following:

- ◆ 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 **wsedir.bak** file.
 - ◆ Run Websense Reporting Tools services on a machine *separate* from Cisco Content Engine and Websense software.
-

In previous versions of Websense, it was necessary to disable Novell Modular Authentication Service (NMAS) on all machines running eDirectory or eDirectory replicas. Websense software now supports using NMAS with the Websense eDirectory Agent. Disabling NMAS is no longer necessary.



IMPORTANT

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. See your Novell documentation for information about installing the Novell Client software. See your Websense installation guide for supported versions of the software.

Determine the eDirectory Agent Protocol

The 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, in Websense v6.1, 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, you can 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 certain other protocols), then you may want to continue using LDAP.

To set the Websense eDirectory Agent on Windows to use LDAP instead of NCP, do the following.

1. Ensure that you have at least one Novell eDirectory replica containing all directory objects you want 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.)

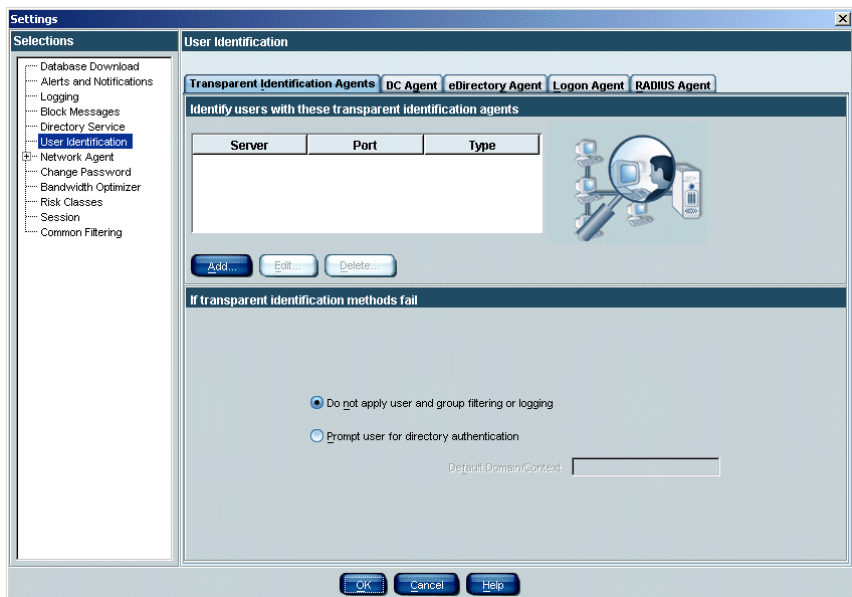
6. Save and close the file when all entries are complete.
7. Restart the Websense eDirectory Agent service.

Configure eDirectory Agent and Filtering Service

When you installed the Websense eDirectory Agent, Websense software was automatically configured to communicate with eDirectory Agent. However, it is recommended to verify your eDirectory Agent configuration.

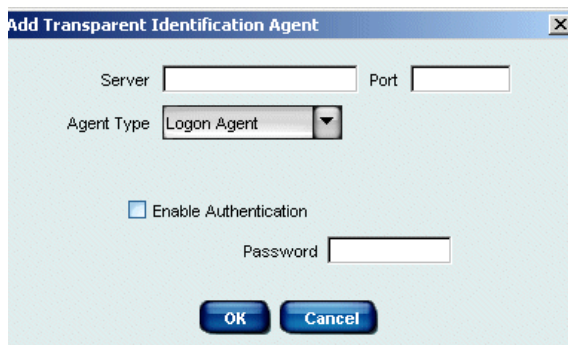
1. Open Websense Manager.
2. Right-click the Policy Server icon, and then choose **Log On to Server**.
3. Enter the password for this Policy Server, and then click **OK**.
4. Choose **Server > Settings**. The **Settings** dialog box appears.
5. Select **User Identification** at the left.

Installed agents appear in a list under **Identify users with these transparent identification agents**.



User Identification settings

6. 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.



Add Transparent Identification Agent dialog box

- 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 automatically specified for this purpose during installation.

If you need to use a port other than 30700, please contact Technical Support for assistance.

- d. For **Agent Type**, select **eDirectory Agent** from the drop-down list.

- 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**.
7. Go to the **eDirectory Agent** tab. The eDirectory Agent user identification settings are displayed.



IMPORTANT

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. See [Configuring Different Settings for an Agent Instance](#), page 182 for information.

User Identification

Transparent Identification Agents | DC Agent | **eDirectory Agent** | Logon Agent | RADIUS Agent

eDirectory Agent Settings

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

TCP Port * Enable Authentication * Password *

Diagnostic Port *

eDirectory Server Settings

eDirectory Server Search Base *

eDirectory Administrator Fully Distinguished Name *

eDirectory Administrator Password *

User Entry Timeout hours

eDirectory Server Replicas

Server *	Port *

eDirectory Agent User Identification settings

8. Under **eDirectory Agent Settings**, specify the following:
 - **TCP Port:** Specify the port over which eDirectory Agent connects to the Websense User Service. Normally, it is recommended to accept the default port (30700).
 - **Diagnostic Port:** Accept the default port for eDirectory Agent diagnostic activities (30701). This is the port over which the eDirectory Agent troubleshooting tool listens for data from eDirectory Agent.
9. To establish an authenticated connection between Filtering Service and eDirectory Agent, check **Enable Authentication**.
10. If you checked **Enable Authentication**, enter a password for the authenticated connection to Filtering Service.
11. Under **eDirectory Server Settings**, specify the following information:
 - **eDirectory Server Search Base:** Enter the root context in your Novell eDirectory server.
 - **eDirectory Administrator Fully Distinguished Name:** Enter the name of the administrative user for Novell eDirectory server.
 - **eDirectory Administrator Password:** Enter the password for the Novell eDirectory server administrative user.
 - **User Entry Timeout:** Specify how long entries remain in the Agent's user map. It is recommended to use 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.
12. Click **OK** to save the addition and close the **Settings** dialog box.

Filtering Service, User Service and eDirectory Agent are configured to communicate.

Configuring eDirectory Agent to Ignore Certain User Names

You can configure eDirectory 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** in order 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.

Windows XP automatically sets up two internal user names (**Local Service** and **Network Service**) for various internal processes to use for communication with domain controllers. You can configure Websense software to ignore such user names.

1. Stop the Websense eDirectory Agent service (see [page 179](#)).
2. Go to the `\Websense\bin\` directory, and locate the file named **ignore.txt**.
3. Open the file in a text editor.
4. Type a one-line entry for each user name to be ignored. Websense software will ignore user names listed this way, regardless of the associated workstation. Do not use wildcard characters, such as “*”.

In the following example:

```
johnsmith  
aperez, enggroup1
```

The user name **johnsmith** will be ignored for ALL workstations. The user name **aperez** will be ignored only for the domain **enggroup1**.

5. Save and close the file when all entries are complete.
6. Restart the Websense eDirectory Agent service.

eDirectory Agent will ignore the user names you have specified, and Websense software will not consider these names in filtering.

Configuring a Multiple-Replica Environment

One instance of the Websense eDirectory Agent can support one 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 need to wait for eDirectory replication to occur.

Novell eDirectory replicates the attribute that uniquely identifies logged-on users only every five 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, you must update the eDirectory Agent configuration, as follows.

1. Stop the eDirectory Agent service (see *Starting and Stopping eDirectory Agent*, page 179).
2. Add each eDirectory replica to Websense Manager using the procedure under *Configure eDirectory Agent and Filtering Service*, page 173, Step 6.
3. Start eDirectory Agent (see *Starting and Stopping eDirectory Agent*, page 179).

Starting and Stopping eDirectory Agent

After you have installed eDirectory Agent, use the procedures below to start or stop the Agent. Your method of starting the Agent depends on the installation method used. (See your installation guide for details.)



IMPORTANT

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: Choose **Start > Programs > Administrative Tools**, and then double-click **Services**.
2. Right-click **Websense eDirectory Agent**, and then choose **Start**.

Starting in Daemon Mode (Linux/Solaris)

Type at a command prompt:

```
WebsenseAdmin start
```

and then press **Enter**.

Stopping eDirectory Agent

Use the methods shown here 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 choose **Stop**.

Linux/Solaris:

1. At the prompt, type the following:

```
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, indicate a level of detail for log messages, and choose a location for log output.

If you did not already enable logging during installation, as follows.

1. Stop eDirectory Agent (see [Starting and Stopping eDirectory Agent, page 179](#)).
2. On the eDirectory Agent machine, go to the eDirectory Agent installation directory.
3. Open the file **wseidir.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 **wseidir.ini** file.
9. Start the eDirectory Agent service (see [Starting and Stopping eDirectory Agent, page 179](#)).

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 certain global settings in the **Settings** dialog box. Settings that can be overridden in this manner are marked with an asterisk (*) in the **Settings** dialog box.

To configure a particular instance of an agent:

1. Stop all Websense services (see [Stopping or Starting Websense Services](#), page 217). Be sure to include the transparent identification agent service (see [Starting and Stopping eDirectory Agent](#), page 179 for an example).
2. On the machine running the agent instance, go to the agent installation directory.
3. Open the appropriate .ini file in a text editor:
 - for DC Agent: **transid.ini**
 - for eDirectory Agent: **wseidir.ini**
 - for RADIUS Agent: **wseiradius.ini**
4. Locate the parameter you want to change for this agent instance. See [.ini Parameter to Field Name Correspondences](#), page 185 for parameter names and descriptions.

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, as shown:

```
password=[xxxxxxx]
```

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.journal**
- **XidDcAgent.bak**

These files will be recreated automatically when you start the Websense DC Agent service.

8. Update the agent settings.
- a. In Websense Manager, choose **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.



IMPORTANT

If you modified the `port` value for this agent instance (equivalent to the **TCP Port** in the **Settings** dialog box), you must 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.



Edit Transparent Identification Agent dialog box

- 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 here 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 217).

.ini Parameter to Field Name Correspondences

Websense Manager field label	.ini parameter name	Description
TCP Port <i>(all agents)</i>	port	The port over which the agent connects to the Websense User Service.
Diagnostic Port <i>(all agents)</i>	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 <i>(all agents)</i>	password	The password the agent uses to authenticate the Websense User Service when it contacts the agent. Specifying this password automatically enables authentication.
Query interval <i>(DC Agent)</i>	QueryInterval	The interval at which DC Agent queries domain controllers.
Server, Port <i>(eDirectory Agent)</i>	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 <i>(Windows Only)</i>	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.

Directory Service Access

Websense software allows you to set up filtering based on individual directory object (user, group, or domain/organizational unit) policies. When Websense software is installed for the first time, all users are filtered by the restrictions in the **Global** policy.

Filtering based on policies assigned to directory objects requires that Websense software be configured to access your directory service to get directory object information.

Refer to the following sections for instructions on configuring access to your directory service.

- ◆ **Windows NTLM-based directory:** See [Windows NTLM-based Directory, page 187](#).
- ◆ **LDAP directory:** See [LDAP-based Directory, page 192](#).



IMPORTANT

You can only configure settings for one type of directory service per Policy Server. Settings for additional directory services will not be saved.

Websense software can communicate with your directory service whether it runs on the same operating system as Websense software or on a different system. 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. For instructions on installing User Service, see your installation guide.

Windows NTLM-based Directory

Websense software accesses your directory service when you add directory objects to Websense Manager in order to assign filtering policies, and when Websense software analyzes internet requests. Before you can filter based on specific user, group, and domain/organizational unit policies, you must add the directory objects that you want 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. See *Chapter 5 Clients* for instructions on adding directory objects.

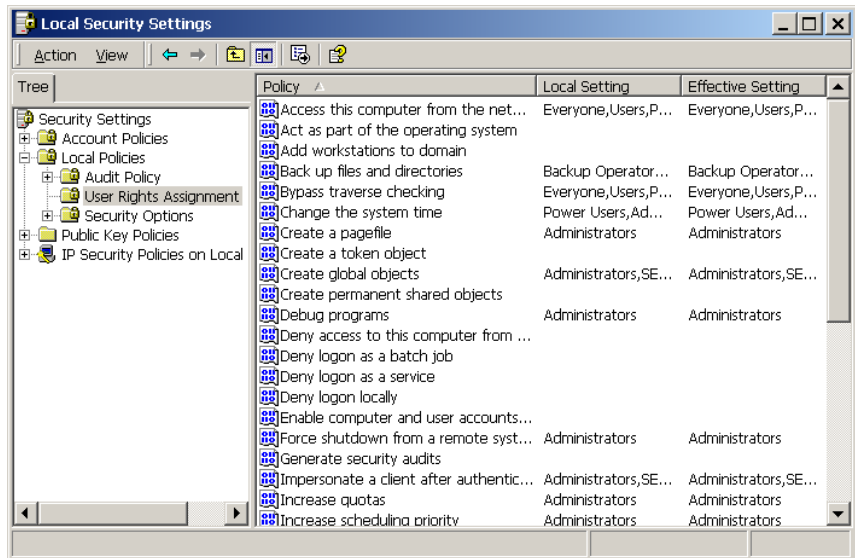
The Websense User Service is specially designed to be compatible with Windows- or UNIX-based operating systems. Even if you are using a Windows NTLM-based directory service, you can run the Websense User Service on Windows, Linux, or Solaris.

Windows 2000/2003 Environment

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

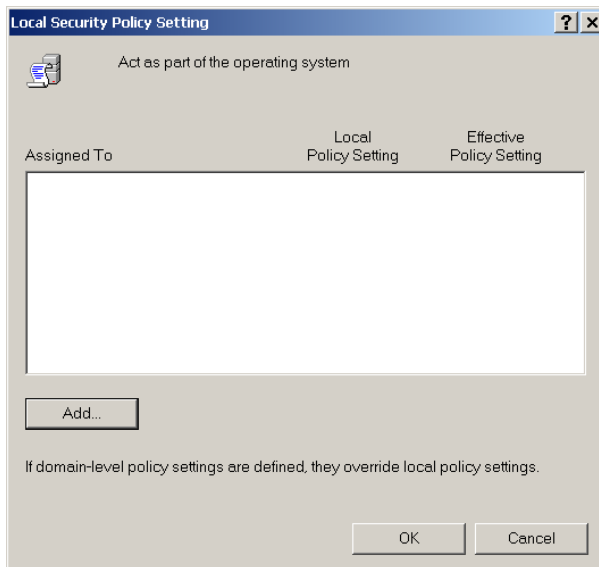
Follow these steps to configure a Local Security Policy for User Service.

1. Log on to the User Service machine as a user with local administrative rights.
2. From the Windows **Start** menu, select **Programs > Administrative Tools > Local Security Policy**.
The **Local Security Settings** window appears.
3. In the console tree, expand **Local Policies > User Rights Assignment**.



User Rights Assignment policies in Local Security Settings Window

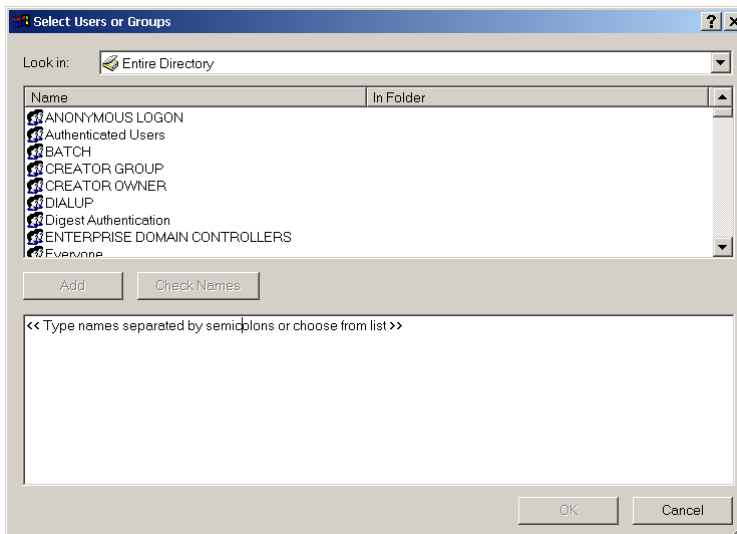
4. Under **Policy**, right-click **Act as part of the operating system**.
5. Select **Security** to display the **Local Security Policy Setting** dialog box. (This is a Windows 2000 command. The Windows 2003 interface may be slightly different.)



Local Security Policy Setting dialog box for the policy, "Act as part of the operating system"

6. Click **Add**.

The **Select Users, Computers, or Groups** window appears.



Select Users, Computers, or Groups window

7. For **Look in**, select the domain where the User Service machine resides.
8. Under **Name**, select **Websense**.

**NOTE**

If you typed a user name in the bottom pane of the **Select Users, Computers, or Groups** window, click **Check Names** to ensure that the selected user name is fully qualified.

9. Click **Add**.
10. Click **OK** to assign the policy to this user, and return to the **Local Security Policy Setting** dialog box.
11. Click **OK** to confirm the addition, and return to the **Local Security Settings** window.
12. Close the **Local Security Settings** window.

The account User Service uses to communicate with the directory service is configured to run as part of the operating system. This enables Websense software to identify users correctly.

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



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. You can create named groups of users based on any LDAP attribute in your directory service, and add these groups to Websense Manager. See [page 205](#) for instructions on identifying groups this way.

Active Directory

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



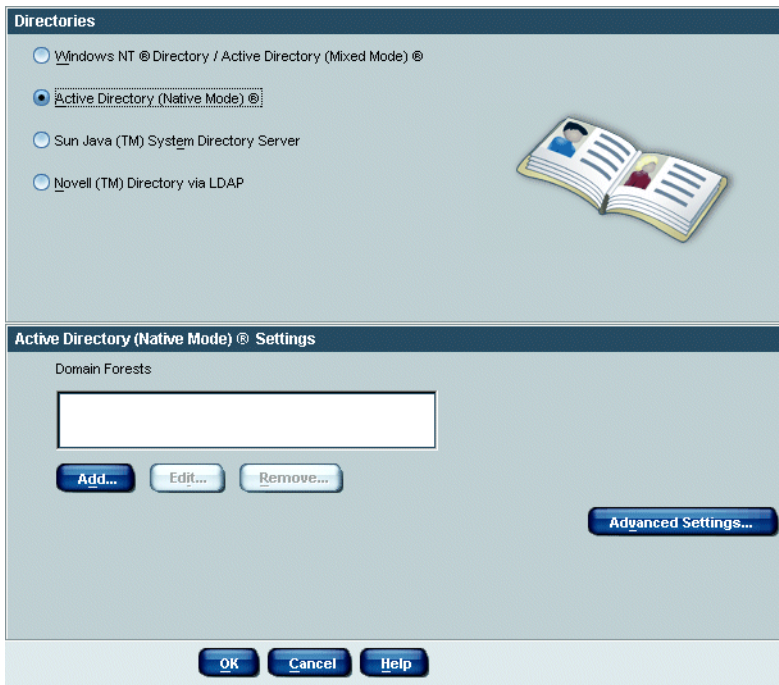
NOTE

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 for instructions. The Knowledge Base is located at <http://www.websense.com/global/en/SupportAndKB/>.

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

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

2. In Websense Manager, choose **Server** > **Settings**. The **Settings** dialog box appears.
3. Select **Directory Service** at the left. The directory service options are displayed.



Directory Service settings

4. Select **Active Directory**.
5. Add Global Catalog Server as a domain forest.
 - a. Click **Add**. The **Domain Forest** dialog box appears.
 - 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

With transparent user identification enabled, it is recommended not to 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 one domain at a time.

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

Domain Forest dialog box

- 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.

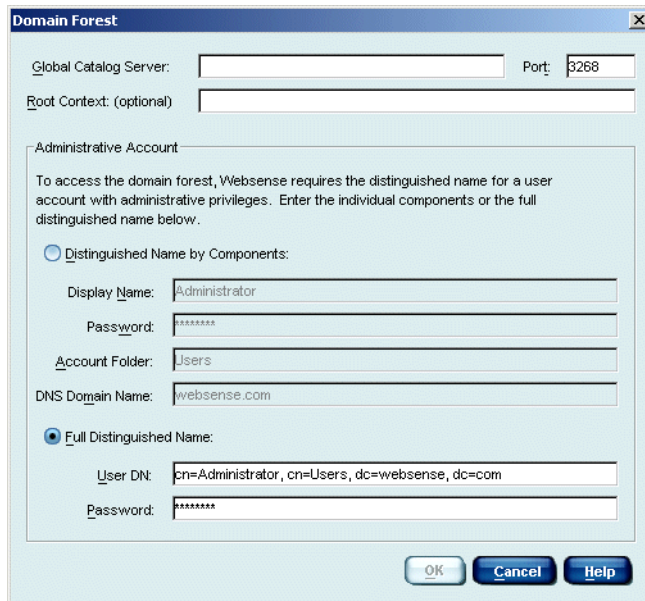
Enter the DN components separately in the **User Name**, **Account Folder** and **Domain Name** fields.



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 one string in the **User DN** field, as shown in the following example.



Domain Forest dialog box, with Full Distinguished Name

- 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 ID Attribute: sAMAccountName

First Name Attribute: givenname

Last Name Attribute: sn

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

Group Attribute: cn

Group Search Filter: objectclass=group

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

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

SSL

Use SSL

Character Set

UTF-8 MBCS

OK Cancel Help

Advanced Directory Settings dialog box

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 Socket 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 Websense software to use a character set other than the options available, please contact Websense Technical Support for assistance.

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 by following the instructions in *Chapter 5 Clients*.

Additionally, you may need to configure Websense software to recognize custom object class types. See *Custom Object Class Types*, page 205.

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. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Directory Service** at the left.
3. Select **Sun™ Java System Directory Server**.

Directories

Windows NT Directory / Active Directory (Mixed Mode) ®

Active Directory (Native Mode) ®

Sun Java (TM) System Directory Server

Novell (TM) Directory via LDAP

Sun Java (TM) System Directory Server Settings

Server Port

Administrator DN

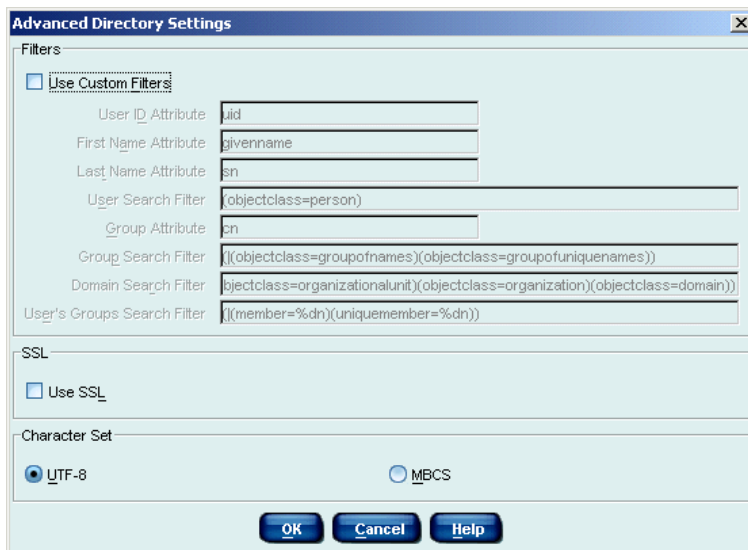
Root Context

Password

[Advanced Settings...](#)

Directory Service settings

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 dialog box

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 Socket 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 Websense software to use a character set other than the options available, contact Websense Technical Support for assistance.

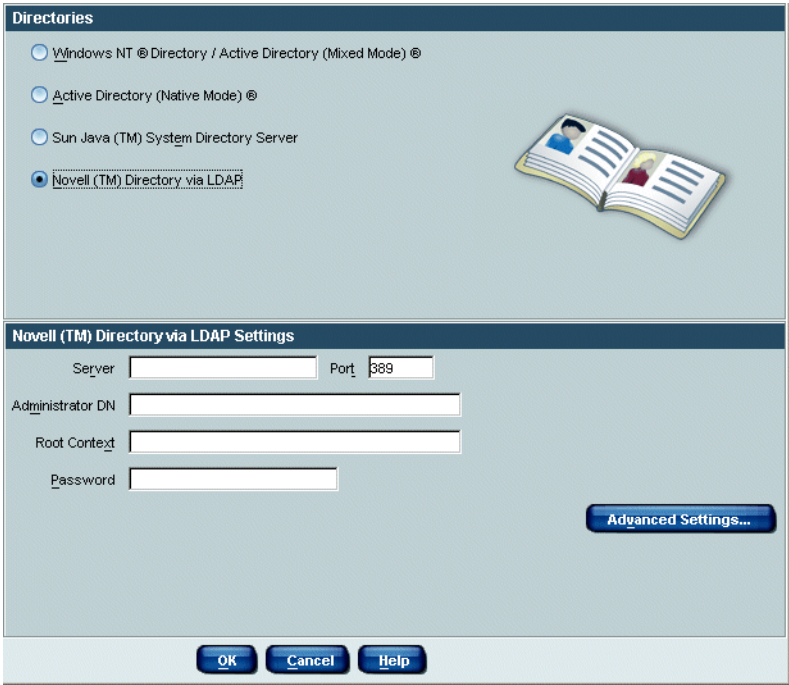
9. Click **OK** to close the **Advanced Directory Settings** dialog box.
10. Click **OK** to close the **Settings** dialog box and activate your changes.
11. Close Netscape Certificate Management System, and stop User Service. For instructions on stopping a Websense Service, refer to [Stopping or Starting Websense Services](#), page 217.

12. Move both database files to the **Policy Server** directory. If prompted, overwrite any existing files.
13. Restart User Service.
14. Add the objects in your Sun Java System directory to Websense Manager by following the instructions in *Chapter 5 Clients*.
15. 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.
16. Enable Websense manual authentication so that if Websense software is not able to identify users transparently, it can prompt users for directory authentication (see [page 208](#) for instructions).
Additionally, you may need to configure Websense software to recognize custom object class types. See *Custom Object Class Types*, [page 205](#).

Novell eDirectory

Follow these instructions to configure Websense software to access the Novell directory service. (This configuration is saved to the Websense Policy Server, and User Service inherits the settings.)

1. In Websense Manager, choose **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**.



The screenshot shows a dialog box titled "Directories" with four radio button options. The "Novell (TM) Directory via LDAP" option is selected. Below this is a section titled "Novell (TM) Directory via LDAP Settings" with several input fields: "Server", "Port" (set to 389), "Administrator DN", "Root Context", and "Password". There is an "Advanced Settings..." button and "OK", "Cancel", and "Help" buttons at the bottom.

Directory Service settings

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**. This is 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 dialog box

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 Socket 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 and activate your changes.
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 will prompt users for directory authentication. See [page 208](#) for instructions.

You may need to configure Websense software to recognize custom object class types. See *Custom Object Class Types*, [page 205](#) for information.

Custom Object Class Types

Adding directory objects to Websense Manager in order 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. To do this, edit search filters via Websense Manager.

1. Choose **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 dialog box

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, as shown. (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)]

SSL

Use SSL

Character Set

UTF-8 MBCS

OK Cancel Help

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 apply your changes and close the **Advanced Directory Settings** dialog box.
7. Click **OK** to close the **Settings** dialog box.

You have applied custom object class types to your directory service search filter.

Manual Authentication

There are some situations where a Websense transparent identification agent cannot identify individual users, such as when the user logs on before the agent is started, or when the agent is otherwise not able to send user information to User Service. In these cases, or when an agent is not installed in your network, you can still filter based on individual directory object policies by enabling Websense manual authentication.

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 configured 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.

Prompting users to authenticate allows Websense software to obtain user information, and then filter based on directory object policies. 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, there are two cases where users may not be able to access the internet and are presented with HTTP errors:

1. The user's password fails after three attempts to enter a password. This occurs when the password is invalid.
2. The user clicks **Cancel** to bypass the authentication prompt.

Enabling Websense Manual Authentication

1. Open Websense Manager.
2. Right-click the Policy Server icon, and then choose **Log On to Server**.
3. Enter the password that was established when Policy Server was first connected, and then click **OK**.
4. If you have not already done so, add the directory objects you want to filter individually. See [Directory Service Access](#), page 187.

5. Choose **Server > Settings**. The **Settings** dialog box appears.
6. Select **User Identification** at the left. The user identification server settings are displayed.
7. Select **Prompt user for directory authentication**.

User Identification

Transparent Identification Agents | DC Agent | eDirectory Agent | Logon Agent | RADIUS Agent

Identify users with these transparent identification agents

Server	Port	Type
1.1.1.1	1234	eDirectory
2.2.2.2	2345	eDirectory

Add Edit Delete

If transparent identification methods fail

Do not apply user and group filtering or logging

Prompt user for directory authentication

Default Domain/Context:

OK Cancel Help

Manual authentication setting



MICROSOFT PROXY SERVER USERS

If you select **Prompt user for directory authentication**, you must enable Anonymous authentication within Microsoft Proxy Server. If you have Basic or NT Challenge/Response authentication enabled in Microsoft Proxy Server, do not select this option.

8. 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.
9. Click **OK** to close the dialog box and save your changes.

Websense software is configured to prompt users to log on to a browser.

Server Administration

The Websense Filtering Service interacts with Network Agent and/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 and set filtering options, first add Policy Server to Websense Manager, so the two can communicate (see [page 212](#)). Then you can log on to Policy Server and configure server settings.

Server settings are available via the **Server > Settings** command. Entering information or settings related to the server does not affect filtering settings.

Policy Server configuration starts with specifying database download behavior: See [Configuring a Server, page 215](#) for information on all Policy Server settings.

One or more Policy Servers can be configured from the same installation of Websense Manager. Each Policy Server stores data for all Filtering Services connected to it. In a large organization, it is sometimes desirable to install multiple instances of Policy Server for load-balancing purposes.

If your organization includes multiple administrators (whether you have one or several Policy Servers), the Distributed Administration and Reporting feature allows highly flexible management of clients and filtering settings. It also provides the ability to distribute configuration settings to multiple servers from a central location. This feature is only available with Corporate Editions of Websense. See [Distributed Administration, page 245](#) for more information.

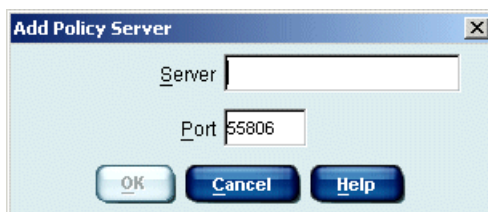
If you are not running Corporate Edition, you can still distribute Websense configuration data to multiple Policy Servers. For information about managing policy configuration data in a multiple-server environment, see [Distributing Policies to Multiple Servers](#), page 287.

Adding a Server

Policy Server cannot be configured until it is added via Websense Manager. To add Policy Server, you must know the IP address or name of the Policy Server machine, which may or may not be the same machine where Websense Manager is installed.

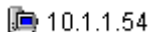
1. Right-click in the Websense Manager navigation tree, and then select **Add Policy Server**.

The **Add Policy Server** dialog box appears.



Add Policy Server dialog box

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.



Server icon

Now you can log on to Policy Server and configure it, or add further instances of Policy Server via Websense Manager. Each Policy Server must be added and configured separately.

Logging On to a Server

After adding a Policy Server, you must log on to it before 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, you must enter your password to connect Websense Manager to the Server. You can change your password as described under *Changing the Policy Server Password*, page 214.



CORPORATE EDITION USERS

It is recommended to use 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 displays as the active **Policy Server** at the top of the Websense Manager 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.



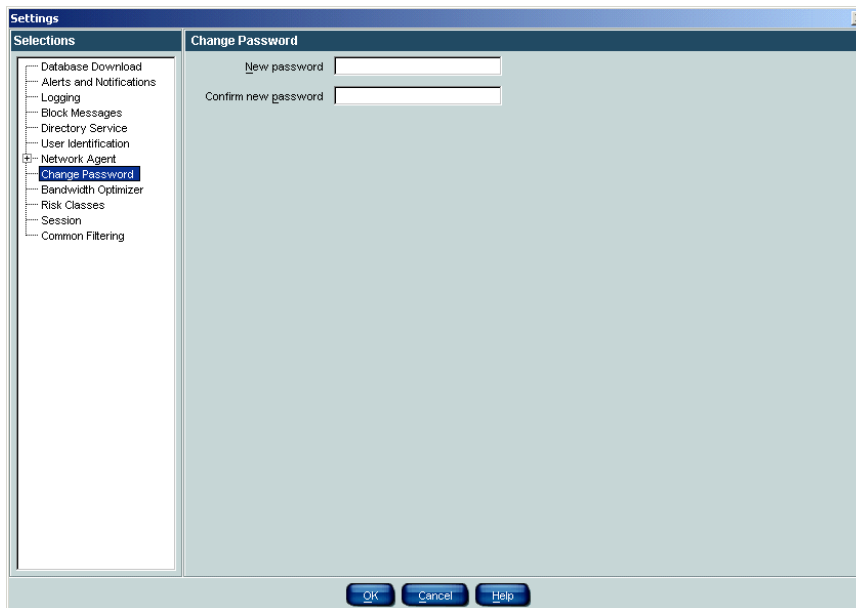
NOTE

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. In Websense Manager, choose **Server > Settings**.
2. Select **Change Password** at the left. The Change Password settings are displayed.



Change Password settings

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**.

The new password you specified is required for logging on to Policy Server.

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 67).
If you have purchased Websense Real-Time Security Updates, enable updates here (see [Websense Real-Time Security Updates](#), page 72).
- ◆ **Alerts and Notifications:** Configure settings for receiving Websense administrative alerts (see [Alerting](#), page 227).
- ◆ **Logging:** Define the location of Log Server, which is installed with Reporter. Log Server must be installed before Websense software can log user requests (see [Logging and Reporting](#), page 79).
- ◆ **Block Messages:** Customize the message displayed when Websense software blocks a requested site (see [Customized Block Messages](#), page 56).
- ◆ **Directory Service:** Configure Websense software to access directory objects in your network (see [Directory Service Access](#), page 187).
- ◆ **User Identification:** Configure User Service to communicate with a transparent identification agent, and prompt users for directory authentication (see [Transparent Identification](#), page 125).
- ◆ **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 85).
- ◆ **Change Password:** Configure the administrative password used to log on to Policy Server (see [Changing the Policy Server Password](#), page 214).
- ◆ **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 [Bandwidth Management](#), page 347).

- ◆ **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 79).
- ◆ **Session:** Configure the length of Policy Server sessions (see [Session Management](#), page 258).
- ◆ **Common Filtering:** Set filtering preferences for:
 - When a user is in multiple groups (see [When Multiple Group Policies Apply](#), page 41)
 - When a subscription expires or is exceeded (see [Subscriptions](#), page 17)
 - Whether Websense can gather protocol usage data about your network (see [Protocol Usage](#), page 102)
 - Where Websense software searches for keywords (see [Keywords](#), page 331)
 - Password override and continue time limits (see [Password Override](#), page 53 and [Continue](#), page 48)
 - Quota session length and default quota time per day (see [Quotas](#), page 49)

When you finish configuring settings, click **OK** to update Policy Server.

Stopping or Starting Websense Services

Websense services are configured to start automatically each time the machine restarts.

However, you might need to stop or start Policy Server, Filtering Service, User Service, or Network Agent separately from a machine restart. For example, a server must be restarted whenever a behind-the-scenes configuration change is made, and after customizing default block messages.



NOTE

If Filtering Service is in the process of downloading the Master Database, it will not stop running until the download is complete.

Follow the instructions in the appropriate section below to stop or start a service.

Windows

1. Open the Windows **Services** dialog box.

Windows NT: Choose **Start > Settings > Control Panel**, and then double-click **Services**.

Windows 200x: Choose **Start > Programs > Administrative Tools > Services**.

2. Right-click the Websense service name, and then choose **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 the following procedure.

1. Go to the `\Websense` directory.
2. Check the status of the Websense services with the following command:
 - `./WebsenseAdmin status`
 - Stop, start, or restart all Websense services with one of the following commands:
 - `./WebsenseAdmin stop`
 - `./WebsenseAdmin start`
 - `./WebsenseAdmin restart`



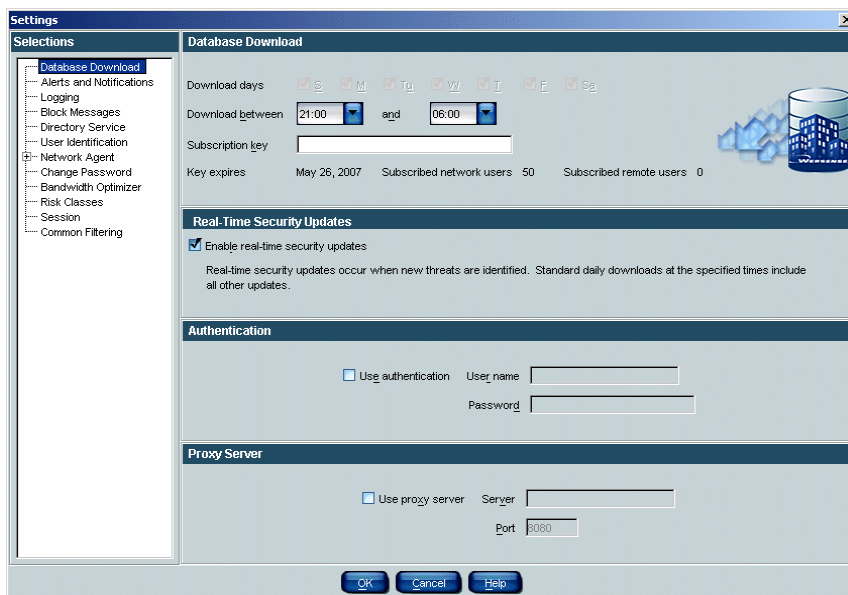
IMPORTANT

Do not use the **kill** command to stop a Websense service, as it may corrupt the service.

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. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Database Download** at the left. The database settings are displayed.



Database Download settings

3. Under **Proxy Server**, check **Use proxy server**.
4. In the **Server** field, 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. In the **Port** field, 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 in order to reach the internet, check **Use authentication**.

The **User name** and **Password** fields are activated.



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** to close the **Settings** dialog box and save your changes.

Removing a Server

Removing a Policy Server from Websense Manager does not uninstall it from the machine where it is installed; it simply removes the Server from Websense Manager's control. The settings remain intact, and the Server can be added again later, if needed, or added to a different installation of Websense Manager.

1. If the Policy Server you want to remove is connected: Right-click the server icon in the navigation tree, and then choose **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 choose **Remove Policy Server** from the shortcut menu.
3. Choose **Yes** when prompted to confirm the delete request.

The selected Policy Server is removed from Websense Manager.

Saving the Configuration

All server configuration and policy settings are stored in the **config.xml** file in the Websense installation directory. After making changes to 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, the **config.xml** file is updated every 30 seconds or every 500 transactions, whichever comes first. Between **config.xml** updates, each transaction is stored in a binary file named **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 for troubleshooting or restoration purposes in case Policy Server doesn't start normally.

Before upgrading Websense software, it is recommended that you back up the configuration file so that settings are not lost in case of a power outage or other problem during the upgrade process.



IMPORTANT

When upgrading Websense components, take extra care to back up all related .ini files. Please refer to your installation guide for complete upgrade instructions.

Backing Up the Configuration File

1. Stop Policy Server (see [Stopping or Starting Websense Services, page 217](#)).
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 217](#)).

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 217](#)).
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 automatically. Websense software detects IP address changes for machines where its components reside, and automatically adjusts so filtering continues uninterrupted. For example, if the IP address of the machine running Policy Server changes, a behind-the-scenes broadcast system activates to inform 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, please 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 217](#) for instructions.

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 [page 182](#) for instructions).

Network Agent

When an IP address on the Network Agent machine is changed, be sure to:

- ◆ Restart the Websense Network Agent service in order for Websense software to recognize the change. The service should be restarted regardless of where Network Agent is installed in relation to other Websense components.
- ◆ Exit and then start Websense Manager. This ensures that Websense Manager displays the updated address information.



IMPORTANT

Changing an IP address (or Network Interface Card and IP address) on the Network Agent machine may require that you update the Network Agent configuration.

Changing the IP address of any *proxy/cache machine* in your network requires that you configure Network Agent to recognize the new IP address. See [Initial Configuration, page 85](#) for instructions.

When Network Agent resides on a multiple-NIC machine that is separate from Filtering Service, you must update the **websense.ini** file, and then restart the Network Agent service to reflect an IP address change.

To update the Network Agent machine's IP address configuration:

1. Stop the Websense Network Agent service (see [Stopping or Starting Websense Services](#), page 217 for instructions).
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.

Network Agent is configured to recognize the IP address change.

Policy Server

If you change the IP address of Policy Server, do the following:

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 212).
3. Remove the old Policy Server from Websense Manager (see [page 212](#)).

If the Policy Server machine has multiple NICs, you must *also* update the **websense.ini** file to reflect any change in IP address, as follows.

1. Stop the Websense Policy Server (see [Stopping or Starting Websense Services](#), page 217 for instructions).
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 specifically 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, do the following:

1. Stop the Websense Policy Server (see [Stopping or Starting Websense Services](#), page 217 for instructions).
2. Update the Policy Server IP address in *each* of these two 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:
 - d. `PolicyServerIP = <IP address>`
 - e. where `<IP address>` is the new IP address of the machine running Policy Server.
 - f. Save the file.
3. Start the Websense Policy Server.

The Web-based Manager is updated to recognize the new IP address.

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. Consult your integration product documentation for information before changing the IP address on a machine running a plug-in.

Alerting

To facilitate tracking and management of both Websense system and user internet activity, Websense software can alert administrators when selected events occur.

Two types of auto-generated alerts are available:

- ◆ **System alerts:** Notification regarding subscription status, Websense Master Database activity, or administrator lockouts (see [Lockouts](#), page 260).
- ◆ **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 three modes:

- ◆ Email
- ◆ Onscreen (Windows net send messaging)

**NOTE**

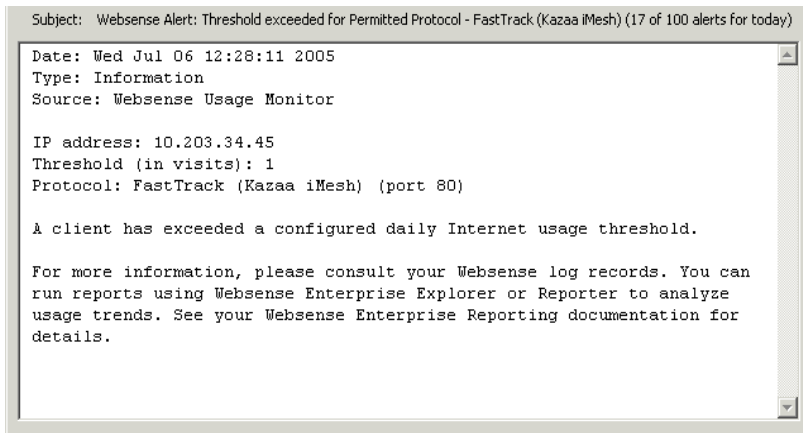
Onscreen alerts cannot be sent to machines running Linux or Solaris. However, they can be sent from a Linux/Solaris machine running Policy Server to Windows machines, provided that the Samba client is installed on that Linux/Solaris machine.

- ◆ SNMP messaging

**IMPORTANT**

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.



Sample email alert

Alerts can be generated for the Websense categories or protocols provided by default, or for custom categories you have added. See [Adding a Custom Category, page 328](#) for information about custom categories.

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 certain 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 one 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).

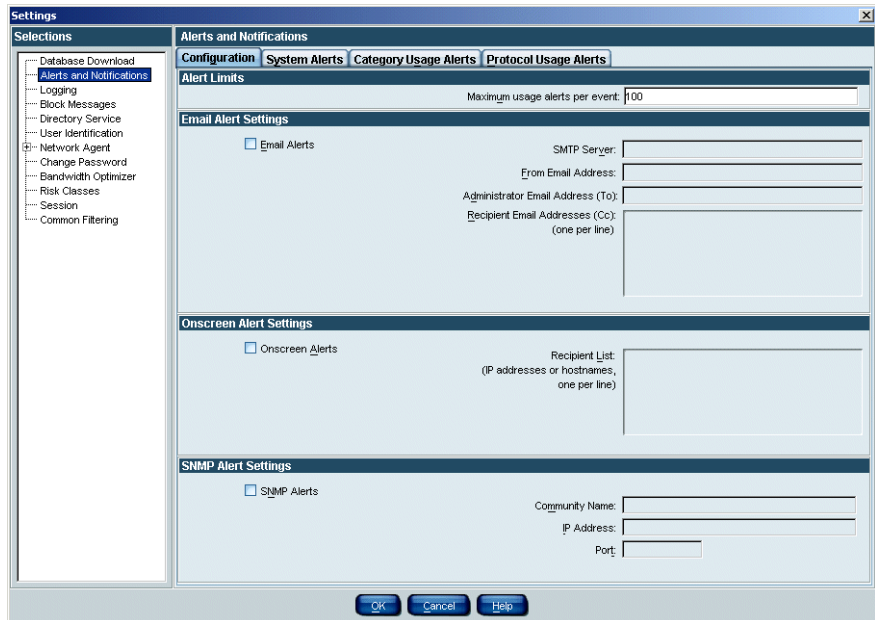
See the next section for instructions on setting these alert limits.

Setting Up Alerting

If you are running a Corporate Edition of Websense, you must have Super Administrator access to Websense Manager in order to set up Websense alerting. A Super Administrator can configure alerts to be sent to any other Websense administrator. See [Administrator Roles, page 247](#) for information about administrative permissions.

If you are running a standard edition of Websense, the first administrator to install Websense software has access to set up alerting.

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Alerts and Notifications** at the left. The alerting global settings are displayed.



Alerts and Notifications global settings

3. For **Maximum usage alerts per event**, specify the maximum number of usage alerts an administrator will 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 will only be 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 settings 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:** Enter the name for the trap community on your SNMP Trap server.
 - **IP Address:** Enter the IP address of the SNMP Trap server.
 - **Port:** Enter the port SNMP messages should use.
10. Go to the **System Alerts** tab to configure system alerts.

Alerts and Notifications

Configuration System Alerts Category Usage Alerts Protocol Usage Alerts

System Alert Conditions

Event	Email	Onscreen	SNMP
The number of users reaches 90% of your subscription level	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Changes have been made to the Websense Master Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administrator locked out after three attempts to log in	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The number of users on your subscription is exceeded	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your subscription expires in one week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Database downloads fail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
An administrator is locked out from Policy Server due to logon failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your subscription expires in one month	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel Help

System alert settings

- For each system event you want to enable alerts for, check the alerting modes to activate for that event. You can select one, two or three 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).

- Go to the **Category Usage Alerts** tab to configure usage alerts for URL categories.

Alerts and Notifications

Configuration | System Alerts | **Category Usage Alerts** | Protocol Usage Alerts

Select a threshold for triggering an alert. A maximum of 9999 alerts will be published for each event.
To edit the alert limit, select the Configuration tab.

Blocked Category Usage Alerts

Category	Occurrence	Email	Onscreen	SNMP
Security PG	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security PG:Phishing and Other Frauds	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adult Material:Nudity	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bandwidth PG:Peer-to-Peer File Sharing	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information Technology:Proxy Avoidance	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information Technology:Hacking	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security PG:Keyloggers	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Illegal or Questionable	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add Category ... **Delete**

Permitted Category Usage Alerts

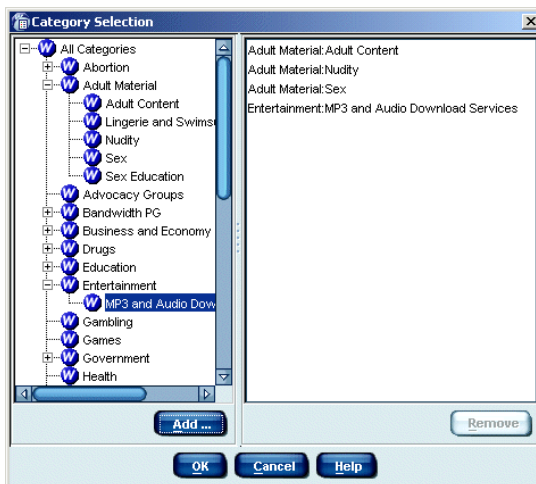
Category	Occurrence	Email	Onscreen	SNMP
Bandwidth PG	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Job Search	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Miscellaneous:Uncategorized	20 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add Category ... **Delete**

OK **Cancel** **Help**

Category usage alert settings

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 one or more categories at the left, and then click **Add**. The selected categories appear at the right.



Category Selection dialog box with categories selected



NOTE

To remove a category from the list, select the category and then click **Remove**.

15. Click **OK**.
16. For each category, specify the following:
 - How many occurrences will 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 one 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 the following:
 - How many occurrences will cause an alert to be generated.
 - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).

21. Go to the **Protocol Usage Alerts** tab to configure usage alerts for protocols.

**NOTE**

Alerts will only be generated for protocols that are logged. See [Editing a Protocol Set, page 357](#) for how to enable logging for protocols.

Alerts and Notifications

Configuration System Alerts Category Usage Alerts **Protocol Usage Alerts**

Select a threshold for triggering an alert. A maximum of 9999 alerts will be published for each event.
To edit the alert limit, select the Configuration tab.

Blocked Protocol Usage Alerts

Protocol	Occurrence	Email	Onscreen	SNMP
P2P File Sharing:FastTrack (Kazaa iMesh)	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2P File Sharing:Gnutella (Morpheus Xolox)	5 Times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add Protocol ... Delete

Permitted Protocol Usage Alerts

Protocol	Occurrence	Email	Onscreen	SNMP
----------	------------	-------	----------	------

Add Protocol ... Delete

OK Cancel Help

Protocol usage alert settings

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 one or more protocols at the left, and then click **Add**. The selected protocols appear at the right.

**NOTE**

To remove a category from the list, select the category and then click **Remove**.

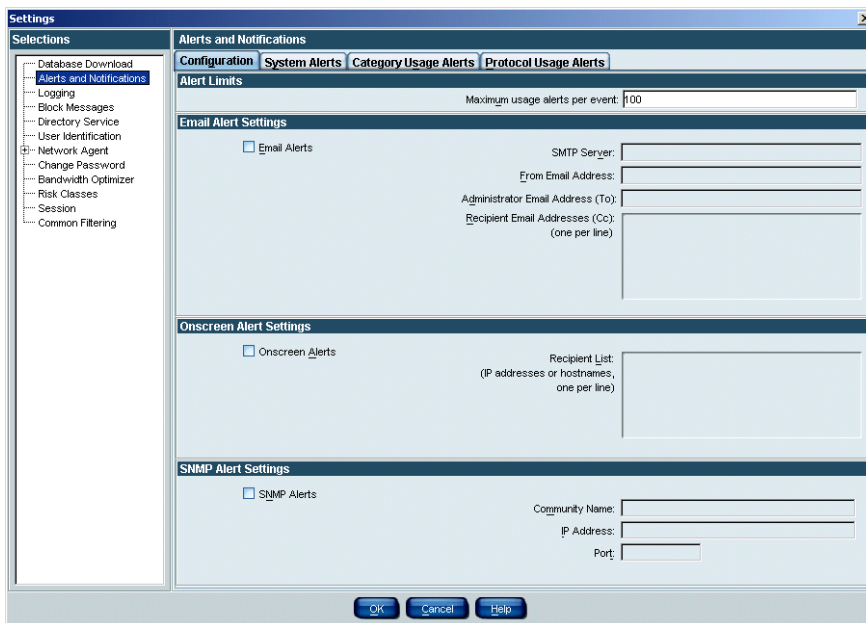
24. Click **OK**.
25. For each protocol, specify the following:
- How many occurrences will cause an alert to be generated.
 - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).
26. Under **Permitted Protocol Usage Alerts**, click **Add Protocol** to set up an alert for protocols that are permitted in policies.
27. In the **Protocol Selection** dialog box, select one 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 the following:
- How many occurrences will cause an alert to be generated.
 - Which alerting modes to enable (**Email**, **Onscreen**, or **SNMP**).
30. Click **OK** to close the **Settings** dialog box.

Alerts are configured to be sent as specified.

Disabling Alerting

To disable one or more alerting modes:

1. In Websense Manager, choose **Server > Settings**.
2. Select **Alerts and Notifications** at the left. The alerting global settings are displayed.



Alerting global settings

3. Uncheck the alert mode you want to disable (**Email Alerts**, **Onscreen Alerts**, or **SNMP Alerts**).
4. Click **OK**.

Alerts will no longer be sent via the mode or modes you have disabled.

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 only available with Corporate Editions of Websense.

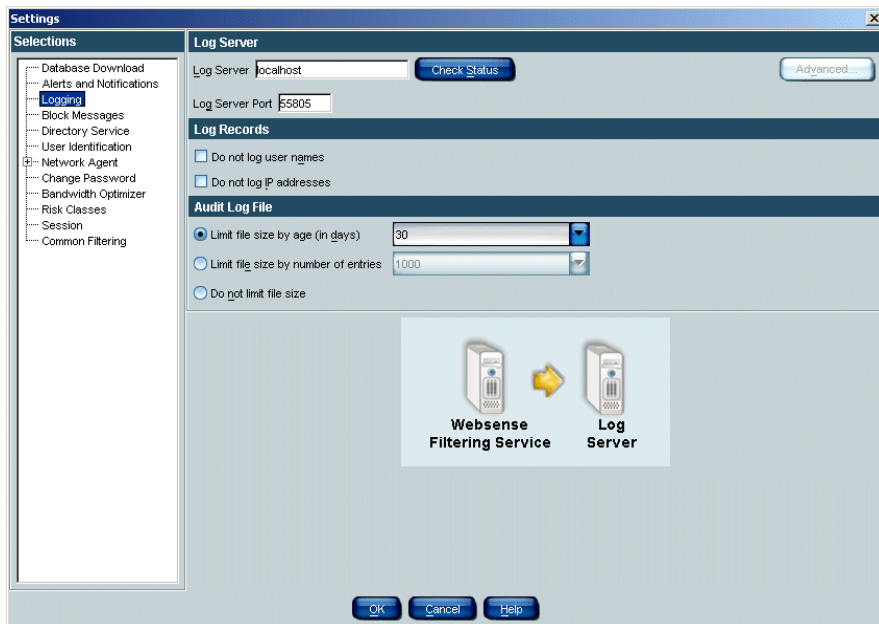
The audit log is only accessible by Super Administrators, and not by Delegated or Remote Administrators without full administrative access. See [Administrator Roles](#), page 247 for information about administrative roles.

For each change, the audit log indicates the following:

- ◆ 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. In Websense Manager, choose **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.



Audit log settings

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

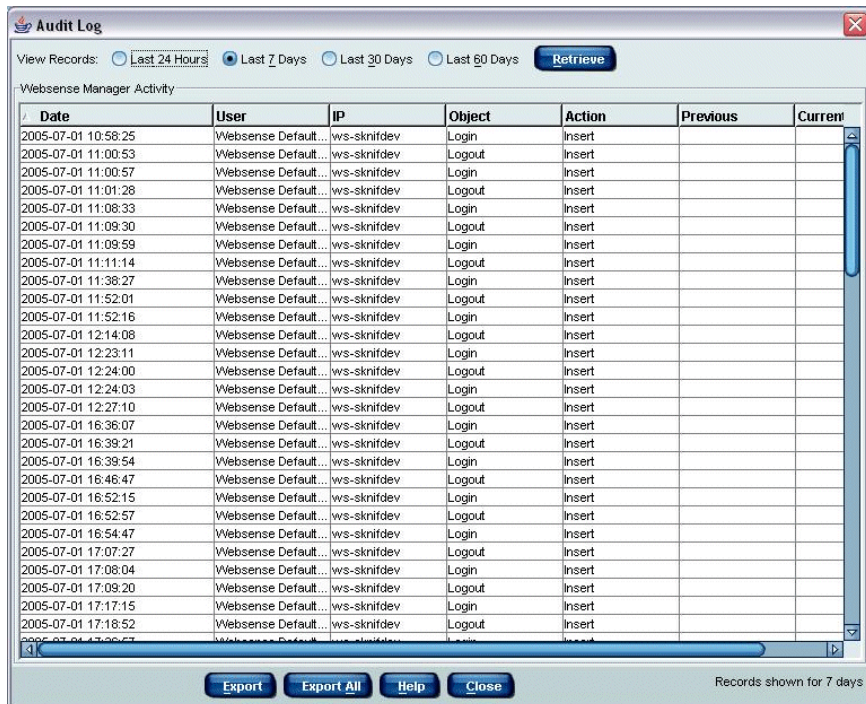
If you have an integration product running on the same machine as Websense software, it is recommended to limit the audit log file to a smaller number of entries (500 or fewer).

4. Click **OK**.

Access the audit log from Websense Manager, and optionally export the log to an encrypted external file.

To view the audit log:

1. Choose **Actions > View Audit Log**. The **Audit Log** dialog box appears.



Audit Log dialog box.

2. Next to **View Records** at the top of the dialog box, select the time period for which you want to view records.
3. Double-click on a column heading to sort records by the criterion for that column.



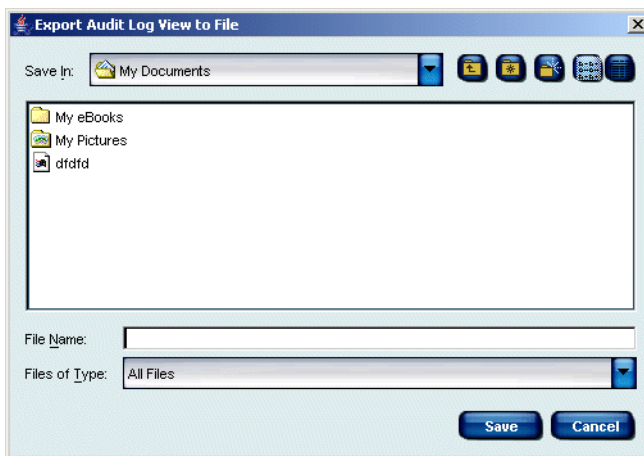
NOTE

If a policy is only renamed, the audit log displays two entries: one for deletion of the original policy, and another 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* in the dialog box.

To export the entire log, click **Export All**.

The **Export Audit Log View to File** dialog box appears.



Export Audit Log View to File dialog box

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 to the location you specified, 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.

Distributed Administration and Reporting

Websense Distributed Administration and Reporting provides flexibility in managing internet filtering and reporting and across multiple sites or Policy Servers. See [Chapter 8 Distributed Administration](#) for details about this feature.



IMPORTANT

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, Distributed Administration and Reporting allows greater flexibility in maintaining unique configurations for multiple servers. It adds the ability to 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 287.

For information on central configuration distribution with Websense Enterprise Corporate Edition, see [Distributing Configuration Settings](#), page 271.

Removing Websense

Use this procedure to remove installed components. Removing components in any other way may hinder configuration or installation.



IMPORTANT

Policy Server service must be running to uninstall any Websense components. To remove Policy Server, you must also remove all the other components installed on the machine.

1. Log on to the installation machine with **local** administrator privileges (*Windows*).
2. Close all open applications.
3. Run the main Websense installation program (**Setup.exe**).

After the welcome screen, the **Add/Remove/Repair** dialog box is displayed asking you what action you want to take with the installed Websense components.

4. Select **Remove Websense Components**, and click **Next**.

A list of installed components is displayed. By default, all selections are checked.

5. Clear the check boxes of the components you do *not* want to remove, and click **Next**.

If Policy Server is not running, a dialog box is displayed advising you that removing Websense components may require communication with Policy Server. You may exit the installer to restart Policy Server or continue uninstalling the selected components.

If you are uninstalling Network Agent on a remote machine after removing Policy Server, the process may take several minutes. Network Agent will be successfully uninstalled, although no progress notification will be displayed.

A summary list is displayed of the components you have elected to remove.

6. Click **Next** to begin uninstalling the components.
A completion message advises you when the procedure is finished.
7. Click **Next** to exit the installer.

Websense software is removed from the machine.

Distributed Administration

The Distributed Administration and Reporting feature provides powerful, flexible methods for managing internet filtering and reporting for particular groups of clients, and across multiple locations.



IMPORTANT

This feature is available only with Corporate Editions of Websense. If you are running a standard version of Websense, you can customize *reporting roles and permissions only*. Contact Websense, Inc. for information on upgrading.

Distributed Administration and Reporting allows you to customize filtering behavior through the use of configurable roles and permissions for both clients and administrative users. This functionality provides greater granularity in employee internet access, plus additional layers of security against unwanted or invasive internet content.

One *Super Administrator* can set up filtering restrictions from a central location, and then distribute those to multiple locations. This Super Administrator can optionally grant limited administrative rights to other administrative users. These *Delegated Administrators* manage employee internet use in a more limited fashion. The Super Administrator can also customize access levels for *Remote Administrators*, administrative users for remote locations.

Whether your organization includes only one additional site, or several sites, you can assign administrative users as needed to manage policies appropriately at each site.

Distributed Administration and Reporting also allows 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 Distributed Administration

Implementing a distributed filtering environment involves several steps, outlined here. The Websense Manager configuration interface makes this process simple and flexible.

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 certain configuration settings with other Policy Servers (see *Central Configuration Distribution*, page 269).

To set up your distributed filtering environment, you will need to do the following:

- ◆ Determine which site will act as the central site and house the central Policy Server.
- ◆ Define additional Policy Servers in Websense Manager as needed (see *Adding a Server*, page 212).
- ◆ Ensure that users and groups in your directory service are added to Websense Manager as directory objects (see *Adding Directory Objects*, page 107).
- ◆ Designate a Super Administrator (see *Administrator Roles*, page 247).
- ◆ Create roles to group similar clients and administrative permissions (see *Creating a Role*, page 252).
- ◆ Specify the Delegated Administrators or Remote Administrators for the role (see *Assigning an Administrative Role*, page 254).
- ◆ Add the clients who will be managed by the administrator in each role (see *Adding Clients to an Administrative Role*, page 255).
- ◆ Configure filtering settings for the role by creating a Web Filter Lock (see *Defining Filtering Restrictions*, page 261).
- ◆ Distribute the Web Filter Lock to other sites (see *Distributing Configuration Settings*, page 271).
- ◆ Allow the Delegated or Remote Administrators to maintain additional filtering settings as needed at their sites.

To facilitate client and policy maintenance by multiple administrators, Websense software features built-in Policy Server session management. This prevents one administrator from overwriting configuration changes made by another administrator. See *Session Management*, page 258 for information on running multiple instances of Websense Manager.

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 as needed.



NOTE

In the unlikely event that the Websense Master Database was not downloaded during installation, then the first user to log on to Websense Manager can only view and configure reporting roles.

Administrator Roles

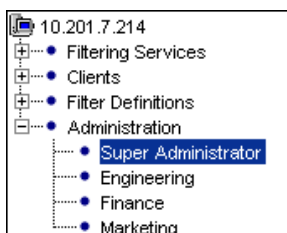
Assigning roles to all administrative users is a good way to organize who has administrative access, and what level of access each user has. Roles also facilitate tracking of administrative actions.

You can track administrative actions via the Auditing feature (see [Administrative Auditing](#), page 237). 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 one 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, as shown.



Roles in the navigation tree

Roles make it easier to maintain filtering policies specific to departments or areas in your organization. As clients change departments or new clients arrive, filtering policy assignments remain intact because they are managed at the role level.

Before creating additional roles, ensure that at least one Super Administrator has been designated. To accomplish this, add the primary administrative user to the Super Administrator role, as follows:

1. In the Websense Manager 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 124.
4. Click **OK**.

The Super Administrator has been designated.



IMPORTANT

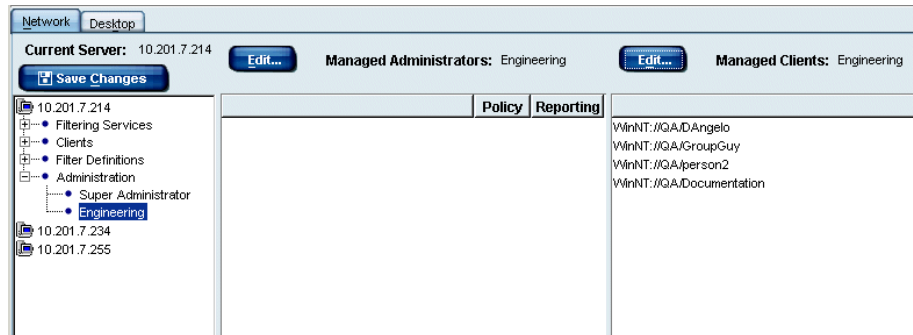
Default filtering settings configured by a Super Administrator are automatically copied over when new administrative roles are created. To define global settings up-front, edit the **Default Settings** category set and protocol set as desired *before* setting up roles. See [The Global Policy](#), page 279 for more information.

Managed Clients

Each administrative role has an associated Managed Clients list. Any administrator in a particular administrative role has the ability to define internet access for those Managed Clients.

For example, you set up administrative roles for the Engineering, Finance and Marketing departments in your organization, and designate a Delegated Administrator for each role. Then you 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:



Users assigned the Engineering role

To simplify administration of users:

- ◆ Create roles corresponding to certain areas of your organization;
- ◆ Add one 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 124).



NOTE

If you plan to change to a different directory service, implement that change before assigning roles. Otherwise, directory objects will have 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 [page 247](#)) or Super Administrator to modify administrative roles.



NOTE

Role creation and management is only available with Corporate Editions of Websense.

View and configure roles in any of the following ways:

- ◆ If you are not already logged on to Policy Server: Double-click the Policy Server IP address, enter the Websense administrative password, and then select a role to administer in the **Select Role** dialog box.
- ◆ Expand **Administration** in the navigation tree, and then select the desired role.
- ◆ From the **Current Role** list box (in the upper right-hand corner of Websense Manager), select the desired role.

When you create a role, specify how users in that role will be managed by associating the following items with the role:

- Clients to be managed by the administrator for the role (see *Managed Clients*, page 249);
- The Delegated Administrator who will create and manage filtering policies governing clients in the role;
- Which elements of policies that Delegated Administrator can modify;
- Which clients that administrator can include in reports (all clients, or only clients in a particular role).



NOTE

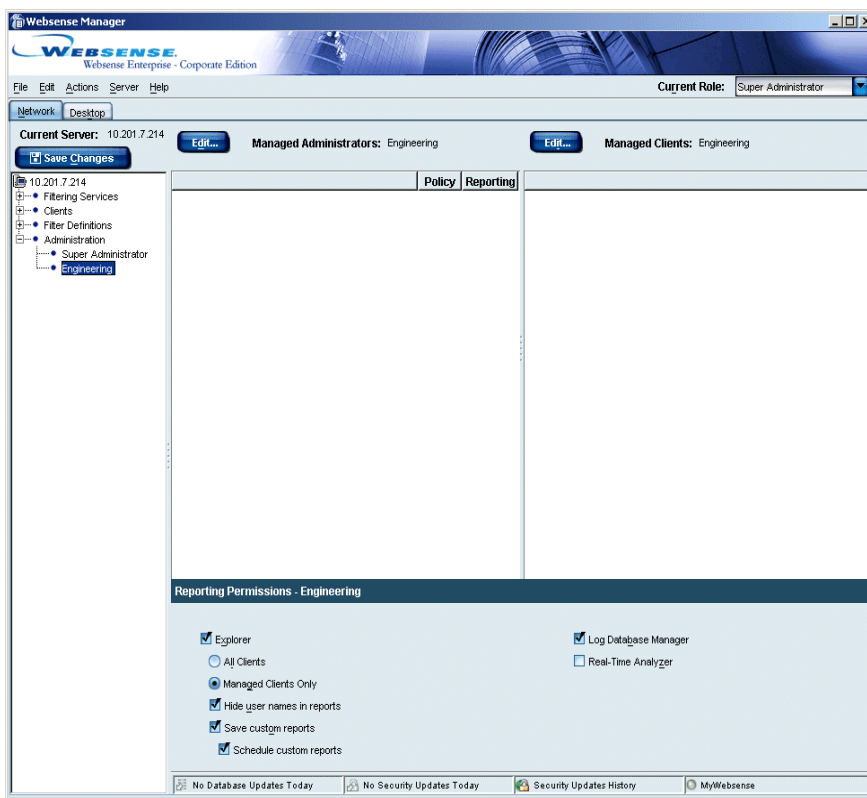
Configurable reporting permissions are available even if you have not purchased a Corporate Edition of Websense.

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 Websense Manager navigation tree, and then choose **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.
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 details in the content pane

4. Under **Reporting Permissions - [role name]** at the bottom of the content pane, specify reporting rights for administrators in this role.
 - Check **Explorer** to allow Delegated Administrators in this role to generate reports using Websense Enterprise Explorer. (See the Websense Enterprise Reporting documentation for more information.)
 - Select **All Clients** to allow administrators in this role to report on all clients added to Websense Manager. Or, select **Managed Clients Only** to restrict reporting only to clients in this administrators role.

**NOTE**

Selecting **All Clients** here gives Delegated Administrators the ability to see and report on all clients, even those outside the roles they manage.

- Check **Hide user names in reports** to make report entries anonymous in reports these administrators run.
 - Check **Save custom reports** to allow these administrators to create and save report criteria for repeated use.
 - Check **Schedule custom reports** to allow these administrators to set Favorite reports to run in Explorer.
 - Check **Log Database Manager** to allow these administrators to use Log Database Manager to manage log database contents (see your Reporting documentation).
 - Check **Real-Time Analyzer** to allow these administrators to access Real-Time Analyzer (see [Chapter 11 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

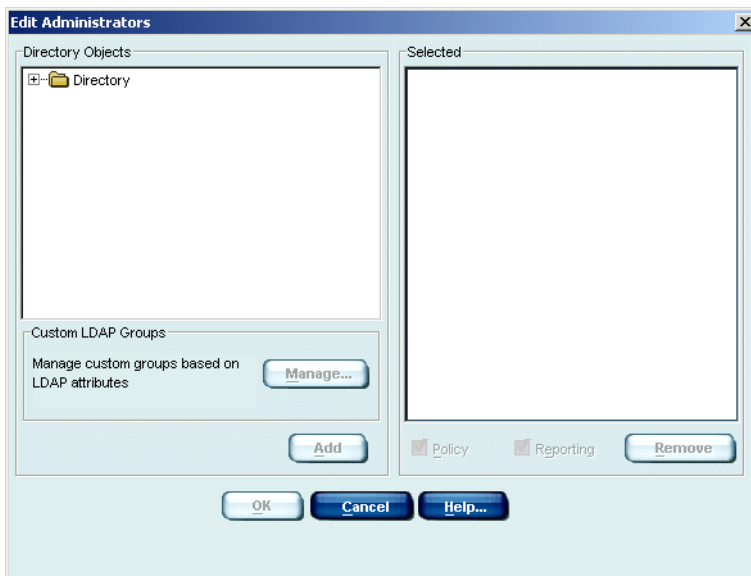
As a Super Administrator, you can designate who administers various roles in your organization. The users you designate become Delegated Administrators for those areas.



NOTE

If you plan to change to a different directory service, implement that change before assigning roles. Otherwise, directory objects will have to be re-added and roles re-assigned after the change.

1. In the Websense Manager navigation tree, expand **Administration**.
2. Select the role you want 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.



Edit Administrators dialog box

4. Select the directory object you want to add as an administrator. For help with custom LDAP groups, see [Adding Directory Objects](#), page 107.

**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 role.
7. Optionally check **Reporting** to enable this administrator to run internet usage reports.
8. Click **OK**.

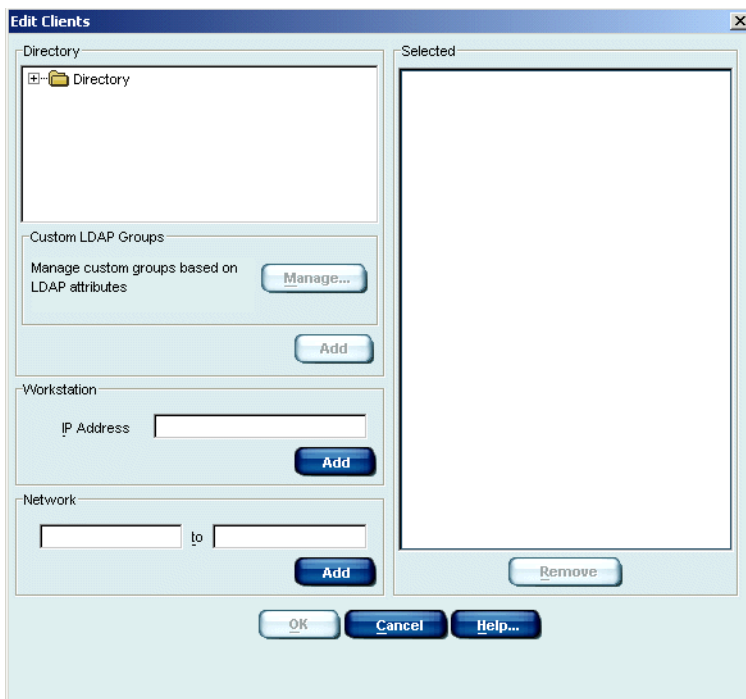
The administrator you added is a Delegated Administrator for the selected role.

Adding Clients to an Administrative Role

The clients you associate with an administrative role are managed by the administrators designated to the same role.

To associate clients with a role to be managed collectively:

1. In the Websense Manager navigation tree, expand **Administration**.
2. Select the role you want 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.



Edit Clients dialog box

4. Select the client object (directory object, workstation or network) you want to assign this role.

For help with custom LDAP groups, see [Adding Directory Objects](#), page 107.



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**.

The added clients appear under **Managed Clients** in the content pane when the associated role is selected in the navigation tree.

Removing an Administrator from a Role

If you no longer need an administrator for a particular role, or need to change who administers that role, use the following procedure to remove an administrator.

1. In the Websense Manager navigation tree, expand **Administration**.
2. Select the role from which you want 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 you want to remove.
5. Click **Remove**.
6. Click **OK**.

The removed user no longer has administrative rights for the selected role.

Administrative roles also serve to define which clients an administrator manages. Assigning the same role to a Delegated Administrator and the clients that Delegated Administrator manages simplifies policy configuration and maintenance in your organization.

Session Management

To allow streamlined administration of Policy Servers and prevent configuration conflicts, the Distributed 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 optionally can be set to as long as four 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, as shown:



Session warning message

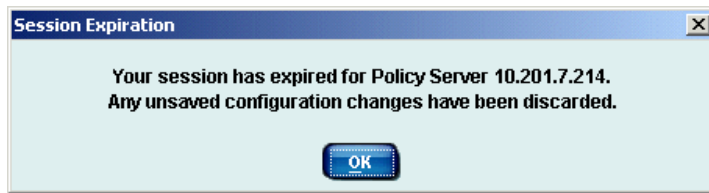
At this time, the logged-on administrator can click **Continue** and keep working. If the session remains inactive, the administrator is logged off automatically, and informed that his session has ended. As soon as the session ends, another administrator can log on.



IMPORTANT

To ensure that configuration settings are preserved as you are working, click **Save Changes** above the navigation tree.

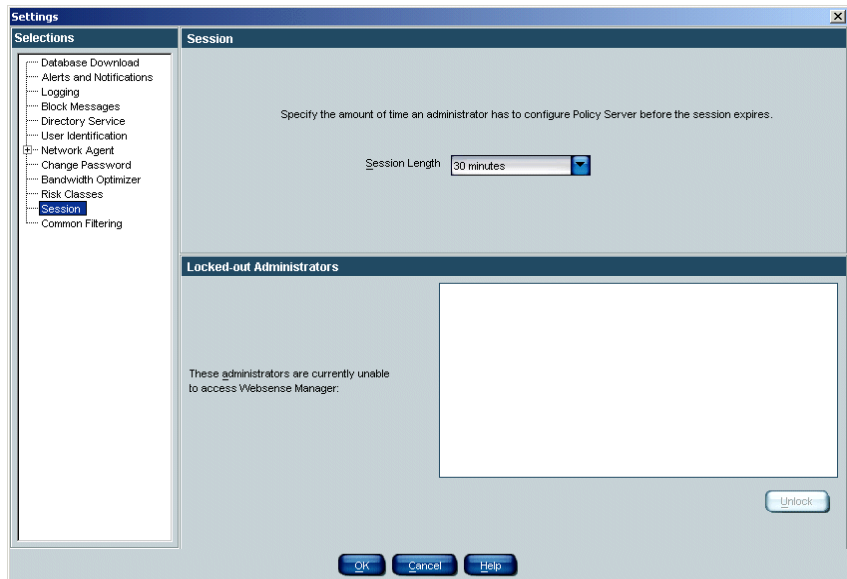
After a session has expired, the administrator has been logged off from Policy Server, and must log on again to continue working.



Session expiration message

To change the Policy Server session length:

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Session** at the left. The session settings are displayed.



Session settings

3. Select the desired session length value from the drop-down list.
4. Click **OK**.

Policy Server sessions for the current Policy Server expire automatically 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), you must restart the Websense Policy Server and Websense Filtering Service in order to restart Manager. See [Stopping or Starting Websense Services](#), page 217.

Lockouts

An administrator is locked out from using Websense Manager after the administrator makes three failed attempts to log on to Policy Server.

When an administrator is locked out, only the Super Administrator can reset the lockout and allow logon. If a Super Administrator is locked out, then another Super Administrator must reset the lockout.

If there is only one Super Administrator and this user has been locked out, contact Technical Support for assistance (see [Websense Technical Support Services](#), page 409).

To reset a lockout:

1. In Websense Manager, choose **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.

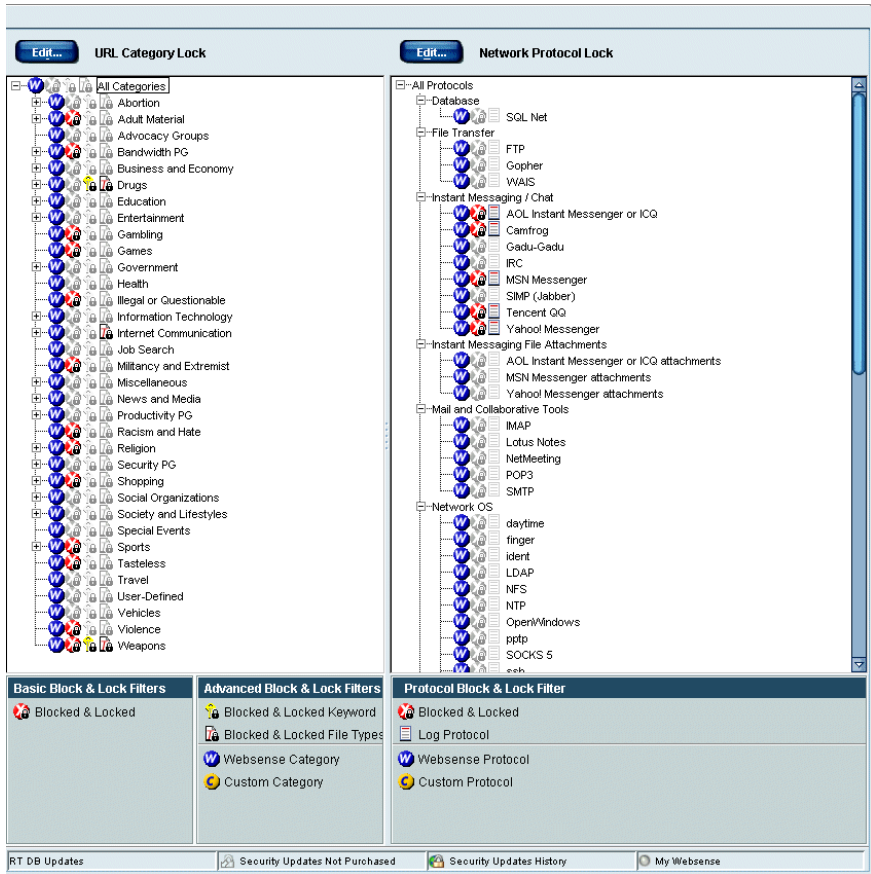
Defining Filtering Restrictions

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. See *Central Configuration Distribution*, page 269 for information about distributing settings to other servers.

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.



Web Filter Lock as seen by Delegated Administrator

Block settings applied and locked by the Super Administrator are indicated by a small lock icon, as shown. Filtering settings exhibiting this icon are not modifiable by Delegated Administrators.



Icon for URL category blocked and locked by Super Administrator



Icons for keywords or file types blocked and locked by Super Administrator



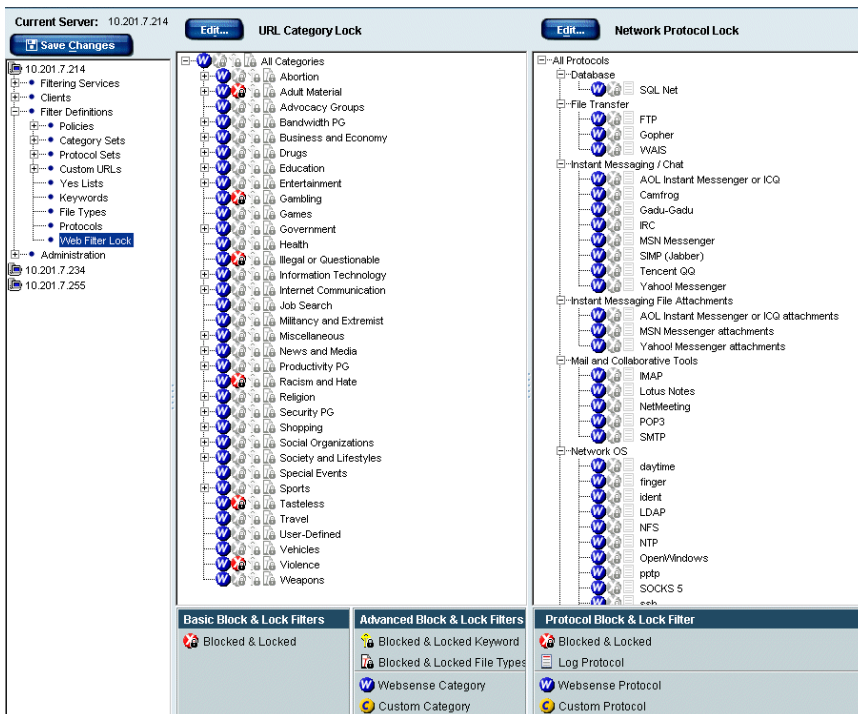
Icon for protocol blocked and locked by Super Administrator

This section describes how to create a Web Filter Lock. For detailed information on configuring Websense filtering settings, see [Chapter 9 Setting Up Web Filtering](#).

Creating a Web Filter Lock

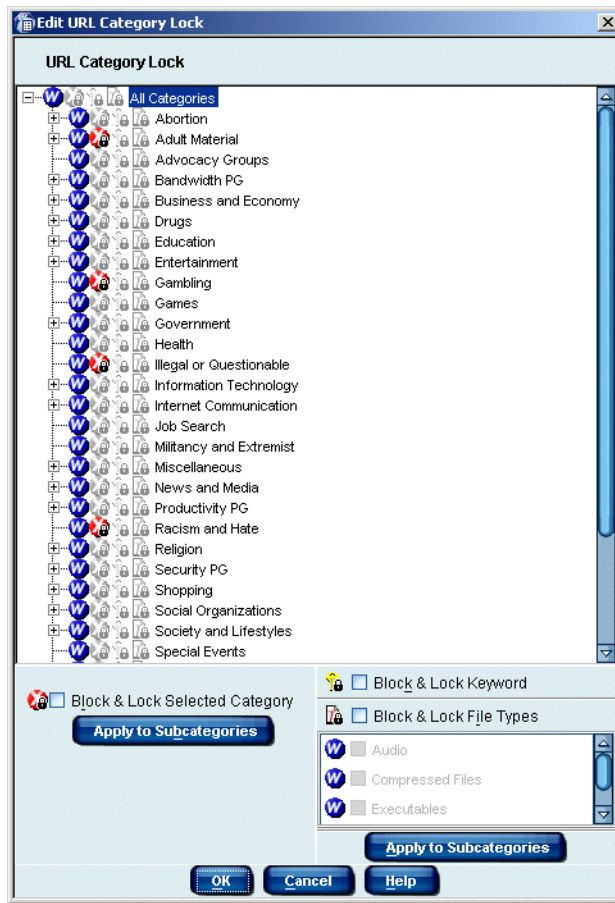
Use the following procedure to create a Web Filter Lock for use by Delegated Administrators, or distribution to remote Policy Servers.

1. In the Websense Manager navigation tree, expand **Filter Definitions** > **Web Filter Lock**. The URL category and protocol filtering settings comprising the Web Filter Lock are displayed in the content pane.



Web Filter Lock displayed in content pane

- Next to **URL Category Lock**, click **Edit**. The **Edit URL Category Lock** dialog box is displayed.



Edit URL Category Lock dialog box

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 the **Apply to Subcategories** button.
5. To block keywords for the category, check **Block & Lock Keyword**. If this box is checked, you must enter keywords by following the instructions on [page 333](#).
6. To apply restrictions based on file extensions, check **Block & Lock File Types**, and then check the file types you want to block.

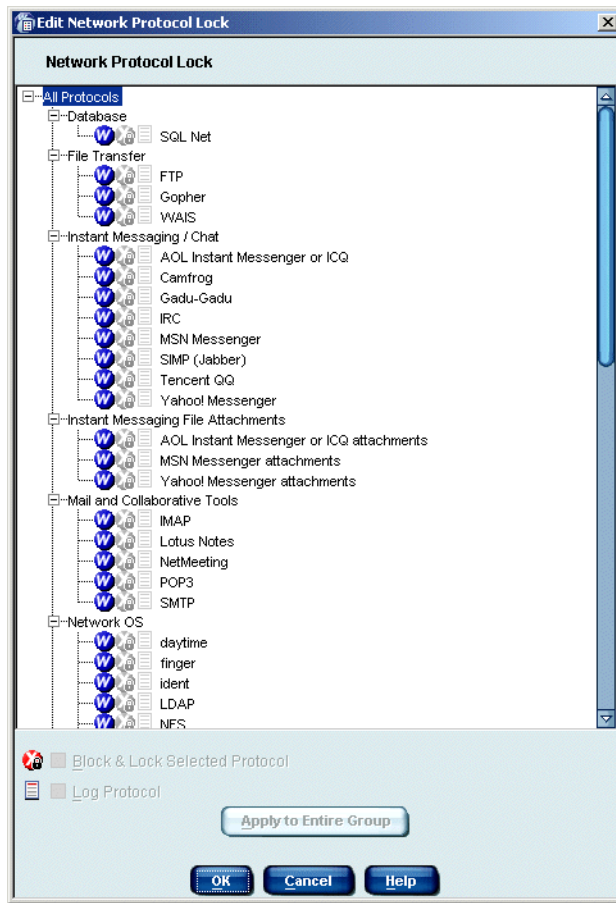
7. To apply the same restrictions to the subcategories associated with the category, click the **Apply to Subcategories** button.



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 you want 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 is displayed.



Edit Network Protocol Lock dialog box

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.



IMPORTANT

In order for administrators to receive usage alerts for a protocol, Log Protocol must be checked. See [Alerting](#), page 227 for more information.

13. To apply the selected filtering options to the whole protocol group, click **Apply to Entire Group**.
14. Click **OK** to save the modified protocol set.
15. Click **Save Changes** above the navigation tree.

You have configured filtering restrictions to be implemented by Delegated and/or Remote Administrators. This Web Filter Lock is the basis for filtering settings that Delegated Administrators will 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 Distributed Administration feature makes it easy to share 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 261)
- ◆ Global server settings
- ◆ Permission for Remote Administrators to modify these settings at their respective sites

The Super Administrator performing distribution has the flexibility to completely control filtering restrictions and server settings, or to allow Remote Administrators to modify certain elements as appropriate for their sites.

**NOTE**

If you are running multiple Policy Servers but only one Log Server, see [Multiple Policy Servers with a Single Log Server](#), page 273 for how to distribute policy data.

Not all server settings are distributed via Central Configuration Distribution. Many server settings are designed to apply to one 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 81)
- ◆ Common Filtering
 - Use more restrictive blocking (see *When Multiple Group Policies Apply*)
 - Block users when subscription expires or is exceeded (see *Subscriptions*, page 17)
 - Keyword search options (see *Setting Up Keyword Blocking*, page 332)
 - Password override timeout (see *Enabling Password Override*, page 116)
 - Continue timeout (see *Continue*, page 48)
 - Quota session length (see *Quotas*, page 49)
 - Default quota time per day (see *Quotas*, page 49)
 - Default quota sessions per day (see *Quotas*, page 49)

Policy Server Relationships

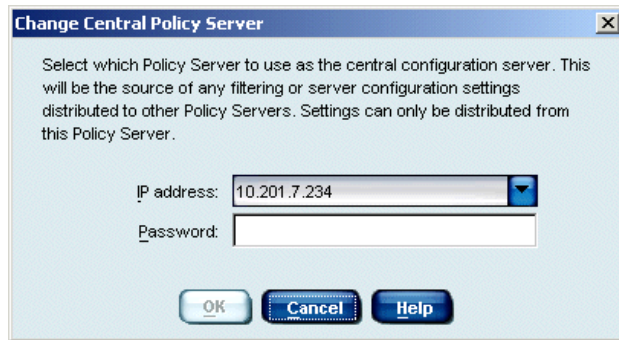
By default, the first Policy Server installed is the central Policy Server. Additional Policy Servers are viewed from the central site as remote servers. However, these relationships can change, as you can set any server to be the central Policy Server. Likewise, an administrator managing a non-central 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, you can reassign which server is the central Policy Server.

To reassign the central Policy Server:

1. In Websense Manager, choose **Server > Change Central Server**. The **Change Central Policy Server** dialog box appears.



Change Central Policy Server dialog box

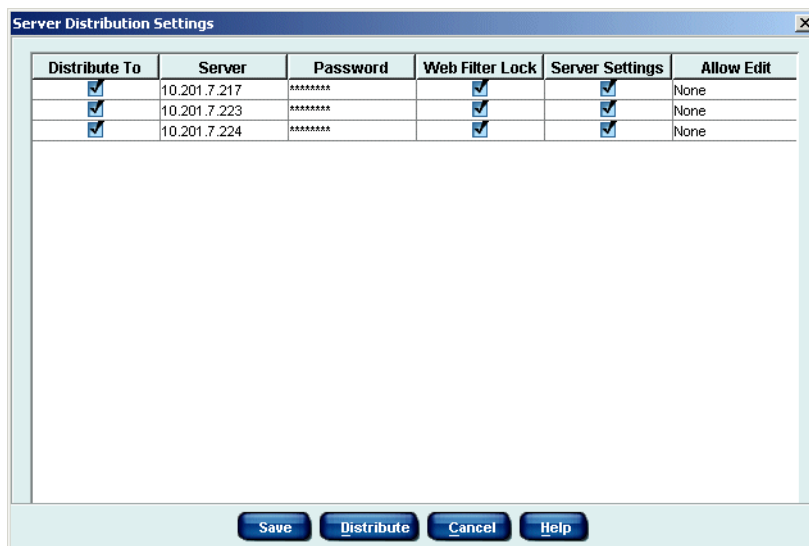
2. Select the IP address of the Policy Server to make the central server.
3. Enter the password to be used for access to the new central server.
4. Click **OK**. The **Set New Central Policy Server** confirmation dialog box appears.
5. Click **OK** to confirm the change. You are disconnected from the current central server, and will need to reconnect to the server to continue working.

The Policy Server you selected is the new central server. All other servers will inherit any global settings distributed from the central server.

Distributing Configuration Settings

Once you have defined a Web Filter Lock as described on [page 263](#), you can distribute the Lock to additional sites.

1. Ensure that all destination Policy Servers are added to Websense Manager (see [Adding a Server](#), [page 212](#)).
2. In Websense Manager, choose **Server > Distribution Settings**. The **Server Distribution Settings** dialog box appears.



Server Distribution Settings dialog box

3. Check the box for each Policy Server to which you want 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 261). To distribute global server settings, check **Server Settings** (see [Central Configuration Distribution](#), page 269).
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.

The configuration elements you selected are distributed to remote Policy Servers for use by the Remote Administrators at those sites.

Multiple Policy Servers with a Single Log Server

Websense, Inc. recommends against running multiple Policy Servers with only one Log Server. However, if your environment requires such a setup, there is another way to distribute data to remote servers.

It is recommended in this case to 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 one Policy Server, usage at another site is logged incorrectly. Synchronizing policy settings across servers maintains the integrity of report output.



WARNING

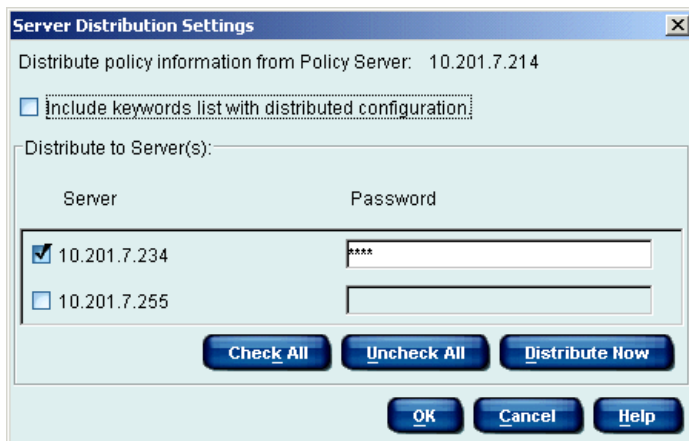
Distributing configuration data in this way overwrites existing settings on the destination Policy Servers, including role definitions. It is a good idea to back up the policy configuration file first (see [Saving the Configuration](#), page 221).

With this distribution method, the following configuration elements are 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. In Websense Manager, choose **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 dialog box

4. Check the boxes next to the IP addresses of the destination Policy Servers. Use the **Check All** or **Uncheck All** buttons to check or uncheck all servers at once.
5. If your organization uses 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, use Websense Manager to assign the policy to the local directory objects it should govern (see [Assigning Policies to Clients](#), page 283). 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.

Policy configuration settings are synchronized across Policy Servers. Any pre-existing settings on other servers are discarded.

Setting Up Web Filtering

In a first-time installation, Websense automatically filters users according to your **Initial Filtering** selection during installation. If you selected **Filter Internet traffic based on a predefined policy**, Websense software employs the **Global** policy (see [page 279](#)) by default for all users. If you selected **Monitor Internet traffic only**, Websense software monitors and logs internet traffic, but permits all requests. See your installation guide for installation instructions.

Filtering Policies

Policies govern user internet access. A policy is a schedule that tells Websense software how and when to filter URLs and protocols. A policy is comprised of these primary elements:

- ◆ **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.

Policy-based filtering lets you permit varying levels of internet access to different users in your organization. By editing and creating policies, you can schedule different category sets and protocol sets to be applied at different times and for different users.

You can edit the **Global** policy to meet the needs of your organization or use it as it is. Either way, it will be in effect for each user until another policy is assigned to the user. If this installation is an upgrade, Websense software filters users according to the settings and policies in your previous version.

When upgrading from an earlier Websense version, Websense software brings forward all configuration settings, including policies assigned to users, groups, workstations, and networks. After upgrading, review your policies to ensure that they are still appropriate for your employees.

To apply different filtering restrictions to different clients within your organization, create new policies or use the sample policies installed with Websense software. For example, you might 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, seven days a week.

With these 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.

The Global Policy

If you selected **Filter Internet traffic based on a predefined policy** during installation for the **Initial Filtering** option, Websense software applies the **Global** policy by default to all users.

The **Global** policy provides an immediate way to manage internet access throughout your organization. Use the **Global** policy as is, or edit it to meet the needs of your organization. Since the **Global** policy is the default policy, it cannot be deleted.

Initially, the **Global** policy restricts requests according to the **Default Settings** category set and the **Default Settings** protocol set 24 hours a day, seven days a week. See [Category Sets/Yes Lists](#), [page 296](#) for more information on category sets and filtering options.

After installing Websense software, review the **Default Settings** category set to determine whether it meets the needs of your organization. Make any appropriate changes and the **Global** policy filters according to the revised settings.

For the **Default Settings** protocol set, the **Permit** option is active by default *except* for protocols in the Instant Messaging/Chat, Instant Messaging File Attachments, P2P File Sharing, and Proxy Avoidance protocol groups. See [Customizing Protocols and Protocol Sets](#), [page 351](#) for information on customizing filtering options for protocol sets.

Additionally, you can 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.

Sample Policies

Websense software comes with additional policies that are designed as models and can be used as is, edited, or deleted at your discretion. To view a sample policy, expand **Policies** in the navigation tree and select one. Information about the selected policy is displayed in the content pane.

Custom Policies

Custom policies allow you to apply more or less restrictive filtering for specific users or computers (clients) without affecting filtering for the rest of the organization.

Enforcing a custom policy requires four steps.

1. Add a new policy via Websense Manager.
2. Edit the policy to define its filtering restrictions (see [page 281](#)).
3. Add a client via Websense Manager (see [page 107](#)).
4. Assign the new policy to the added client (see [page 283](#)).

Adding a Policy

The first step in creating a custom policy is adding a new policy.

1. Right-click in the Websense Manager navigation tree, and then choose **Add Policy**.

The **Add Policy** dialog box appears.

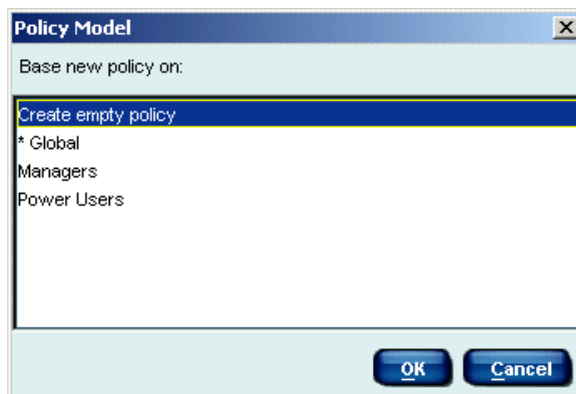
2. Enter a name for the new policy in the **Add Policy** dialog box.



Add Policy dialog box

Policy names must be between 1 and 25 characters in length, including spaces, and should be descriptive of the policy's characteristics.

3. Click **OK**. The **Policy Model** dialog box appears.



Policy Model dialog box

4. Select an existing policy on which to base your new policy, or select **Create empty policy**.
5. Click **OK**.

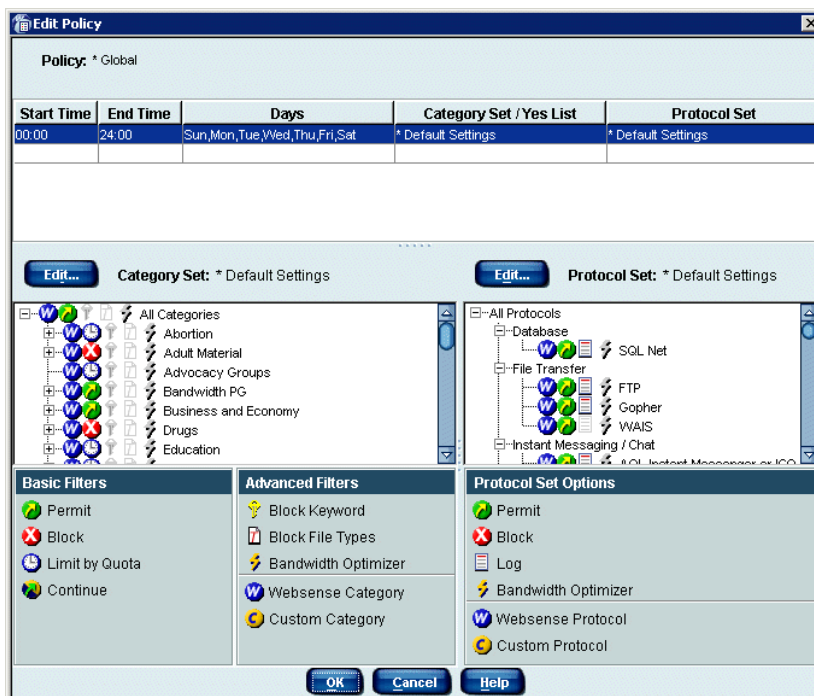
Once these steps are complete you can either add more policies or begin editing your newly-created policy. If you based your new policy on an existing one, you must edit it or it will remain a replica of the original. If you created an empty policy, you must edit it to specify restrictions.

Editing a Policy

A policy consists of specified time periods. During each time period, a particular category set (or set of filtering options for the categories in the Master Database) is 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.



Edit Policy dialog box

4. Click inside an existing row or right-click and select **Add Row**. A new row appears, displaying default time and day values.
5. Double-click in a row under the **Start Time** and **End Time** headings and select a start time and end time from the drop-down lists. This defines the time period during which the category set in this row will be enforced.
Do not define a time period that spans midnight. For example, to use the same category set from 5:00 pm to 8:00 am, define two 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).
6. Double-click in the **Days** column. From the list, select each day of the week that this category set should be enforced. Click **Done** to close the list.
7. Double-click in the **Category Set/Yes List** column and select the category set to be enforced during the days and times shown in the current row.

8. Double-click in the **Protocol Set** column and select the protocol set to be enforced during the time period shown in the current row. (For more information on configuring protocol-based filtering, see [Managing Protocols](#), page 337).
9. Repeat [Step 3](#) through [Step 8](#) 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**.
10. Exit the table area by clicking outside the table or by pressing **Ctrl+Shift+Tab**.
11. Click **OK** to accept the new policy definition.
12. Click **Save Changes** above the navigation tree.

Now that you have edited the policy, you must assign it to a client (see below). Websense software cannot use this policy to filter internet requests until you do this.

Assigning Policies to Clients

The **Global** policy is assigned to all users by default. To assign a different policy to an individual user, group, workstation, or network, you must first add the client to Websense Manager (see [page 107](#)).

Assign a policy to one client at a time, or assign the same policy to multiple clients at once. You can also view a list of all clients to which a policy is assigned (see [page 286](#)).



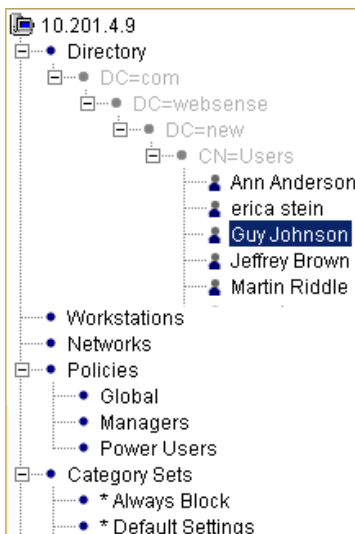
NOTE

Filtering Service applies one policy per site request. If more than one policy applies (for example a computer and its user each have an assigned policy), Filtering Service evaluates those policies in a specific order. See [page 41](#) for more information.

Assigning a Policy to a Single Client

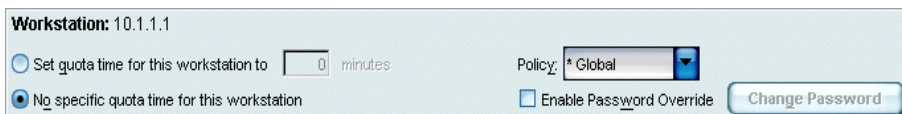
To assign a policy to a single user, group, workstation or network, or to change the policy assigned to a single client:

1. Select the appropriate user, group, workstation, or network in the navigation tree.



User list in navigation tree

Information regarding the client's policy appears in the content pane.



Client's current policy

2. Select the desired policy from the **Policy** drop-down list.



NOTE

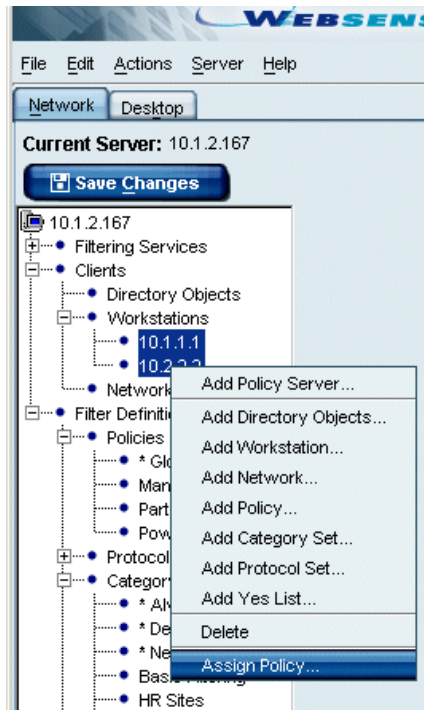
Alternatively, right-click the client name in the navigation tree, and then choose **Assign Policy**.

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

Assigning a Policy to Multiple Clients

Websense Manager makes it convenient to assign a single policy to multiple users, groups, workstations, or networks at the same time.

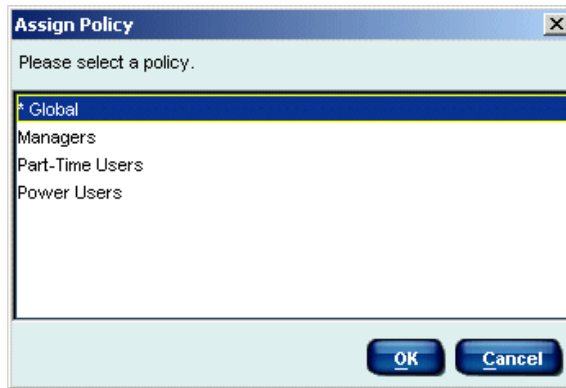
1. To select multiple users, press the **Ctrl** key while clicking each group name. To select a range of users, hold down the **Shift** key while clicking the first and last users in the range.
2. Right-click one of the selected clients, and then choose **Assign Policy**.



Shortcut menu in navigation tree

The **Assign Policy** dialog box appears.

3. Select the policy you want to assign, and then click **OK**.



Assign Policy dialog box

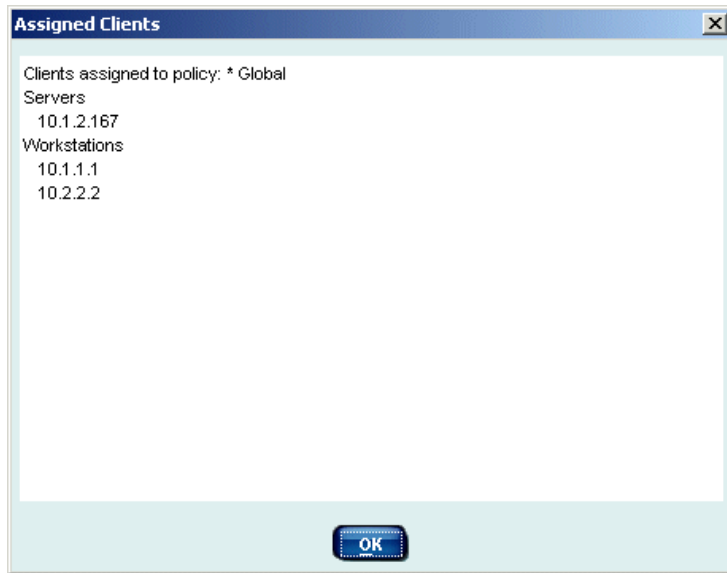
4. Click **Save Changes** above the navigation tree.

Viewing Assigned Policies

You can view a list of all clients assigned to a particular policy.

1. Right-click the policy name in the navigation tree.
2. Select **View Assigned Clients**.

The **Assigned Clients** dialog box appears.



Assigned Clients list

3. Click **OK** to close the **Assigned Clients** dialog box.

Distributing Policies to Multiple Servers

If there are multiple Policy Servers installed in your network, 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 allows you to distribute configuration data in this way.



NOTE

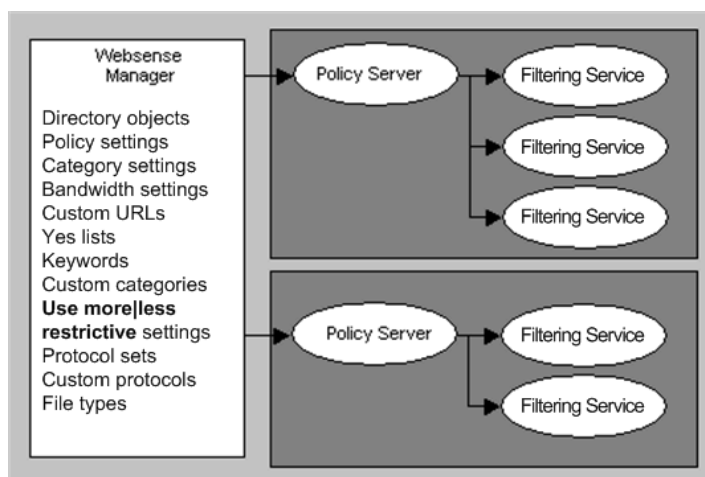
If only one Policy Server is connected to Websense Manager, central policy distribution commands are temporarily disabled in all locations.

If you are running Websense Enterprise Corporate Edition, your options for distributing central data are more flexible. See [Central Configuration Distribution, page 269](#) for information on distributing data in a Corporate Edition environment.

Central policy distribution offers several advantages in managing multiple locations. This feature allows you to:

- ◆ Implement filtering settings across locations in your organization, in one easy step.
- ◆ Manage and configure filtering policies in one 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.

Server and filtering settings are configured via Websense Manager. Filtering settings are activated for the central Policy Server, and then communicated to all Filtering Services connected to that Policy Server. Settings from one Policy Server can be 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 configuration settings by default. This scenario is established during installation; see your installation guide for details.



NOTE

Each Filtering Service must be configured to communicate with a Policy Server. See your installation guide for installation and setup instructions.

Once you distribute configuration settings to multiple servers, a distribution profile is stored locally in Websense Manager. The next time you distribute settings, the same distribution profile is used, unless you specify differently during distribution.

When you distribute settings from one Policy Server to additional Policy Servers, configuration data related to Websense policies is pushed to the other servers, including:

- 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
- Common Filtering settings

The following 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

You can use the central policy distribution feature in the following scenarios:

- 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, and all local offices have access to the same directory service information. You may be using filtering policies assigned to particular directory objects.
- c. Your network includes a directory service, but the various locations in your organization do *not* share directory service information. You may be using filtering policies assigned to particular directory objects.

If scenario *a* or *b* applies to you, you do not need to do any special configuration after distribution. If scenario *c* applies, then you will need to ensure that any directory objects associated with distributed policies exist at all destination locations. How to do this is described in the next section.

Be aware that when you distribute policy data and Websense directory objects to multiple locations, any existing, local policies and objects are overwritten. In general, the more information various locations share, the more convenient central policy distribution can be.

Single Log Server Environment

Websense, Inc. does not support unique configuration of multiple Policy Servers with only one Log Server in non-Corporate Editions of Websense. If you need to maintain unique filtering settings on separate Policy Servers, it is recommended to install a separate Log Server for each Policy Server. This way, any custom settings (such as custom categories or custom URLs) will be 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

You configure settings to be used in central policy distribution by all Policy Servers connected to Websense Manager. Follow these steps to specify distribution settings, and then distribute policies.



IMPORTANT

If Websense Manager is open at a destination location, and the local administrator makes setting changes after distribution occurs, all distributed changes are discarded. Ensure that local administrators are informed appropriately and that they have closed Websense Manager before you distribute data.

1. If your network uses separate directory services for different locations, ensure that you have configured directory objects. See *Configuring Distribution Settings* in the previous section for details.
2. In Websense Manager, choose **Server > Distribution Settings**. The **Server Distribution Settings** dialog box appears.

Server Distribution Settings dialog box

3. Check the boxes next to the IP addresses of the destination Policy Servers. Use the **Check All** or **Uncheck All** buttons to check or uncheck all servers at once.

4. *If your organization uses separate directory services at different locations, do the following. (If all locations share the same directory service information, do not 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 283). 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.
5. For each Policy Server selected, enter the password.



NOTE

You must enter a valid password for each destination Policy Server. If no password is entered, distribution may fail for any server that does not have a valid password.

6. To distribute data now, 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.
7. Click **OK** to exit the **Server Distribution Settings** dialog box.

Policy configuration data is distributed to all Policy Servers you selected, as long as they are connected to the current instance of Websense Manager.

Printing Policies to a File

Websense software offers the capability to export your filtering policy configuration information to an external file. This is a good way to retain a view-only copy of your policy configuration when you make changes. This can serve as a record of your policy configuration, in case you want to revert to the previous configuration later on. Exporting enables you to view all policy configuration details at a glance, in an organized fashion.



NOTE

It is not currently possible to re-import exported policy configuration data back to Websense software. Policies must be configured manually, or using the central policy distribution feature.

Standard Websense users: See [Distributing Policies to Multiple Servers](#), page 287).

Corporate Edition users: See [Central Configuration Distribution](#), page 269.

Configuration details are written to a text file by default. However, you can paste the text output into another application, such as Microsoft Excel, for more sophisticated formatting.

	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 Name	Start Time	End Time	Days	Category	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 Blk	* Never Block				
24											
25											
26	Yes Lists	Yes List Name	URL								
27											
28											
29	Category Name	Category				Generated Basic Filte	Block Key	Block File	Bandwidth	Optimizer	
30		Monitor Only									
31		All Category				Websense Permit	No	No	No		
32			---	Business		Websense Permit	No	No	No		
33			---	Financial		Websense Permit	No	No	No		
34			---	Religious		Websense Permit	No	No	No		

Policy information exported to a file

To print policy configuration information to a file:

1. In Websense Manager, choose **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**.

Your policy configuration details are saved to the text file you specified.

Deleting a Policy

You can delete any policy that becomes obsolete (except the **Global** policy, which is the default policy).

1. Right-click the policy you want to delete in the navigation tree.
2. Choose **Delete** from the shortcut menu.
3. Click **Yes** when prompted to confirm the delete request.
4. If no clients are assigned to the policy, it is deleted immediately.
5. If the policy *is* assigned to clients, Websense software alerts you to the fact that they will be reassigned the **Global** policy.
6. Click **Yes** to delete the selected policy and reassign the **Global** policy for those users. Click **No** to cancel the delete request.

Managing Sites

In addition to using existing filtering settings for URL categories and network protocols, you can use yes lists, Custom URLs, keywords and bandwidth limits to enhance and fine-tune filtering.

Category Sets/Yes Lists

The Websense Master Database contains over 90 categories, covering web page subject matter as diverse as adult material, job search, games, and weapons. It is organized into general categories and specific subcategories. For example, the Information Technology category includes the subcategories Computer Security, Hacking, Proxy Avoidance, Search Engines and Portals, URL Translation Sites, and Web Hosting.

Before you enter your subscription key, category names are not displayed in Websense Manager. Once you have entered the key, the list of categories appears, but some categories may be 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 option is always set to 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 will be marked **[monitor only]**. However, new categories added to the Master Database are *permitted by default*.

You can create custom categories for storing sites you want to control that are not in the Master Database, and for reclassifying sites so they are filtered differently. For instructions, see page [Adding a Custom Category, page 328](#).

Filtering settings determine whether Websense software blocks, permits, or limits a site by quota or continue options. Descriptions of the filtering options are on [page 314](#).

Filtering settings for each category are selected in Websense Manager and stored collectively as *category sets*. Filtering settings for each protocol are stored collectively as protocol sets. Category sets and protocol sets are assigned to time periods in policies.

Policies are schedules of category sets/yes lists and protocol sets that tell Websense software which category and protocol filtering settings to apply and when (see *Filtering Policies*, page 277). Category and protocol sets are scheduled into policies by time and day of the week, giving you the flexibility of enforcing stricter filtering during business hours and more liberal access before and after working hours.

A yes list is a list of explicitly-allowed URLs. A yes list can be used in a filtering policy, 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. See page 303 for details about configuring yes lists.

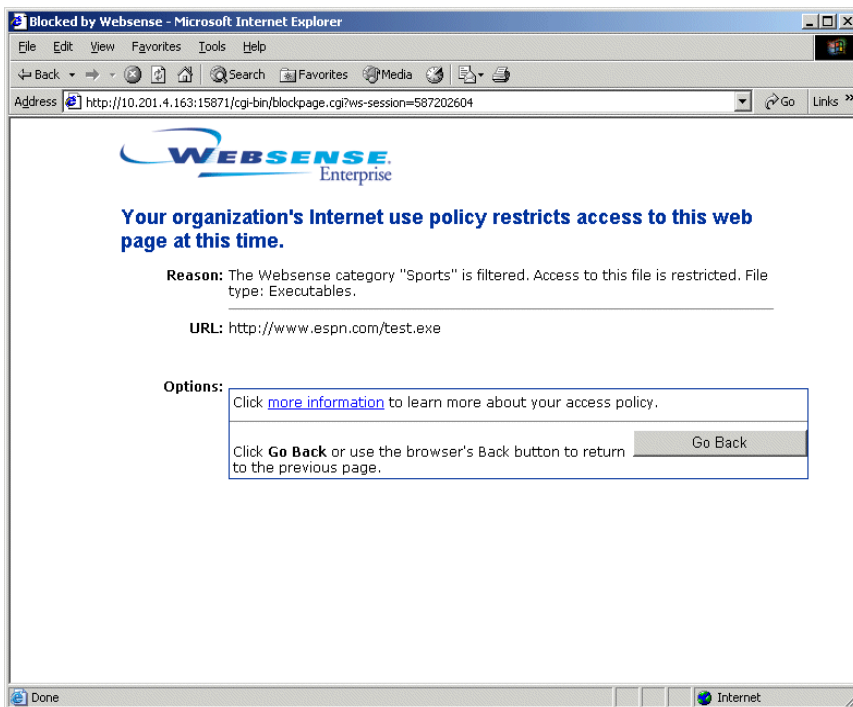
Category sets, protocol sets and yes lists can be created and edited at any time. Adding multiple category or protocol sets via Websense Manager gives you increased flexibility in managing internet access for your organization.

File Types

In addition to filtering based on category sets, you can filter based on file extensions. You can combine access to a category set with restrictions on particular types of files from sites within that category set. For example, you can permit access to the category **Sports**, but block access to 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.

When filtering an internet request, Websense software first determines the URL category of the request, and then checks any file extensions against filtering settings for that category. See page 39 for more information about filtering precedence.

When a user tries to access a file whose extension is blocked, a Websense block page is displayed in the user's web browser, as shown.



Block page resulting from blocked file request



NOTE

The standard block message does not appear if a GIF or JPEG image comprises just a portion of an otherwise-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.

File type blocking is associated with a particular category set, to be applied by any policy that uses that category set. (To edit a category set, see [page 314](#).)

To edit the category set for a particular policy only, see [Editing a Policy](#), page 281.

**NOTE**

To implement full filtering for video *and* audio internet media, combine protocol-based filtering with file type filtering (see [page 297](#)). In this case, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

Websense software provides several predefined file types, or groupings of file extensions used for similar purposes. You can implement filtering policies based on predefined file types, modify the existing file type definitions, or create new file types to use in filtering policies. Websense file types are continually updated in the Master Database. Updates can be acquired via the nightly Master Database download.

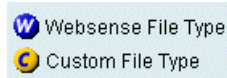
The following table is a sampling of file type definitions. File types are continually being added to the Websense Master Database.

Audio	Compressed Files	Executables	Video
.aif	.ace	.bat	.asf
.aifc	.arc	.com	.asx
.aiff	.arj	.exe	.avi
.au	.b64		.ivf
.m3u	.bhx		.mlv
.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		

File types and associated file extensions

To view the file extensions associated with each file type:

1. Open Websense Manager, and then log on to Policy Server.
2. Expand **Filter Definitions** > **File Types** in the navigation tree. A list of file types is displayed on the right-hand side, under **File Types**. Websense predefined file types and custom file types are distinguished by the icons shown.



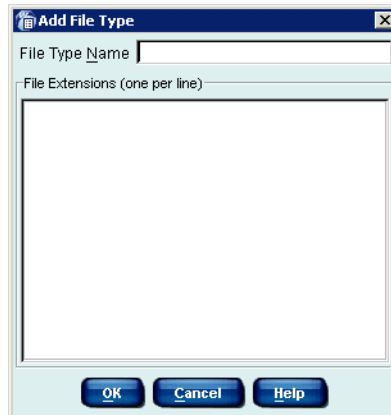
File Type legend

3. Select a file type to display its associated file extensions under **File Extensions** at the right.

Adding a New File Type

You can add up to 32 file types (groups of file extensions) to suit your organization's needs. When you add a file type, it appears in Websense Manager as a custom file type.

1. Expand **Filter Definitions** > **File Types** in the Websense Manager navigation tree. A list of file types is displayed on the right-hand side, under **File Types**.
2. Click **Add File Type** at the bottom of the Websense Manager window. The **Add File Type** dialog box appears.



Add File Type dialog box

3. Enter a **File Type Name** for the new file type. (This must be different from any existing file type names.)
4. Type the file extensions, one per line, for all types to include in this file type definition. You do not need to type a dot “.” before each three-letter extension.
5. 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 Websense Manager navigation tree. A list of file types is displayed on the right-hand side, under **File Types**.
2. Select the file type you want to modify, and then click **Edit File Type** at the bottom of the Websense Manager window.

The **Edit File Type** dialog box appears.

3. Add or remove file extensions, as desired. (You can only remove file extensions from custom file types.)



NOTE

If you add a file extension that is already used in an existing Websense file type definition, your entry will take 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** to save your changes.

Permanent Category Sets

Websense software includes three permanent category sets. These cannot be deleted. Of the permanent category sets listed below, 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 Websense software uses when a request is not filtered by any other category set. The Default Settings category set blocks sites in some categories, permits sites in others, and uses the Limit by Quota filtering option in the remaining categories. Default settings can be edited to meet your needs.
- ◆ **Never Block:** Allows total, unrestricted access to all internet sites.

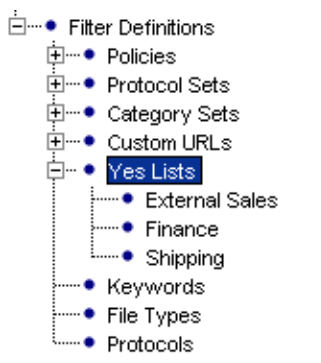
Websense software also installs category sets designed as models that can be used as is, edited, or deleted.

- ◆ **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 for clients (users, groups, workstations and networks) in your organization. Yes lists can be used to:

- ◆ Allow very 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.



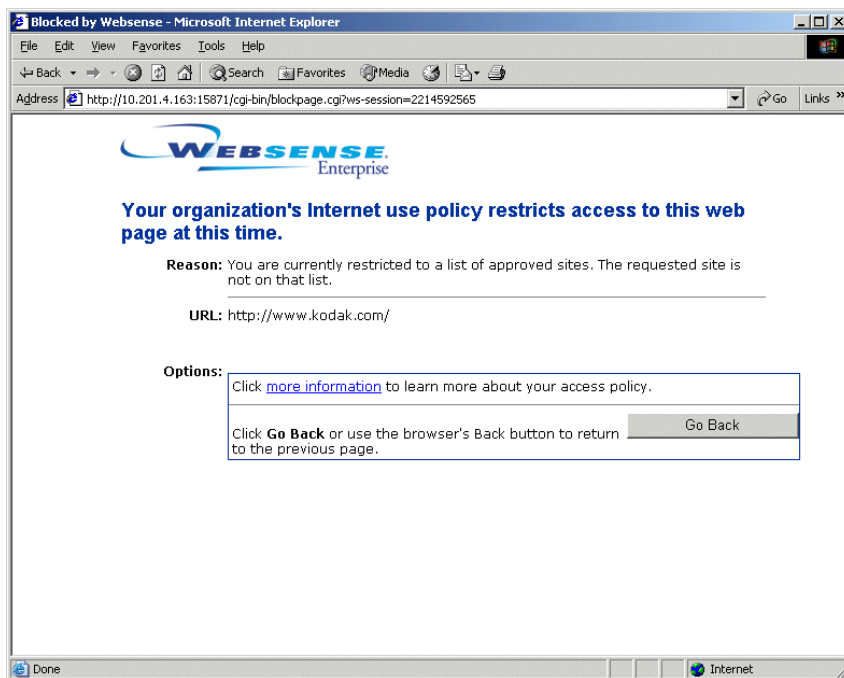
Yes lists in navigation tree

You can create and apply yes lists as needed. (Websense software can support 2,500 yes lists containing 25,000 URLs.)

A yes list is active for a particular time period in a policy. Only one yes list can be applied to a time period. A yes list and a category set cannot both be assigned to the same time period; only one or the other is active.

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 yes list is active in a policy, *only* those sites on the selected yes list are allowed for users governed by that policy. All other sites are blocked.

When a user is governed by a yes list, a block page is returned for any requested URL *not* included on that yes list.



Block page for yes list user

Yes Lists and Filtering Precedence

There are some special considerations when using yes lists in combination with other category sets, custom URLs, and certain global filtering options. Multiple filtering settings can be involved when a user is in more than one 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 might affect just one group.

Yes Lists and Multiple Groups

The **Use more restrictive blocking** setting (see [page 41](#)) determines what happens when multiple group policies apply. By default, this setting is off. Filtering behavior involving yes lists in combination with the **Use more restrictive blocking** option may not always be as expected.

Websense software determines which filtering setting is more or less restrictive at the category set/yes list level. How a URL is categorized has no effect unless the URL category is in an active policy.

	<i>Use more restrictive blocking off (default scenario)</i>	<i>Use more restrictive blocking on</i>
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 filtering policies, the filtering setting for the *category* takes precedence. This is because the least restrictive filtering case is used by default, and a category set is considered less restrictive than a yes list. So, if the category is blocked, a request for a URL in that category is blocked, even though the URL is also on a yes list.

When the **Use more restrictive blocking** option 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. If the **Always Block** category set and a yes list are both active at the same time (for example, when a user is in multiple groups governed by different policies), the user can still access URLs on the yes list.

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** is the more restrictive case.

Yes Lists and Custom URLs/Not Filtered

Though they might seem similar, yes lists and Custom URLs/Not Filtered are two separate entities. Yes lists are viewed, created and modified much like custom URLs. However, yes lists only become active when they are applied in policies. Meanwhile, custom URL lists always factor into Websense filtering behavior for all users.

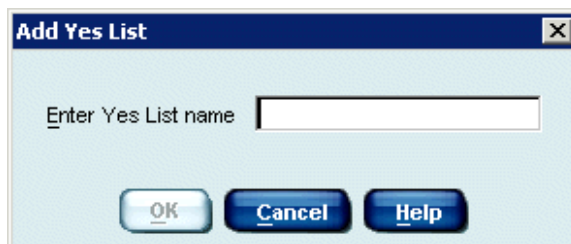
By default, if the same URL is on both a yes list and the Custom URLs/Not Filtered list, the URL is always allowed. The exception is if the **Always Block** category set is active at the time, and the **Use more restrictive blocking** setting is *not* active.

The list that is active at the time an internet request is made allows the URL, and is recorded in Websense reports. For example, if <http://www.cnn.com> is on a yes list that is active at the time of a request, then the yes list allows the URL. If <http://www.cnn.com> is on a Custom URLs/Not Filtered list, and no yes list is active at the time of the request, then the URL is allowed as a custom URL. See [Custom URLs, page 319](#) for more information about custom URLs.

Adding a Yes List

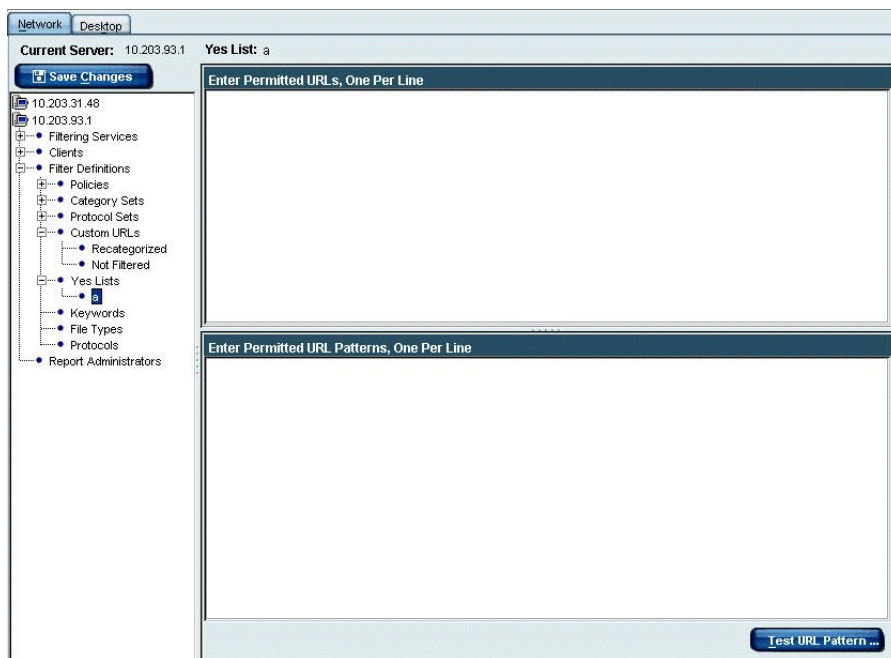
Create a yes list by assigning it a name, and then entering a list of allowed URLs. Then apply the yes list to clients as described in the next section.

1. Right-click in the Websense Manager navigation tree, and select **Add Yes List**. The **Add Yes List** dialog box appears.



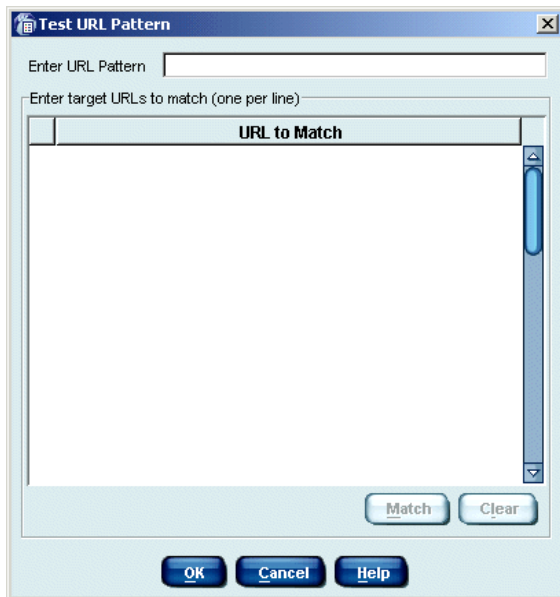
Add Yes List dialog box

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 at the right.
5. Enter the URLs or URL patterns to be included in this yes list, one at a time. URL patterns can be in regular expression form.
URLs must be separated with at least a space.



Yes List editor

6. If you entered any URL patterns, verify that a pattern matches the desired URL:
 - a. Click **Test URL Pattern**. The **Test URL Pattern** dialog box appears.



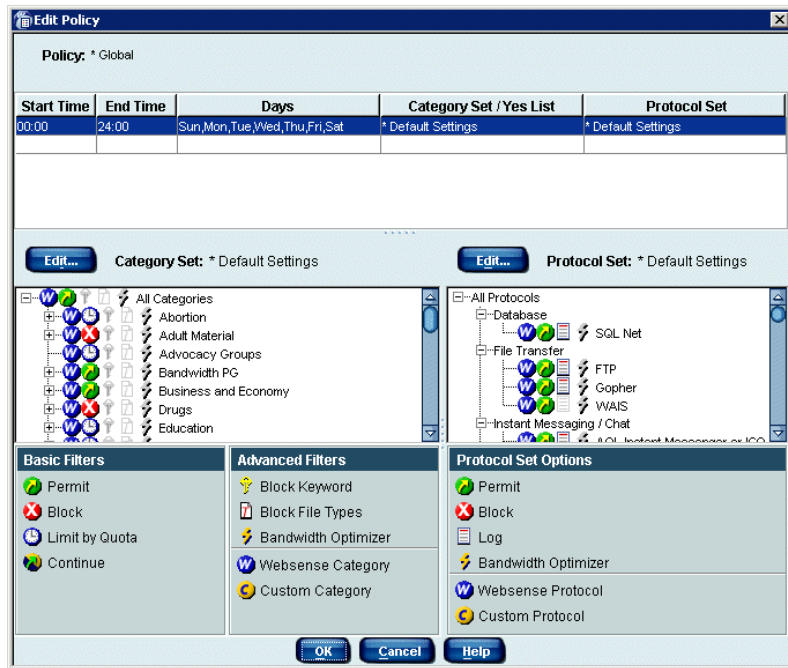
Test URL Pattern dialog box

- b. Enter the URL pattern to test.
 - c. Type the desired target URLs.
 - d. Click **Match**.
 - 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

To permit only a specific list of URLs for a certain group in your organization:

1. Create a yes list, as described on [page 308](#).
2. Locate the policy that will govern this group of clients. To create a policy, see [page 280](#).
3. Select the desired policy in the navigation tree to display the start and end times, days, category sets/yes lists, and protocol sets that make up the policy.
4. Click **Edit**. The **Edit Policy** dialog box appears.



Edit Policy dialog box

5. Double-click under the **Start Time** and **End Time** headings and select a start time and end time from the drop-down lists. This defines the time period during which the yes list will be enforced.

Do not define a time period that spans midnight. To use the same category set from 5:00 pm to 8:00 am, for example, define two 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).

6. Double-click in the **Days** column. From the list, select each day of the week that the category set on this row should be enforced.
7. Click **Done**.
8. Double-click in the **Category Set/Yes List** column, and then select the category set you created earlier.



NOTE

Only one yes list can be selected for a time period in a policy. This also means that only one yes list can be applied to a particular object (user, group, workstation or network).

9. Double-click in the **Protocol Set** column, and then select the protocol set to be enforced during the selected time period. (See [Customizing Protocols and Protocol Sets](#), page 351 for details about protocol filtering options.)
10. Click **OK** to accept the modified policy definition.
11. Click **Save Changes** above the navigation tree.
12. Assign the policy to the desired group, as described in [Assigning Policies to Clients](#), page 283. This group will have access only to URLs on the yes list during the time periods specified in the policy.

Adding a Category Set

You can add as many category sets as needed for your organization. For example, create a category set for your marketing group that permits all sites except those dealing with adult material, and another for your accounting group that also blocks entertainment and shopping sites.

Once a new category set or yes list is created, it must be added to a policy so Websense software knows when to enforce it and for which clients.

When you add a category set, you must base it on an existing category set, and then edit it to suit your needs. Review the existing category sets before you add a new one, to base the new category set on the most appropriate one.

To review a category set, select **Category Sets** in the navigation tree and select the category set you want to view. The list of categories in that category set appears with the filtering setting shown for each. Listings are not shown for the **Always Block** and **Never Block** category sets, because these categories are blocked or permitted, respectively.

To add a category set:

1. Right-click in the Websense Manager navigation tree, and then choose **Add Category Set**.
2. The **Add Category Set** dialog box appears.
3. Enter a name for the new category set, and then click **OK**.
4. In the **Category Set Model** dialog box, select an existing category set as the basis for the new set.
5. Click **OK**.

The new category set appears in the navigation tree. It remains a replica of the category set it is based on until it is edited, and will not be enforced until it is added to a policy (see *Filtering Policies*, page 277).

Editing a Category Set

Category sets can be edited to change the filtering settings for any or all categories. The Websense filtering options are:

- ◆ **Permit:** Permits access to all sites in the selected category.
- ◆ **Block:** Blocks access to all sites in the selected category.
- ◆ **Limit by Quota:** Gives the user two options:
 - Continue and view the site or view any other site in a quota category for a short time.
 - Go back to the previous web page.
- ◆ **Continue:** Gives users two options:
 - Continue and view the site for a limited amount of time. The time limit is defined via **Server > Settings > Common Filtering**. See [Continue](#), page 48 for more information.
 - Go back to the previous web page.

In addition to setting a basic filtering option for the selected category, you can:

- ◆ **Block Keyword:** Blocks sites whose URLs contain keywords assigned to the category set (see [Keywords](#), page 331). When this option is active, a key appears over the icon of the filtering option, next to the category name. The **Block Keyword** option can be combined with any other filtering option. Overall performance may be affected when this option is enabled.
- ◆ **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:** Block internet content based on bandwidth usage associated with the URL categories governed by a filtering policy. For example, a policy could block the sites in its category set if total network bandwidth usage exceeds 50% of available network bandwidth. To set bandwidth limitations based on a category set, edit the category set assigned to a particular policy.

Websense software provides default maximum values for available network bandwidth for the network and for each protocol. You can change these values. See [Bandwidth Management, page 347](#) for instructions on viewing and changing available bandwidth values.



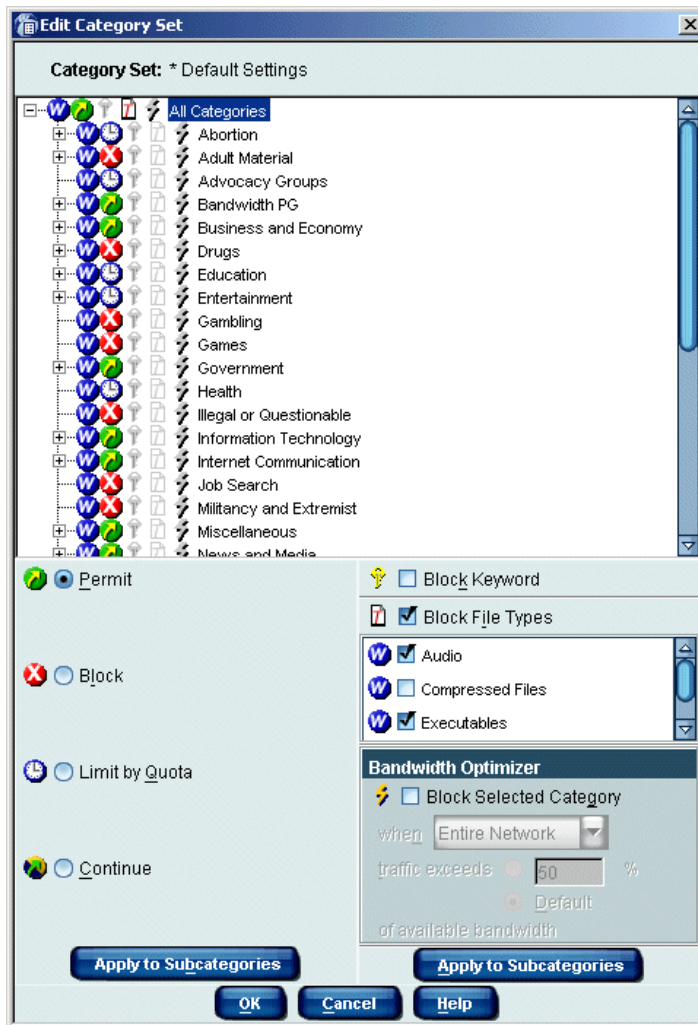
NOTE

If you activate the **Block Selected Category when HTTP traffic exceeds [Default/N%] of available bandwidth** settings, Network Agent monitors only HTTP traffic for bandwidth data.

- ◆ **Apply to Subcategories:** Clicking this button applies the current filtering option to all subcategories associated with the selected category. For example, you might select the Information Technology category, set a filtering option, and then click **Apply to Subcategories** to ensure that all subcategories under the Information Technology category are filtered the same way.

To edit a category set.

1. Select a category set in the navigation tree to display its settings in the content pane.
2. Click **Edit** to open the **Edit Category Set** dialog box.
3. Select a category, and then select the desired filtering option. 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 this category, click **Apply to Subcategories**.
5. To block keywords for the category, check **Block Keyword**. If this box is checked, you must define keywords (see [Adding Keywords, page 333](#)).



Block File Types option

6. To apply restrictions based on file extensions, check **Block File Types**, and then check the file types you want to block.
7. To apply limitations on bandwidth for this category set, check **Block Selected Category**, and then specify the conditions for blocking.
8. To apply the same restrictions to the subcategories associated with the category, click **Apply to Subcategories**.
9. Repeat [Step 3](#) through [Step 7](#) for each category you want to change.

10. Click **OK** to close the **Edit Category Set** dialog box.
11. Click **Save Changes** above the navigation tree.

If the category set is already included in a policy, the new filtering options are automatically enforced when that category set is active. If the category set is not part of any policy, it must be added to a policy before Websense software can enforce it. See [Editing a Policy, page 281](#) for instructions on configuring a policy.

**NOTE**

Filtering options for Premium Groups cannot be changed unless the groups have been purchased from Websense, Inc.

Copying a Category Set

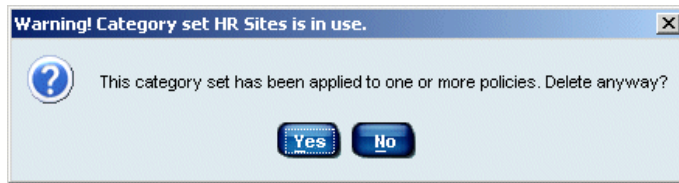
You may want to have identical category sets with different names. To accomplish this:

1. Select the category set you want to copy in the navigation tree.
2. Click **Save As** in the content pane.
3. Enter the new name of the copied category set in the **Add Category Set** dialog box that appears.
4. Click **OK** to close the **Add Category Set** dialog box.
5. Click **Save Changes** above the navigation tree.

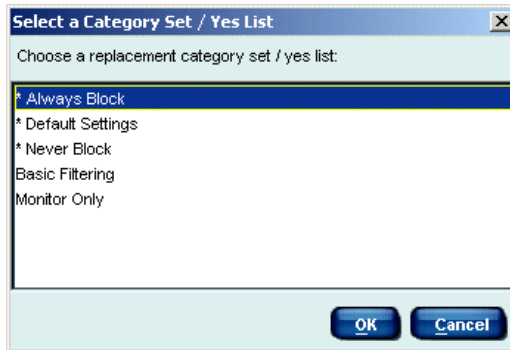
Deleting a Category Set

Category sets, with the exception of the **Always Block**, **Never Block**, and **Default Settings** category sets, can be deleted at any time:

1. Expand **Filter Definitions > Category Sets** in the navigation tree.
2. Right-click the category set you want to delete, and then choose **Delete**.
3. Click **Yes** to confirm the deletion.
4. If the category set is included in a policy, you are asked to select a replacement category set to use in its place.



5. Select a replacement category set, and then click **OK**.



Replacing a deleted category set

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

Custom URLs

The custom URLs feature offers administrators two benefits. This feature enables you to:

- ◆ 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.

To provide these benefits, Websense Manager offers two distinct custom URL lists: Custom URLs/Not Filtered and Custom URLs/Recategorized.

The Custom URLs /Not Filtered list enables you to specify internet sites that are to be permitted to all users, regardless of how the site's category is filtered. (The one exception is the **Always Block** category set, which blocks all internet access even to unfiltered custom URLs.)

The Custom URLs/Recategorized list serves a dual purpose. It lets you classify sites that are not in the Master Database by adding them to a database category. Websense software then filters these sites according to the filtering setting for that category. This list also lets you reclassify sites that already exist in the Master Database. You can single out specific sites to be filtered differently than their original categories. This feature is useful if you want to block a site in an otherwise-permitted category.

For added flexibility, Websense Manager lets you create new categories in which to store custom URLs (see [page 328](#)). These custom categories are added as subcategories to existing Master Database categories and are filtered according to the same options as the major category. Custom categories provide more precise filtering and reporting by allowing you to populate them with a narrower spectrum of URLs.

Custom-permitting Sites

The Custom URLs/Not Filtered list allows specified sites to be permitted for all clients, regardless of category set or policy (with the exception of the **Always Block** category set). To specify a list of URLs not to be filtered according to their original category or policy association, add the sites you want to permit to the Custom URLs/Not Filtered list.



NOTE

When upgrading from v4.x to v5.x, custom URL lists are automatically converted to a yes list named **Original Yes List**. Any policy that previously used the **Yes List Only** category set will instead use **Original Yes List** as its category set in v5.x.

All sites added to the Custom URLs/Not Filtered list are automatically accessible to clients, except those filtered by the **Always Block** category set, or those governed by a yes list in a policy. When a yes list is active for a time period in a policy, users governed by the yes list can *only* access sites on that list.

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 to the list 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 automatically match a custom URL with its equivalent IP address. To permit both the text URL and the IP address of a site, you must add both to the Custom URLs/Not Filtered list.

To add sites to the Custom URLs/Not Filtered list:

1. Expand **Custom URLs/Not Filtered** in the navigation tree. The URL categories from the Websense Master Database are displayed in the content pane.

Category	URL or URL Pattern
Games	RegEx: zxc
Games	http://asd

Custom URLs editor

2. Under **Choose a category**, select a category for the site you want to permit. Category selection is for logging and reporting purposes only. Alternatively, create a custom category if needed (see [page 328](#)).
3. Click inside the **Enter URLs for the highlighted category** text box and enter the complete URL for each site you want to permit under the selected category. Press **Enter** after each URL.

Be sure to include the protocol for any non-HTTP site – for example, `https://63.212.171.196:443`. If the protocol is omitted, Websense software automatically filters the site as an HTTP site.



NOTE

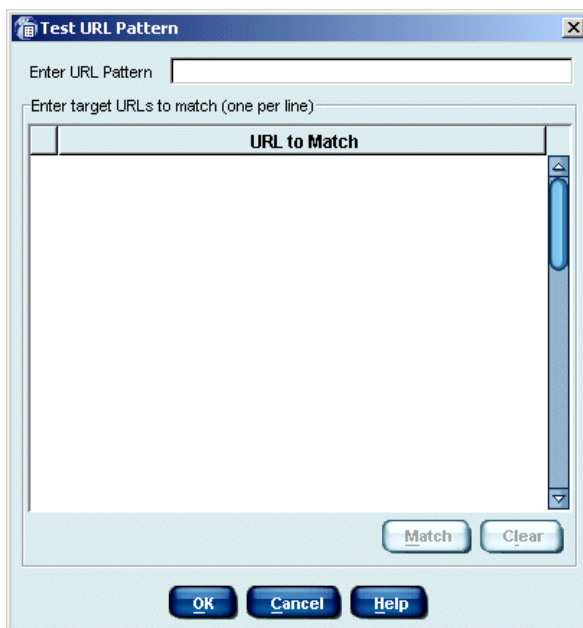
Websense software recognizes custom URLs exactly as they are entered (much like keywords). If Yahoo! sites are blocked, but you custom-permit “`http://www.yahoo.com`”, that site is permitted only if users type the full address, “`www.yahoo.com.`” If a user types just “`yahoo.com,`” the site is still blocked. Meanwhile, if “`yahoo.com`” is entered as the custom URL, all sites and sub-domains with “`yahoo.com`” in the address are permitted.

4. Click **Add**. The URLs appear, along with their assigned categories, in the URLs list at the bottom of the editor.

Category	URL
Cultural Institutions	http://www.artefacts.org
Cultural Institutions	http://www.virtualscientist.com

Added Custom URLs

5. Alternatively, enter URL patterns to be treated as custom URLs, one 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.



Test URL Pattern dialog box

- b. Enter the URL pattern to test.
 - c. Type the desired target URLs.
 - d. Click **Match**.
 - e. Click **Clear** to clear the URLs and test another pattern.
6. Click **OK** when finished.
7. Click **Add**.

8. Repeat [Step 2](#) through [Step 7](#) for each category to which you want to add custom URLs.
9. Click **Save Changes** above the navigation tree.

All clients are now permitted access to these sites (except those who have been assigned policies with the **Always Block** category set).

Using Custom URLs for Sites With Multiple Addresses

The custom URLs feature increases the functionality and effectiveness of your Websense installation. For example, you can use this feature to block sites that are not classified under **Miscellaneous/Uncategorized** in the Master Database or listed in an otherwise-permitted category.

Sites With Multiple URLs

Some sites can be accessed via multiple URLs. Set up each URL as a separate custom URL to ensure that the site is permitted or blocked as intended.

For example, you might set up <http://www.performancebikes.com> as a recategorized custom URL for a bicycle shop's site. However, the site can be accessed via <http://www.performancebikes.com> or <http://www.performancecycles.com>. In this case, users are filtered only if they request <http://www.performancebikes.com>, which is blocked because of its new category association. If they request the URL <http://www.performancecycles.com>, the site is permitted.

To make sure that users are always filtered when accessing the site, try one of two techniques for setting up custom URLs:

- ◆ Determine whether all the URLs point to the same IP address. If so, set up a custom URL with that IP address in place of the domain name. This blocks all URLs that point to the IP address.
- ◆ Set up a separate custom URL for each URL that can be used to access the site.

Sites with Redirected URLs

An organization might move its site from one server to another, and then use the HTTP redirect feature or the HTML refresh feature to make sure users requesting the original site are redirected to the new site. For example, if you add the original site to the Custom URLs/Not Filtered list, users still will be blocked when the original site directs them to the new site, because the new site has not been set up as a custom URL. In this case, be sure to set up separate custom URLs for the original and the new URLs.

One technique for determining whether a site you plan to custom permit redirects to a different URL is to request the site through your browser. After the site opens, check the URL displayed in the address bar. If the URL in the address bar is different, set up separate permitted custom URLs for both addresses.

Recategorizing URLs

Recategorizing custom URLs allows you to:

- ◆ Filter sites not contained in the Master Database
- ◆ Recategorize existing Master Database sites in order to filter them differently

You must associate each site with either a Master Database category or a custom category. (Adding custom categories is discussed on [page 328](#).)

To block a site that is in a permitted Master Database category, enter the site as a recategorized custom URL and associate it with a category whose filtering option is set to block in the appropriate category set. For example, the category **Business & Economy** is permitted, but you want to block a particular commercial real estate site in that category. You can add that real estate site to a filtered custom URLs list, and associate it with the blocked category **Shopping: Real Estate**.

Adding a site to the Custom URLs/Recategorized list does not mean Websense software automatically blocks it. In order to block the site, you must associate it with a category whose filtering option is set to block or limit by quota in the appropriate category set.



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 automatically match a custom URL with its equivalent IP address. To filter both the text URL and the IP address of a site, you must add them both as recategorized custom URLs.

To specify sites as recategorized custom URLs:

1. Expand **Custom URLs/Recategorized** in the navigation tree. The Custom URLs editor appears in the content pane.

Category	URL or URL Pattern
Games	RegEx: zxc
Games	http://asd

Custom URLs editor

2. Under **Choose a category**, select a category with which to associate the site.
3. Click inside the **Enter URLs for the highlighted category** text box, and enter the complete URL for each site you want to filter under this category. Press **Enter** after each entry (each URL must be on a separate line).

Be sure to include the protocol for any non-HTTP site – for example, *https://63.212.171.196:443*. If the protocol is omitted, Websense software automatically filters the site as an HTTP site.



NOTE

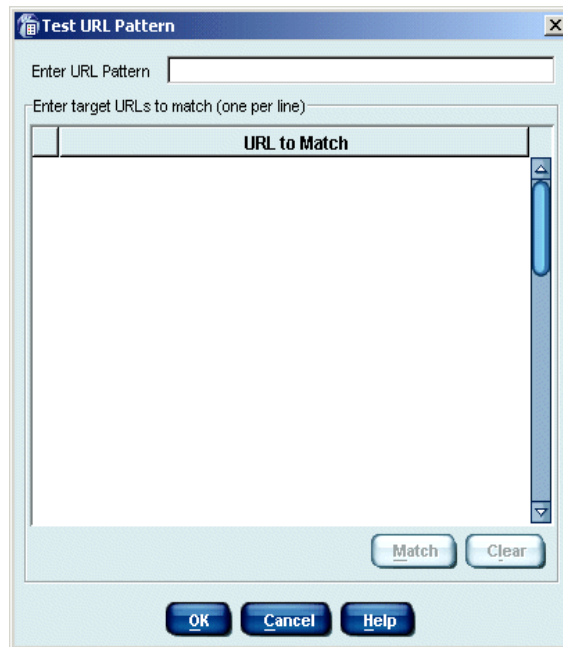
Websense software recognizes custom URLs exactly as they are entered (much like keywords). If Yahoo! sites are blocked, but you enter “http://www.yahoo.com” as recategorized custom URL, that site is permitted only if users type the full address, “www.yahoo.com.” If a user types just “yahoo.com,” the site is still blocked.

Meanwhile, if “yahoo.com” is entered as the custom URL, all sites with “yahoo.com” in the address are permitted.

4. Click **Add**. Newly-added URLs appear at the end of the list.
5. Alternatively, enter URL patterns to be treated as custom URLs, one 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.



Test URL Pattern dialog box

- b. Enter the URL pattern to test.
- c. Type the desired target URLs.
- d. Click **Match**.
- e. Click **Clear** to clear the URLs and test another pattern.
6. Click **OK** when finished.
7. Click **Add**.
8. Repeat [Step 2](#) through [Step 7](#) for each category to which you want to add custom URLs.
9. Click **Save Changes** above the navigation tree.

All sites on the Custom URLs/Recategorized list are filtered according to the options selected 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.

Deleting Custom URLs

To remove sites from a custom URLs list:

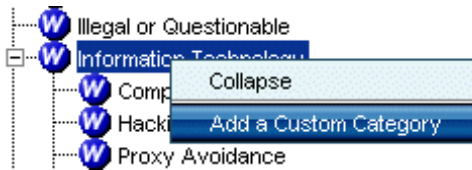
1. Expand **Filter Definitions** > **Custom URLs** in the navigation tree. Click **Not Filtered** or **Recategorized**, depending on which list contains the custom URL you want to delete.
2. In the content pane, select the URL you want to delete.
3. Click **Remove** at the bottom of the content pane.
4. Click **Yes** when asked to confirm the change.
5. Click **Save Changes** above the navigation tree.

Adding a Custom Category

You can create custom categories to contain your custom URLs and keywords. For example, create a custom category called **Business Related** and populate it with sites used for daily business. Sites not in the Master Database can be added to this category, as well as sites listed under different categories in the database, such as your vendors or travel agents.

A custom category must be added as a subcategory associated with a Master Database parent category. Add or view custom categories wherever a category list is shown in Websense Manager, up to 100 custom categories.

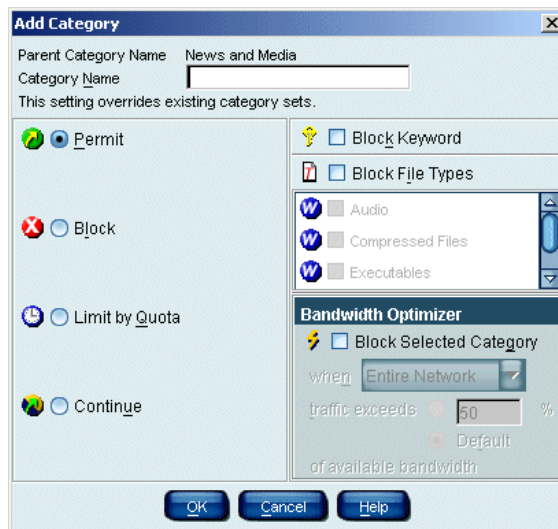
1. Expand **Filter Definitions** > **Categories** in the navigation tree. Alternatively, select any custom URLs list or keyword topic in the navigation tree. A category list appears.
2. Right-click the category under which you want to create a custom category, and then choose **Add a Custom Category**.



Shortcut menu in a category list

The **Add Category** dialog box appears.

3. Enter a **Category Name**.



Add Category dialog box

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 [Permanent Category Sets](#), page 303).
5. To apply keyword, file type, or bandwidth-based filtering, check the appropriate boxes. See [Editing a Category Set](#), page 314 for details on these filtering options.
6. Click **OK**. The custom category appears everywhere there is a category list.
7. Click **Save Changes** above the navigation tree.

Editing a Category

Follow this procedure to apply a global filtering setting to a Websense or custom category. The selection you make here 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 [Permanent Category Sets](#), page 303).
5. To apply keyword, file type, or bandwidth-based filtering, check the appropriate boxes. See [Editing a Category Set](#), page 314 for details on these filtering options.
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.

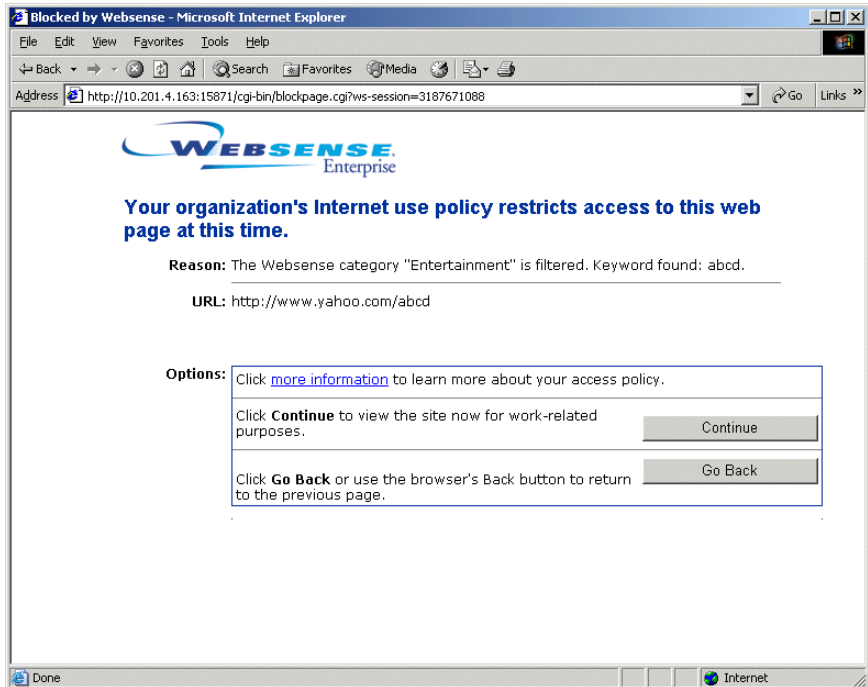
1. Right-click the custom category you want to delete in any category list, and then select **Remove this Category**.
2. Select **Yes** when asked to confirm the delete request. If the custom category has keywords associated with it, you are notified that they will be deleted as well.
3. Click **Save Changes** above the navigation tree.

Keywords

Keyword blocking is the last step in processing a site request. It offers protection against unacceptable sites that have not yet been added to the Master Database or a custom URLs list. Keywords are associated with categories in the Master Database.

When the **Block Keyword** option is active for a category, Websense software blocks any site in that category whose URL contains an associated keyword. Once you have specified a keyword for a particular category, URLs within that category that contain the specified keyword are blocked. 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, the requesting user sees a Websense block page, as shown.



Block page for a blocked keyword

The **Block Keyword** option is available at the category set level. See [Editing a Category Set, page 314](#) for more information.

Keyword blocking may result in unintended blocking of acceptable sites. 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 “sex” embedded in them.

Setting Up Keyword Blocking

1. Right-click the icon of the Policy Server you want to configure, and then select **Log On to Server**.
2. Enter the password for this server.
3. Right-click the icon again and select **Settings**. The **Settings** dialog box appears.
4. 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. The CGI query string appears after the “?” in a URL. Websense software does not search for keywords before the “?” when this option is selected.

Example: **http://search.yahoo.com/bin/search? p = Websense**
CGI query string

For more information on CGI requests, see [CGI Requests, page 78](#).

- **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 “?” when this option is selected.
- **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 “?” This is the default selection.



IMPORTANT

Do not select **Disable keyword blocking** from the drop-down list. **Disable keyword blocking** turns off all keyword blocking, even if **block keywords** is selected for a category.

5. Click **OK**.
6. Expand **Filter Definitions** in the navigation tree, and select **Keywords** to open the keyword editor.
7. Add keywords (see the next section) and associate them with Websense categories.
8. Select a named category set in the navigation tree, and then click **Edit Category Set**.
9. Check **Block Keyword** for any category to which you associated keywords (see [page 314](#)).
10. Add the keyword-blocking category set to a policy (see [Editing a Policy, page 281](#)), and then assign this policy to the appropriate clients (see [Assigning Policies to Clients, page 283](#)).

Adding Keywords

Use the keyword editor to list words or file types you want to block. Follow these guidelines:

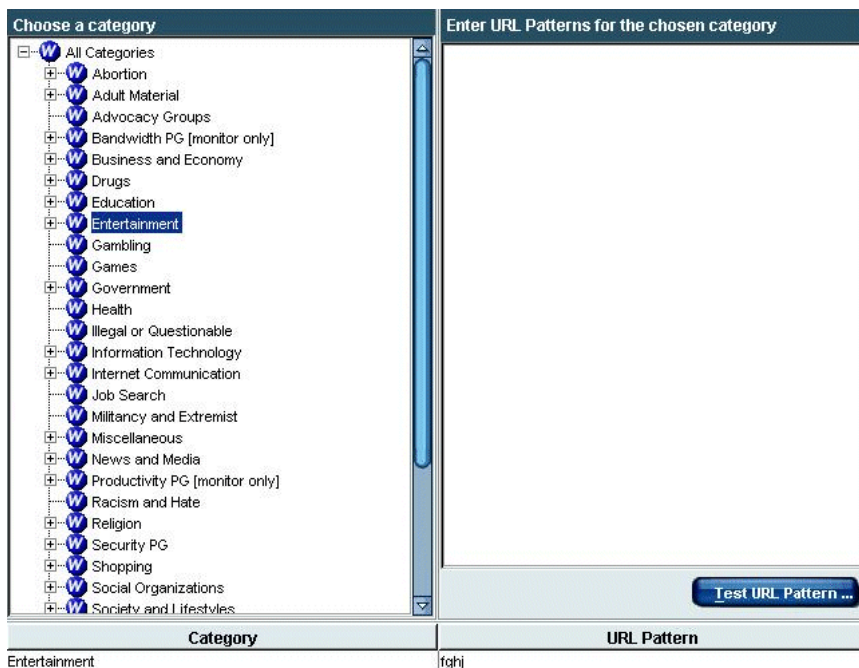
- ◆ Enter each word or file type on a separate line. If you make more than one entry per line, Websense software interprets them together as a single keyword.
- ◆ Do not use spaces between words on a line in the keyword editor. URL and CGI strings do not contain blank spaces between words, and Filtering Service looks for keywords in the URL of the requested site (*not* in the site content). Filtering Service matches exact words or character strings that you have entered as keywords.
- ◆ If any special characters such as a period (.), comma (,), pound sign (#), question mark (?), asterisk (*), or plus sign (+) appear anywhere in the keyword, enter a backslash (\) before the character. The backslash indicates that the character is part of the keyword.

For example, to block all URLs or CGI strings that include the characters *.cfm*, enter **\.cfm** into the keyword editor, instead of just *.cfm*. If you enter *.cfm* as a keyword without the backslash, Websense software ignores the period, and matches any URL or CGI string that includes *cfm*, without the period. Enter the backslash first to include the period as part of the keyword.

A special character may also be within a keyword. Instead of entering *team#1* in the keyword editor, enter **team\#1** to make the pound sign (#) part of the keyword.

To add keywords:

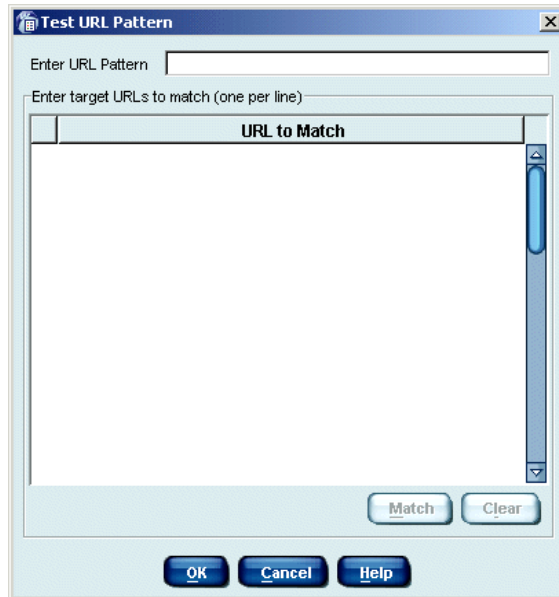
1. Select **Keywords** in the navigation tree to display the keyword editor.



Keyword editor

2. Select a category from the **Choose a category** list.
3. Enter the keywords for the selected category under **Enter URL Patterns for the chosen category**. Each keyword must be on a separate line. You can use regular expressions that are straight character strings, or expressions containing special characters.
4. Click **Add**. The keywords and their associated category are listed at the bottom of the keyword editor.

5. 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.



Test URL Pattern dialog box

- b. Enter the URL pattern to test.
 - c. Type the desired target URLs.
 - d. Click **Match**.
 - e. Click **Clear** to clear the URLs and test another pattern.
6. Click **OK** when finished.
7. Click **Add Keywords**.
8. Repeat [Step 2](#) through [Step 7](#) for each category to which you want to add keywords.
9. Click **Save Changes** above the navigation tree.



NOTE

Keyword blocking occurs only after you enable it in the **Settings** dialog box and in the appropriate category sets. See [page 332](#) for instructions.

Deleting Keywords

There is an expedient way to turn off all keyword blocking without having to delete keywords from every category. This is especially useful if you find that keyword blocking slows response time.

To disable all keyword blocking:

1. Choose **Server > Settings > Common Filtering** in Websense Manager.
2. Select **Disable keyword blocking** for **Keyword search options**.

To delete keywords:

1. Select **Keywords** in the navigation tree to display the keyword editor.
2. In the **Choose a Category** list, select the category from which you want to delete keywords.
3. Select each keyword you want 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** when asked to 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.

Managing Protocols

The Dynamic Protocol Management and Bandwidth Optimizer features enable internet filtering based on protocol, application and/or bandwidth usage. The Websense Network Agent enables protocol management. See [Network Agent, page 83](#) for more information.

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 various 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 can accurately identify these tunneling protocols, and filter 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.

If you have installed Websense Reporting Tools, 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 internet usage reporting capabilities, see your Reporting documentation.

This section discusses protocols in the following 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 in order to manage internet traffic.

Existing protocol definitions are called Websense protocols, and are sorted into named groups such as **Instant Messaging** and **File Transfer**. These protocol groups are housed in the Websense Master Database, and are verified and/or updated as frequently as nightly. For a listing of available protocols, see:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/>

Websense protocols are defined by the ports they use, IP address, or a “signature” identifying the protocol.



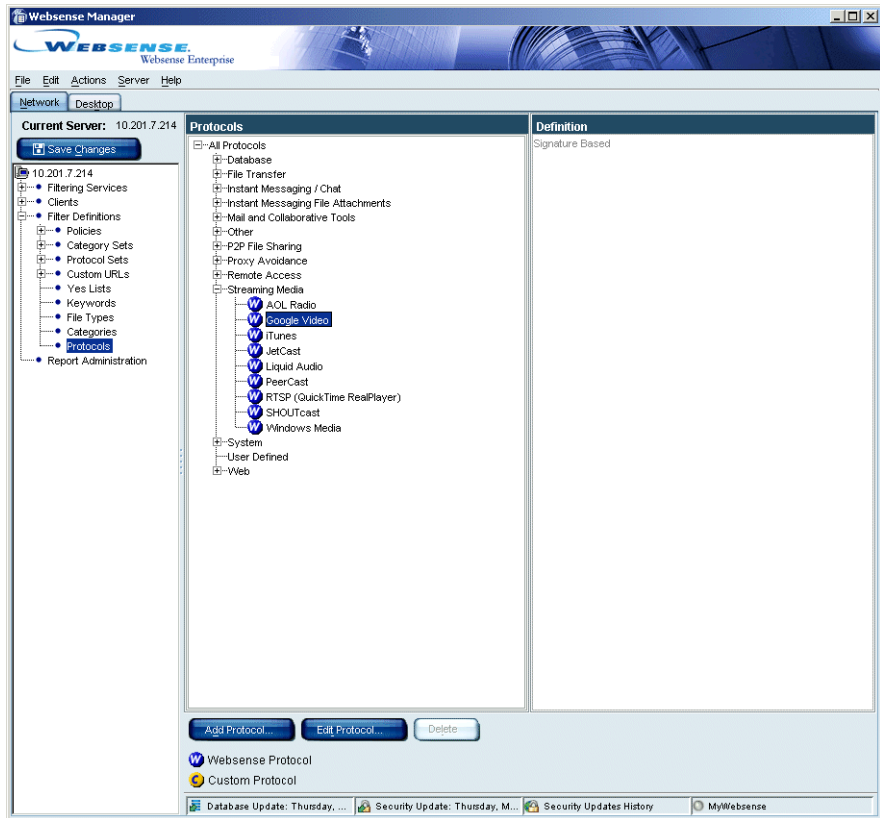
SIGNATURE-BASED PROTOCOLS

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. An initial 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, you can create and edit custom protocols according to your needs. Custom protocol definitions can be based on IP addresses or port numbers, and can be edited as needed. Websense protocol definitions cannot be edited.

View and edit protocols and *protocol sets* via Websense Manager. (A protocol set is a list of the protocols managed by a particular policy, plus the filtering settings applied to each of those protocols.)

1. Expand **Filter Definitions** in the navigation tree, and then select **Protocols**.
2. Select a protocol to display its definition.



Protocols displayed 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 when creating a new protocol (see [page 352](#)). To change this only for a particular policy, edit the protocol set used in that policy.

Port Blocking

Websense software filters internet requests based on a protocol signature or destination address, or via port blocking. 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.

See [Creating a Custom Protocol, page 352](#) and [Adding to a Websense Protocol Definition, page 356](#) to define a protocol by port number.



NOTE

Occasionally, *internal* network traffic sent over a particular port may not be blocked, even when the protocol using that port is blocked. This can happen when the protocol sends data via an internal server more quickly than the Websense Network Agent can capture and process the data. This does not occur with data from sources external to 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 organization to an external server will be blocked. However, you cannot block outbound traffic associated with a custom protocol.

You can suggest that a particular server be added to the list of destination servers that can be blocked. This list is stored in the Websense Master Database, and is maintained by Websense, Inc. Suggestions can be made at the Websense website:

<http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLChange.php>

You can also email suggestions to *databaseservices@websense.com*.

How Protocols Are Filtered

When protocol filtering is active in a policy and a protocol request is made, Websense software performs queries to:

- ◆ Determine the protocol (or internet application) name
- ◆ Identify the protocol based on the request destination address
- ◆ Search for related port numbers or IP addresses in custom protocol definitions
- ◆ Search for related port numbers, IP addresses, or signatures in Websense protocol definitions

Websense software uses these queries to filter the protocol appropriately. If Websense software cannot determine any of this information, all content associated with the protocol is permitted.

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. See *Bandwidth Management*, page 347 for details about managing network bandwidth.

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, with subsequent data sent via UDP, Websense software blocks the initial TCP request and thus disallows any subsequent UDP traffic from occurring.

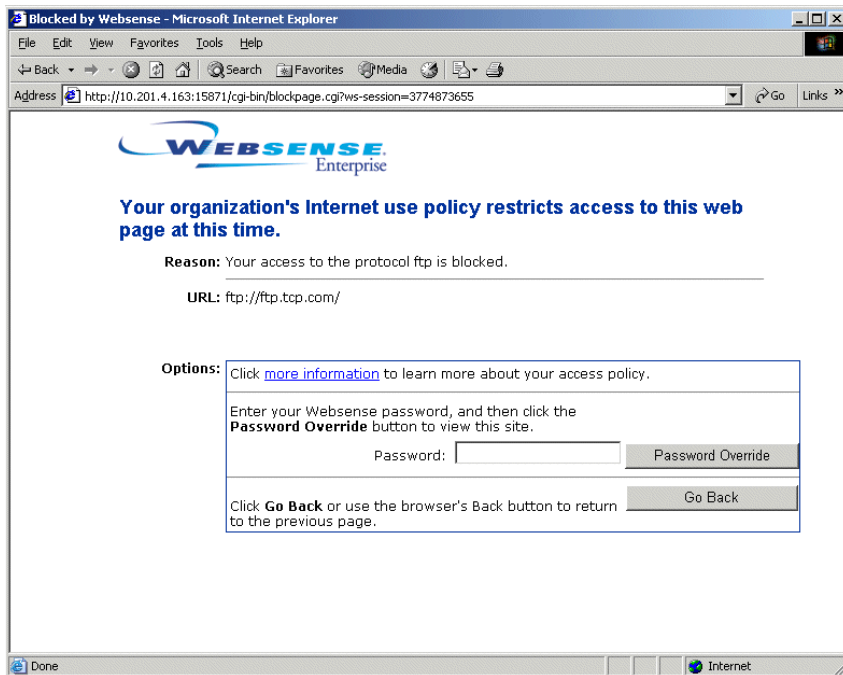
**NOTE**

UDP requests are not actually blocked, though they are logged as blocked.

Block Messages

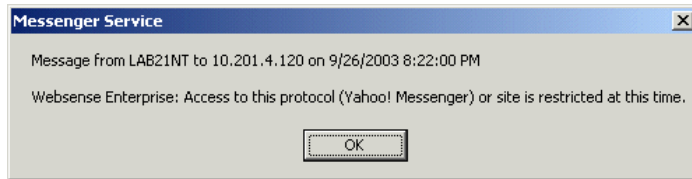
When a protocol is blocked, and a user tries to access content associated with that protocol, Websense software notifies the user in one of two ways:

- ◆ 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.



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.



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 an employee terminates the active session, Websense software blocks any requests for the protocol. This ensures that existing connections are not terminated without notice.

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.



WINDOWS XP SERVICE PACK 2

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. You can start this application from a command prompt, or configure it to start automatically by copying it into the **Startup** folder. Refer to your operating system documentation for instructions.



NOTE

Protocol block messages are not displayed on client machines running Linux or Solaris. This does not affect filtering in any way. Block *pages* display regardless of operating system.

Websense software continues to filter protocol requests whether or not protocol block messages are configured to display on user workstations.

Protocol Filtering Options

To configure filtering options for protocols, edit a protocol set. Filtering options are applied to individual protocols, and then enforced when a protocol set is applied to a policy.

Available protocol filtering options are:

- ◆ **Block/Permit:** Blocks or permits the selected protocol.
- ◆ **Log (checked/unchecked):** Tells Websense software whether to log usage data for this protocol in report output. Report data includes the number of attempted internet requests for that protocol, and bandwidth usage for that protocol. When unchecked, prevents Reporting Tools from including usage data for this protocol in report output.



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 357](#) for instructions on editing a protocol set.

- ◆ **Block Selected Protocol when:** Applies bandwidth filtering options to the selected protocol. Options include blocking the selected protocol when **[Protocol|Entire Network] traffic exceeds [Default|N%] of available bandwidth**. Default maximum bandwidth values are specified via **Server > Settings > Bandwidth Optimizer**.

**NOTE**

This option is available only if you have purchased the Websense Enterprise Bandwidth Optimizer feature (see [Bandwidth Management, page 347](#)).

For details on filtering protocols based on bandwidth usage, see [Bandwidth Management, page 347](#).

**NOTE**

By default, new protocol definitions are permitted, and are not logged.

To manage a particular protocol in the same manner for all users, define a protocol to be always permitted or always blocked for all users. (The protocol must have the same filtering option 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. See your installation guide for instructions on enabling Websense filtering in a SOCKS/WinSOCK environment.

See [Practical Applications, page 385](#) for examples of how you can use the protocol management feature.

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 feature enhances the default IM controls by allowing you to permit certain IM traffic while blocking the transfer of attachments by those IM clients.

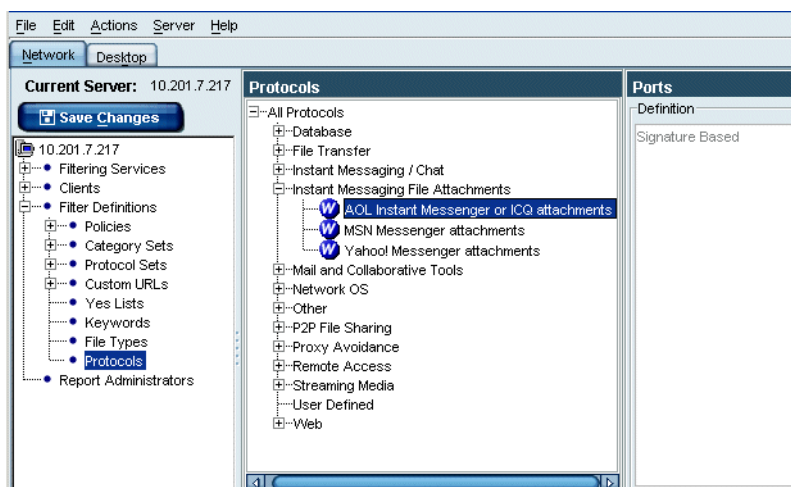
Instant Messaging File Attachments comprises a separate group of network protocols for IM file attachments. This group includes entries for IM clients such as MSN, AOL/ICQ, and Yahoo.



NOTE

IM attachment filtering can be applied to internal traffic as well. To enable this, define the portion of your network you want to monitor via the Network Agent Global settings (see *Initial Configuration*, page 85).

When the IM Attachment Manager is activated, the Instant Messaging File Attachments protocols are displayed with the protocol list in Websense Manager, as shown.



Instant Messaging File Attachments protocols in Websense Manager

The Instant Messaging File Attachments group of protocols is included in all protocol sets. You can modify the filtering setting for these protocols in any protocol set, or create a new protocol set that indicates a particular filtering setting for Instant Messaging File Attachments. See *Protocol Filtering Options*, page 344 for filtering option descriptions.

Bandwidth Management

Websense software can filter internet sites, protocols or applications based on bandwidth usage. This threshold filtering restricts internet content based on available network bandwidth. Websense software allows you to specify filtering settings that limit user access to sites, protocols or applications based on bandwidth usage. The ability to limit internet access based on available network bandwidth is provided with Websense Enterprise® Bandwidth Optimizer, an optional feature available for purchase.

You can 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.

Bandwidth usage per protocol is bandwidth usage over all the ports, IP addresses or signatures defined for that protocol. A port-based protocol uses all ports specified in its protocol definition. Some protocols or internet applications use a single port, while others “hop” ports, or use more than one port for data transfer. Some peer-to-peer applications, however, can select from multiple ports to transfer data.

Websense software effectively monitors and blocks protocols that use multiple ports via multiple port entries in its protocol definitions. However, if an internet application uses a port not in its definition, network traffic over that port is not included in bandwidth usage measurements. Websense, Inc. ensures that Websense protocol definitions are updated regularly to ensure a high level of bandwidth measurement accuracy.

Bandwidth Limits

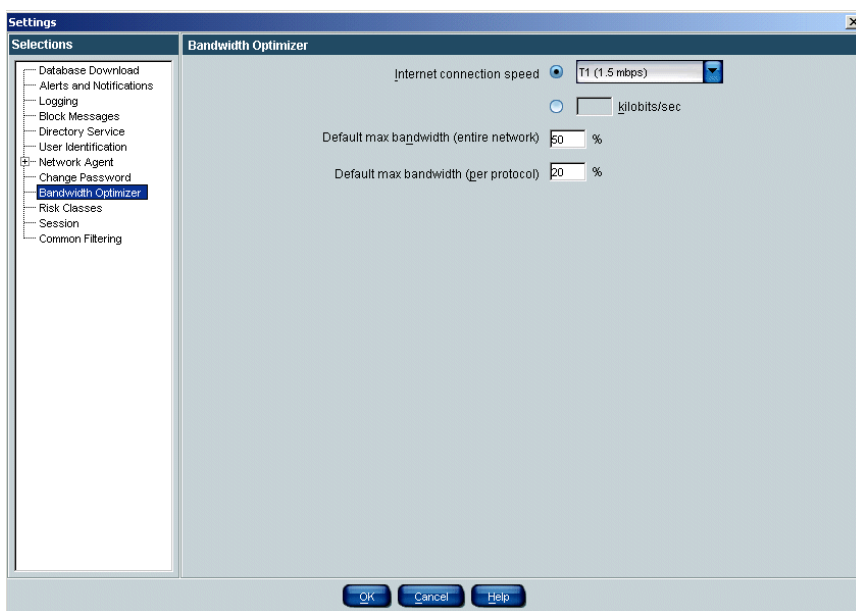
Before specifying bandwidth settings in policies, verify the default bandwidth limits that serve as the basis for filtering settings. The default maximum values in the **Settings** dialog box under **Bandwidth Optimizer** are as follows:

Default max bandwidth (entire network): 50%

Default max bandwidth (per protocol): 20%

To change the default maximum values for bandwidth:

1. In Websense Manager, choose **Server > Settings**.
2. Select **Bandwidth Optimizer** in the list at the left.



Default bandwidth values for Bandwidth Optimizer

3. Edit the bandwidth percentage values as desired.
4. Click **OK**.

The new values you entered will be applied whenever filtering based on bandwidth usage is active.

**NOTE**

Default bandwidth values apply to all instances of Network Agent installed in your network, whether or not they reside on the same machine as Websense Manager. These default values are stored in Policy Server, which communicates with all instances of Websense Manager.

If you have multiple Policy Servers in your network, each Policy Server affects only its own network segment. See [page 47](#) for information about using multiple Policy Servers.

To manage bandwidth usage associated with a particular protocol, edit the protocol set associated with the appropriate policy. The bandwidth usage 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. 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. These ports are specified via **Server > Settings > Network Agent**. To set bandwidth limitations for URL (HTTP) requests, see [Editing a Category Set, page 314](#).

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 against the information in its user map.

If transparent identification is enabled in your network, and no match is found between the source IP address and a user name in its map, 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.

If the user cannot be identified, or your network configuration does not support transparent identification, Websense software attempts to resolve 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.

See [page 125](#) for information about transparent identification and its configuration requirements.

If Websense *manual authentication* (see [page 208](#)) is enabled, Websense software identifies users by prompting them 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.

The following permanent protocol sets are predefined in Websense Manager:

- ◆ **Default Settings:** This is the default protocol set that is 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. 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, you can 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 provides instructions for customizing protocol definitions and associated policies:

- ◆ Create a custom protocol (see [page 352](#)).
- ◆ Edit a custom protocol (see [page 355](#)).
- ◆ Remove a custom protocol (see [page 355](#)).
- ◆ Add to a Websense protocol definition (see [page 356](#)).

Creating a Custom Protocol

Follow these instructions to create a new protocol definition, in addition to the protocol definitions Websense, Inc. provides. New protocols must be defined by port number or IP address.

1. In Websense Manager, expand **Filter Definitions** > **Protocols** in the navigation tree. The existing protocol groups are displayed in the content pane.
2. Select the protocol group to which you want to add the new protocol.
3. Click **Add Protocol**.

Add Protocol

Protocol Group: Streaming Media

Protocol Name:

Protocol Identifiers

Port/Port Range	IP Address/Range	Transport Method
-----------------	------------------	------------------

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:

traffic exceeds: %

Default

of available bandwidth

Add Protocol dialog box

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 and/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 one 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 will overlap 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 will be 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 to that protocol in all protocol sets.
8. If you have purchased Bandwidth Optimizer, you can elect to block this protocol based on bandwidth usage. See [Bandwidth Management, page 347](#) for more information about Bandwidth Optimizer.
9. Click **OK** to save the new protocol definition.
10. Follow the instructions on [page 359](#) to configure a policy for protocol-based filtering.

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**.
4. To change a protocol identifier, select the row, and then click **Edit**. Modify criteria, following the guidelines under [Creating a Custom Protocol](#), page 352. Click **OK**.
5. To change the filtering setting for this protocol, check **Apply to all protocol sets**.
 - a. Select **Permit** or **Block**.



IMPORTANT

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**.

Removing a Protocol

You can only remove custom protocols, and not Websense protocols.

1. In Websense Manager, expand **Filter Definitions** > **Protocols** in the navigation tree. The existing protocol groups are displayed in the content pane.
2. Under **Protocols**, expand the appropriate protocol group.
3. Select the custom protocol whose definition you want to remove.
4. Click **Delete** at the bottom of the content pane. The **Delete Protocol** dialog box appears.
5. Click **Yes** to confirm deletion of the selected protocol.

The deleted protocol can no longer be used in any filtering policies.

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. In Websense Manager, expand **Filter Definitions** > **Protocols** in the navigation tree. The existing protocol groups are displayed in the content pane.
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, following the instructions on [page 352](#).

Add or change port numbers as needed.



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.

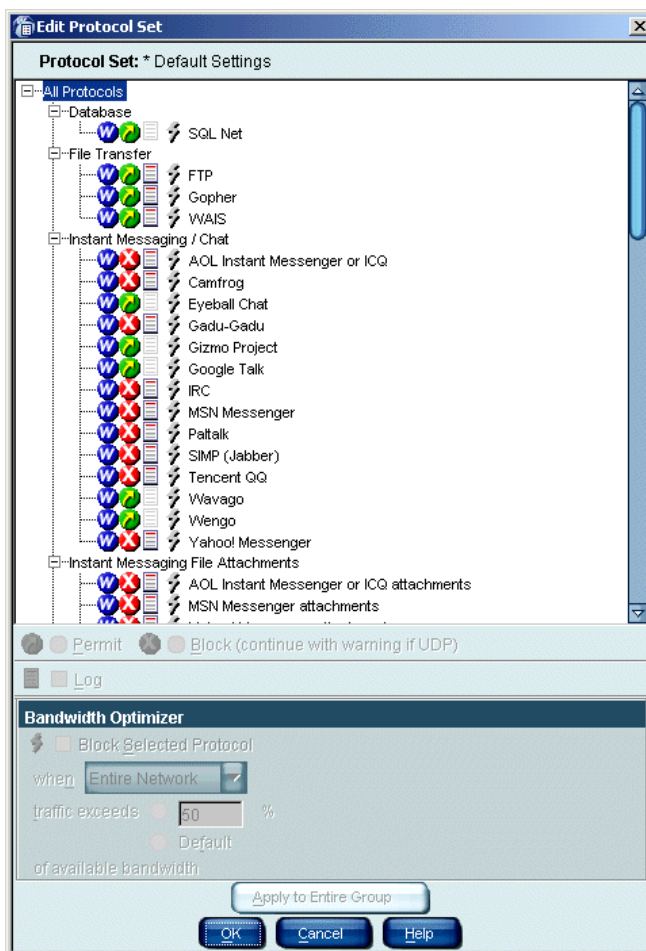
4. Click **Save Changes** above the navigation tree.

Adding a Protocol Set

1. In Websense Manager, right-click in the navigation tree, and then choose **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 will not be used in filtering until it is added to a policy (see [page 359](#)).

Editing a Protocol Set

1. In Websense Manager, 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 top left-hand corner of the content pane). The **Edit Protocol Set** dialog box appears.



Edit Protocol Set dialog box

4. Customize the filtering settings for a protocol by selecting the protocol and specifying the desired filtering options.

For a description of the available filtering options for protocols, see [page 341](#). By default, any new protocols created or downloaded after Websense software was installed have the **Permit** option checked, and the **Log** option *unchecked*.

5. To optionally apply the selected filtering options to the whole protocol group, click **Apply to Entire Group**.
6. Click **OK** to save the modified protocol set.

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

If the protocol set is already included in a policy, the new filtering options are automatically 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 *File Types*, page 297). In this case, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

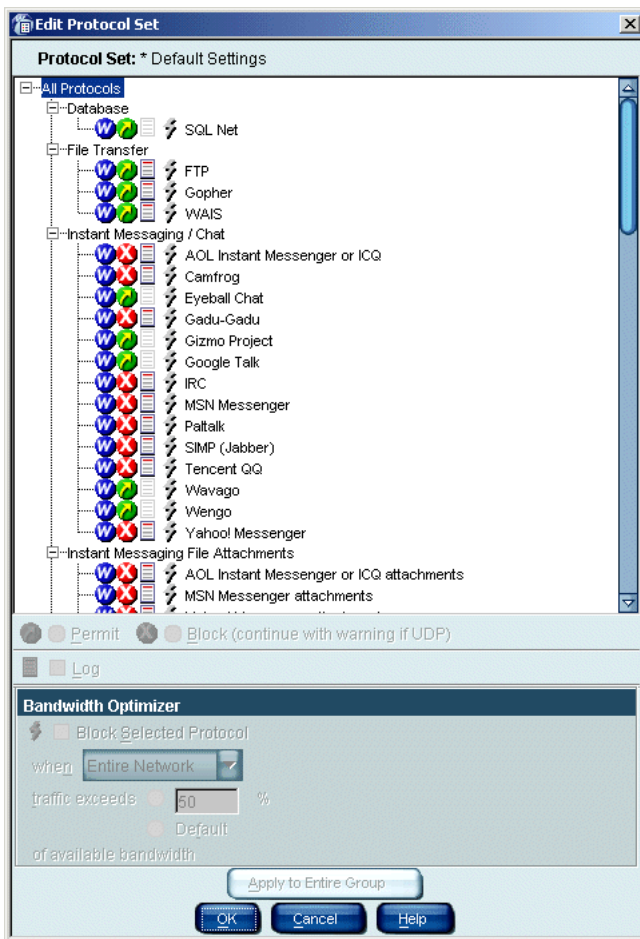
See [page 407](#) for an example of how to set up full video and audio filtering.

Before implementing protocol management or bandwidth-based filtering options, verify that the default server settings for Network Agent fit your network configuration (see [page 85](#)).

To configure a policy to filter internet requests based on protocols or applications.

1. In the Websense Manager navigation tree, expand **Filter Definitions > Policies**.
2. Select the policy with which you want 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 you want to edit.
6. Click **Edit**. The **Edit Protocol Set** dialog box appears.



Edit Protocol Set dialog box

7. Select the protocol for which you want to configure filtering options.

8. Select the filtering options you want to apply to the selected protocol or protocols (see *Protocol Filtering Options*, page 344).



NOTE

You can also modify protocol filtering options by editing a protocol set, as described under *Editing a Protocol Set*, page 357. Changes made to a protocol set apply wherever that protocol set is used in a policy.

9. To apply the selected filtering options 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.



NOTE

Websense services do not need to be stopped and then restarted in order to activate protocol set configuration changes.

Websense software is configured to manage the selected protocols for the group governed by the policy you just modified.

CHAPTER 10 | Troubleshooting

Should you encounter a problem not addressed in the previous chapters, following are previously-encountered problems and suggested solutions. If you encounter a problem, please check this chapter before you contact Technical Support.

The Websense website also features an extensive knowledge base. Search topics by keyword or by reference number (if known). Check the Top Ten FAQs for answers to commonly-asked questions. The Websense Knowledge Base is at <http://www.websense.com/global/en/SupportAndKB/>.

Problems addressed in this chapter are as follows:

- ◆ The Master Database does not download ([page 364](#))
- ◆ Master Database download doesn't occur at the time specified ([page 367](#))
- ◆ I made a mistake during installation ([page 367](#))
- ◆ Where can I find download and error messages? ([page 367](#))
- ◆ I forgot my Policy Server password ([page 368](#))
- ◆ I cannot log on to Policy Server via Websense Manager ([page 368](#))
- ◆ Sites in the Information Technology category are being blocked ([page 368](#))
- ◆ Online Help shows a blank frame when viewed in Netscape 6.x ([page 369](#))
- ◆ Keywords are not being blocked ([page 369](#))
- ◆ Sites in blocked categories are not always being blocked ([page 370](#))
- ◆ Custom or yes list URLs are not being filtered as expected ([page 370](#))
- ◆ A Websense block message does not appear for a blocked file ([page 371](#))
- ◆ A blank white page displays instead of the block message ([page 373](#))
- ◆ A "Page not found" error appears instead of a block message ([page 373](#))
- ◆ A protocol block message does not appear in Windows ([page 373](#))
- ◆ A protocol block message appears instead of a block page ([page 374](#))
- ◆ Protocol block messages do not appear as expected ([page 374](#))
- ◆ Some protocol requests are not being logged ([page 374](#))

- ◆ A user cannot access a protocol or application as expected ([page 375](#))
- ◆ An FTP protocol request is not blocked as expected ([page 375](#))
- ◆ Two log records are generated for a single request ([page 375](#))
- ◆ Websense is not filtering based on a directory object policy ([page 376](#))
- ◆ Directory objects are incorrectly filtered by the **Global** policy ([page 379](#))
- ◆ Remote users are not being filtered correctly ([page 380](#))
- ◆ RADIUS Agent does not start ([page 380](#))
- ◆ eDirectory Agent mis-counts eDirectory Server connections ([page 381](#))
- ◆ Quota, continue, or password override doesn't work as expected ([page 381](#))
- ◆ Manager does not display distributed policy information ([page 382](#))
- ◆ Distributed policy configuration data is lost ([page 382](#))
- ◆ An authentication error appears during policy distribution ([page 382](#))
- ◆ Filtering does not occur after an IP address change ([page 383](#))
- ◆ User authentication fails in an English operating system set for an Asian locale ([page 383](#))
- ◆ RTA does not report information immediately after restarting ([page 384](#))
- ◆ An alert appears stating that RTA cannot contact Policy Server ([page 384](#))

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. In Websense Manager, choose **Server > Settings**, and then select **Database Download** at the left.

- ◆ Compare the key you received via email or in the Websense package to the key in the **Subscription key** field. The key must be entered and must use the same capitalization as shown in your key document. You must click **OK** to close the **Settings** dialog box before the key takes effect 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.



IMPORTANT

If you edit host files and/or routing tables in a firewall or internet router that restrict the URLs a Websense server can access, permit the following:

download.websense.com

ddsdom.websense.com

ddsint.websense.com

portal.websense.com

www.my.websense.com

To access database downloads and your Websense subscription data, you must permit these URLs.

To verify internet access, first determine whether Websense software is accessing the internet through a proxy server.

1. In Websense Manager, Choose **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 following address:
<http://www.websense.com/global/en/Downloads/>
5. If you reach the site, the Websense logo appears, along with a message indicating that you will be redirected to the Websense home page. This means Policy Server's proxy settings are correct, and Policy Server should have appropriate HTTP access for downloading.

If you are not able to reach the download site, and the system requires proxy information, the Policy Server proxy settings need to be corrected.

If no proxy information is required, use the `nslookup` command with the address of your download site to make sure the Policy Server machine is able to resolve the download location to an IP address. For example:

```
nslookup asia.download.websense.com
```

If this does not return an IP address, you must set up the system running Websense software to access a DNS server. If you need assistance, contact Websense Technical Support (see *Appendix A* for contact information).

If Websense software must access the internet through an upstream firewall or proxy server that requires authentication, check the following:

- ◆ The correct user name and password must be entered under **Database Download** in the **Settings** dialog box. Verify spelling and capitalization.
- ◆ The firewall or proxy server must be 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 will be unable to download the database. Make appropriate changes on the firewall, or change the download times under **Database Download** in the **Settings** dialog box.

If you are running Websense software behind a Gauntlet firewall, check the FAQs at www.websense.com/support for specific information about running Websense software behind your firewall.

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 troubleshooting topic, *The Master Database does not download*, page 364.

I made a mistake during installation

Run the installation program again, choosing either the **Modify** option (Windows) or the **Continue installation and overwrite current configuration settings** option (Solaris or Linux), whichever is appropriate.

Where can I find download and error messages?

Windows NT

Check the Windows Application Event log for any listings about database download as well as other error and status messages. The Application Event log is accessed via **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 as well as other error or status messages. The Application Event log is accessed 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.

I forgot my Policy Server password

If you forget your Policy Server password, call Websense Technical Support for assistance (see [page 409](#) for contact information).

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, you must remove the old server from Websense Manager, add the server with its new IP address, and then log on to the server again. See [page 212](#) for instructions on adding, logging on to, and removing Policy Server.

If Websense Manager has been stopped via the `kill` (Linux/Solaris) or **End Task** (Windows) commands, you must restart the Websense Policy Server in order to log on to Policy Server again. See [Stopping or Starting Websense Services, page 217](#). Alternatively, you can wait for the current Policy Server session to time out (see [Session Management, page 258](#)).

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 217](#)), and then log on again. Policy Server remembers who was previously logged on.

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. This means that 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 to be a search request, not a site request. It then displays the most likely site the user is looking for, along with a list of closely matching sites.

Because Internet Explorer handles the user's requested site as a search request, 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, searching from the Address bar must be turned off in Internet Explorer.

To turn off searching from the Address bar, do the following. These steps apply to Internet Explorer versions 4.0, 4.01, 4.1 (Service Pack 1, Service Pack 5 for Windows 95 and Windows NT 4.0), 5.0, and 6.0.

1. From the **Tools** menu, choose **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**.

Online Help shows a blank frame when viewed in Netscape 6.x

Online Help uses Java to display the contents, index, and search options in the left frame. The *typical* installation of Netscape version 6.x does not install Java components.

To correct this problem and view the online help completely, reinstall Netscape 6.x and select either **Complete** or **Custom** when prompted for a setup type. If you select the **Custom** installation, be sure to check **Sun Java 2** when presented with a list of possible components.

Keywords are not being blocked

Some possible reasons for this problem are described below.

- ◆ You may have **Disable keyword blocking** selected in Websense Manager, under **Settings > Common Filtering**. Follow these steps to correct the problem.
 - a. Right-click the Policy Server icon, and then choose **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, URLs containing blocked keywords are still accessible to users.

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 sometimes, 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.

Follow these steps to prevent access to blocked websites via virtually hosting IP addresses.

1. Select **Custom URLs/Recategorized** in the Websense Manager navigation tree. The Custom URLs editor appears in the content pane.
2. Under **Choose a Category**, select **User-Defined**.
3. Under **Enter URLs for the highlighted category**, type the following:

<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.
6. Click **Save Changes** above the navigation tree.

If users enter IP addresses for sites in blocked categories, they will not be able to access those sites.

Custom or yes list URLs are not being 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 the URL on 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 one domain.

A Websense block message does not appear for a blocked file

If a block message does not appear for a blocked file type, it may be because the block message is called but is not visible to the user. For example, when a website is designed so that 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 will still not be able to access or download the blocked file. If Filtering Service is installed on a multi-homed machine, identify Filtering Service in your network by the method listed under the appropriate operating system.

Windows

- ◆ Enter the IP address of the machine running Filtering Service as a resource record in your DNS server. See your DNS server documentation for instructions.
- ◆ *If you do not have internal DNS:* Add an entry to the **EIMserver.ini** file by following these instructions.
 - a. Open the Windows **Services** dialog box.
 - Windows NT/2003:* Choose **Start > Settings > Control Panel**, and then double-click **Services**.
 - Windows 2000:* Choose **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 the following command 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. See your DNS server documentation for instructions.
- ◆ *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 the following command 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 217).

A blank white page displays instead of the block message

Some possible reasons for this problem 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 another graphic file indicator, have the user reenter the URL in the address bar, leaving off the *.gif portion. The page will then be displayed if it is in a permitted category, or a block message will be presented.
- ◆ Some older browsers may not automatically detect the encoding (character set) 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). Refer to the Netscape or Microsoft Internet Explorer documentation for details.

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. Though this is not a common scenario, verify that the browser is not set to use an *external* proxy.

A protocol block message does not appear in Windows

In Windows NT and 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. Open the **Services** dialog box and check to see if the Messenger service is running.

In Windows 98, the **winpopup.exe** application must be running for the block message to display. You can start **winpopup.exe** from the command prompt or copy it into the **Startup** folder on your local drive to have it run automatically at startup.

The Websense User Service must be installed on a Windows machine in order for protocol block messages to display properly. See your installation guide for detailed requirements and instructions.

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, an HTTPS site request that is blocked via category settings may be interpreted by Network Agent as a protocol request. This results in a protocol block message being displayed. The HTTPS request is also logged as a protocol request.

Protocol block messages do not appear as expected

- ◆ Block pages and/or protocol block messages may not reach client machines if Network Agent is installed on a machine with multiple network interface cards (NICs), and one NIC is monitoring a network segment separate from Filtering Service. To enable block page display, ensure that client machines have HTTP access to the network segment where Filtering Service is installed. To enable protocol block message display, 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). This can occur when Network Agent is configured to monitor requests *to* internal machines.

Some protocol requests are not being logged

A few protocols, such as those used by ICQ and AOL, prompt requesting 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 (see [page 370](#)) and/or Reporter (see [page 37](#)).

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 as the integrated proxy, 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 then 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.

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 two requests for each single HTTP or protocol request made from the Websense Network Agent machine. (This duplication does not occur with internet requests made by client machines within your network.)

To fix the problem, you can disable Windows QoS Packet Scheduler on the Network Agent machine.

This problem will *not* occur if you use Network Agent for all logging purposes. See your installation guide for details about enabling full logging.

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 have been assigned, please read the following suggestions. (Additional suggestions are available in Websense Knowledge Base item 493.)

- ◆ If you have not added directory objects to Websense Manager, users are filtered by workstation or network policies (if created), or by the **Global** policy. See [Adding Directory Objects, page 107](#) for information about adding directory objects to Websense Manager so you can assign policies to them.
- ◆ If your integration product is Microsoft ISA Server, check to make sure 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 will not be applied to users belonging to a sub-group, and not directly to the parent group. See your directory service documentation for details on user and group hierarchies.
- ◆ If you installed the 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: Choose **Start > Programs > Administrative Tools > Services** (*Windows 2000*). Right-click **Websense DC Agent**, and then choose **Properties**. Change **local** to **administrator**.
 - DC Agent and/or User Service may have been installed as a service using the Guest account. The Guest account is 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, then when DC Agent attempts to get the list as a Guest, it will not be allowed to download the list.

Go to the machine running the domain controller and follow these steps. Stopping the DC Agent and User Service services could stop transparent access to the internet until you restart those services.

- a. Create a user account such as **websense** in your domain controller. You can use an existing account, but setting up a Websense account is preferable so that the password can be set not to expire. No special privileges are required.
Set the password never to expire. This account's only function is to provide 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 to display the **Service** dialog box.
- e. On the **Log On** tab, select the **This account** option.
- f. In the text box, 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 three 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, perform the following workaround.

1. From the Windows **Start** menu on the client machine, choose **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.

DC Agent or Logon Agent can now get user logon information from this machine.

- ◆ If you have deployed the Websense eDirectory Agent, a user may not be identified and/or 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 for one of several reasons:
 - 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 Websense Manager, under **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. As a backup measure, if there are shared workstations in your network where users log on anonymously, you can 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 181](#).
- 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 you see that a user is being identified, but is still not being filtered as expected, check your Websense 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 the following:

- 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 the service is running under. 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\$. Simply add the following entry in 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 your 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 doesn't recognize RADIUS Agent as a client (source of RADIUS requests). Ensure that your RADIUS server is configured as described under *Configuring the RADIUS Environment*, page 152.

You can use RADIUS Agent's built-in diagnostic tool to isolate communication problems with Filtering Service, or other causes of filtering problems. See *Troubleshooting RADIUS Agent*, page 168 for instructions on activating the tool.

If you have implemented the Remote Filtering feature (see *Filtering Remote Clients*, page 120), remote users cannot be filtered if the Remote Filtering Client installed on the client machine cannot communicate with the Remote Filtering Server within the network.

See your installation guide for instructions on setting up Remote Filtering.

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).

The usual cause is that 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 only shows 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 an unlikely scenario and affects a small minority of users.

To work around this limitation, you can optionally add a parameter to the **wsedir.ini** file that will count server connections accurately.

To add the parameter (*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 the following 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.

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, one of the following reasons may apply. Quota, continue, or password override functions may not behave as expected when:

- ◆ An internet transaction is interrupted. For example, while 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. This resends the same request to the external server. The external 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. See [page 47](#) for more information about using multiple Policy Servers.

Manager does not display distributed policy information

This can occur when an administrator is 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

If this occurs, two 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, choose **Server > Distribution Settings** in Websense Manager. In the **Server Distribution Settings** dialog box, verify that an appropriate password is entered for each destination Policy Server. Then, try again to distribute policy data.

Filtering does not occur after an IP address change

If filtering stops after you have changed the IP address of a machine running a Websense component, it could be because Policy Server does not recognize the change. Refer to [Changing an IP Address, page 222](#) for details about configuring IP address changes.

To troubleshoot this problem:

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, for security reasons, 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 217](#)). You can disable `secureid` again after making the change.

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) via Control Panel (**Regional Settings/Options**), Websense software will be unable to authenticate users unless the Policy Server locale is set to the appropriate language. The user might be prompted to log on manually (which will fail) or will be filtered by the **Global** policy, depending on your Websense configuration.

The same issue exists with 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 217.)
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.

Practical Applications

Websense is a powerful system for managing internet access in your organization. With easy-to-use tools like Websense Manager, Reporter and Real-Time Analyzer, Websense software provides a secure solution for the internet usage issues you encounter.

This chapter introduces the varied capabilities of Websense software and demonstrates its flexibility in addressing internet access management situations. Scenarios begin with simple monitoring, and then introduce concepts such as policies, custom URLs, keyword blocking, quotas, and transparent identification. Each scenario provides an overview of the steps required to accomplish the recommended changes.

Each scenario highlights a different Websense feature and builds on information given in previous scenarios. By the end of the chapter, you will have an overview of many of the capabilities of Websense software. The scenarios are slanted toward a corporate environment, but can be applied to any organization.

Scenario 1: Monitoring Access Trends

This scenario serves as a starting point for managing internet access. Install the necessary components in your network and then generate and view reports of internet activity. Initially, Websense software blocks some categories and permits others.

1. Install Websense software (see your installation guide).
2. Install or upgrade Websense Reporting Tools v6.1, and install Log Server on a different machine in the network (for optimal performance).

Websense Reporting Tools, a separate suite of programs included with Websense software, are used to generate reports of internet activity. Log Server, installed with Reporter, must be installed in order for internet activity to be logged. Refer to the Reporting documentation for installation instructions.



NOTE

Websense software sends log information that can only be read by the corresponding version of the Websense Reporting Tools. Install or upgrade as indicated in your installation guide in order to generate reports.

3. After installation, the **Global** policy directs Websense software to filter requests according to default settings from 00:00 to 24:00, seven days a week.

The **Default Settings** category set blocks the Adult Content, Nudity, Sex, 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, and Weapons categories by default, and limits some other categories by quota (see [page 49](#) for information about quota time).

The **Default Settings** protocol set blocks the Instant Messaging/Chat, Instant Messaging File Attachments, P2P File Sharing, and Proxy Avoidance protocol groups by default.

4. Run Websense software with the default settings for a period of one to two weeks. During this period, Log Server tracks all filtered internet requests. It records the site or protocol requested and any category assignment. It also tracks whether the request was permitted, blocked, or limited by quota.
5. Set up reporting roles to determine which administrators can run reports, and for which clients. See your Reporting documentation for instructions).
6. Run Reporter or Explorer to view easy-to-read reports and charts depicting your organization's internet access trends. Refer to the Websense Enterprise Reporting documentation for information on generating reports.
7. For a dynamic, real-time assessment of internet usage trends in your network, take advantage of Websense Real-Time Analyzer, a built-in, browser-based reporting tool. See your Reporting documentation or Real-Time Analyzer online Help for details.

The Websense Reporting Tools can help you identify network bandwidth use, high/low internet traffic periods, types of sites most frequently visited, and much more.

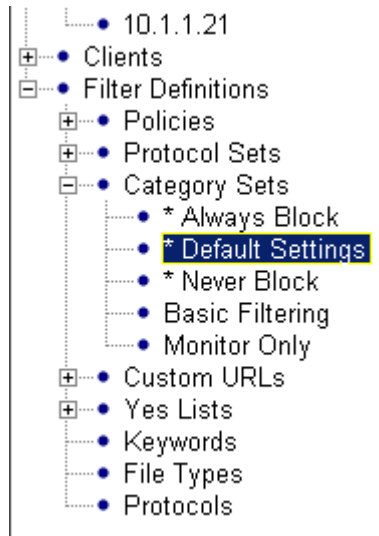
If authentication is enabled, Reporter or Explorer can generate reports by user name and group, letting you identify any potential abusers of internet privileges.

Scenario 2: Permitting Travel Sites

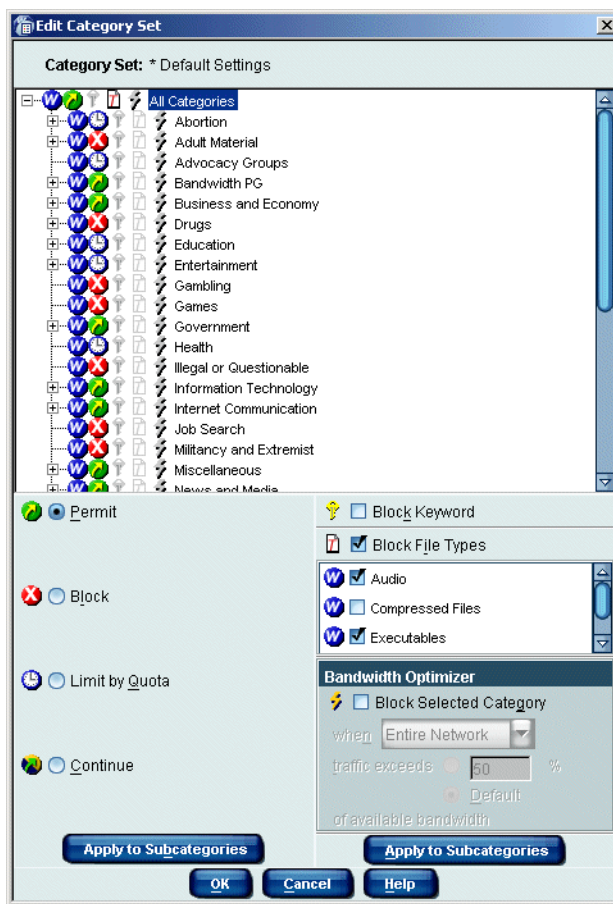
Upon reviewing the reports, you realize that many employees are using travel-related sites to make travel arrangements for business purposes. With the initial Websense setup, an employee requesting a travel site is given the option to view it for work-related purposes, but only for a brief time. You decide to provide open access to the Travel category so that employees can easily access travel sites during working hours.

Because Websense software filters sites by category, you can grant access to travel sites by editing the **Default Settings** category set. See [page 314](#) for more details on editing a category set.

1. Open Websense Manager and expand **Filter Definitions > Category Sets > Default Settings** in the navigation tree.



2. Locate the category set details in the content pane, and then click **Edit**. The **Edit Category Set** dialog box appears.



Edit Category Set dialog box

3. Select the **Travel** category.
4. Select **Permit**.
5. Click **OK**.
6. Click **Save Changes** above the navigation tree.

Category sets determine how Websense software filters site requests. Editing the **Default Settings** category set changes the way Websense software filters requests from all users. Once Policy Server has been updated, any requests made for travel sites are automatically permitted.

Scenario 3: Deferring News and Media Sites

Upon analyzing reports generated by Reporter or Explorer, you realize that the largest non-work-related use of the internet is accessing news sites. You don't mind employees being able to access news and media sites before and after work, or during the lunch hour. However, your employees are generally viewing news sites for personal reasons, and you don't want work time and resources spent on personal news reading.

The solution: Add a new category set that blocks the News and Media category, with no option to continue and view the page. After adding the new category set, edit the **Global** policy to filter site requests with this new category set during business hours.

Add a Category Set

Adding a category set is necessary when you want to customize how Websense software filters sites during different days or time periods, or for different people. See [page 313](#) for more details about adding a category set.

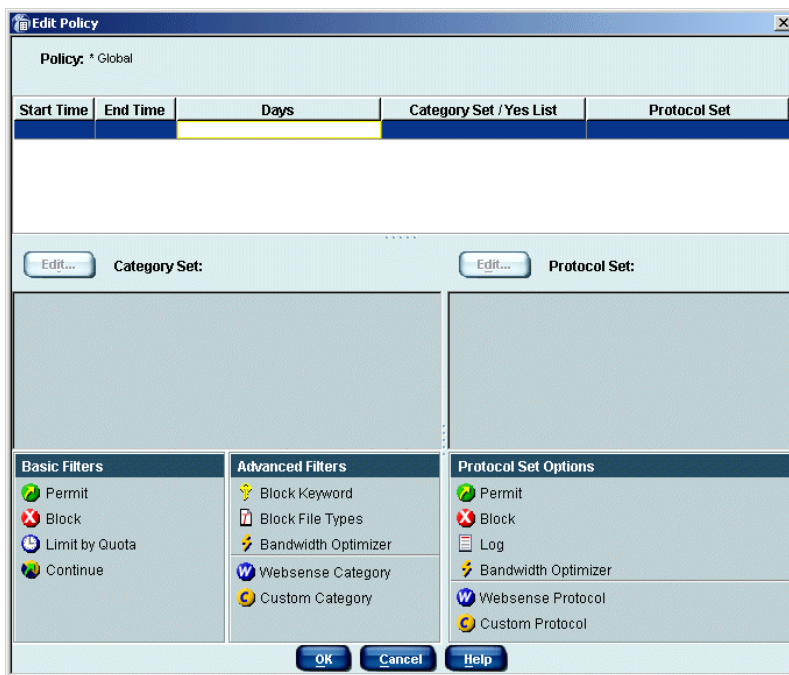
1. Right-click in the navigation tree, and then select **Add Category Set**.
The **Add Category Set** dialog box appears.
2. Name the new category set **Business Hours**. Click **OK**.
3. Choose **Default Settings** as the basis for the new category set. Click **OK**.
4. Select the **Business Hours** category set in the navigation tree.
5. Locate the category set details in the content pane, and then click **Edit**.
6. Select the **News and Media** category, and then select the **Block** filtering option.
7. Click **OK**.
8. Click **Save Changes** above the navigation tree.

Now that you have created a new category set, tell Websense software when to use it by editing the **Global** policy.

Edit the Policy

Editing a policy is necessary when you want to enforce different category sets based on the time or day of the week. Websense software uses a 24-hour clock, since category sets can be scheduled at any time. For example, 1:00 PM is entered as 13:00. See [page 281](#) for more details on editing a policy.

1. Expand **Filter Definitions > Policies** in the navigation tree.
2. Select the **Global** policy. Its policy settings appear in the content pane.
3. Click **Edit**.
4. Right-click each row and select **Delete Row** so that the table is cleared.



Global policy with policy table cleared

5. Double-click each field in the first row and set the following values:
 - Start Time**—00:00
 - End Time**—08:00
 - Days**—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
 - Category Set**—Basic Filtering
 - Protocol Set**—Default Settings
6. Double-click each field in the second row and set the following values:
 - Start Time**—08:00
 - End Time**—12:00
 - Days**—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
 - Category Set**—Business Hours
 - Protocol Set**—Default Settings
7. Double-click each field in the third row and set the following values:
 - Start Time**—12:00
 - End Time**—13:00
 - Days**—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
 - Category Set**—Default Settings
 - Protocol Set**—Default Settings
8. Double-click each field in the fourth row and set the following values:
 - Start Time**—13:00
 - End Time**—17:00
 - Days**—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
 - Category Set**—Business Hours
 - Protocol Set**—Default Settings

9. Double-click each field in the fifth row and set the following values:

Start Time—17:00

End Time—24:00

Days—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Category Set—Basic Filtering

Protocol Set—Default Settings

10. Exit the table area by clicking outside the table or by pressing **Ctrl+Shift+Tab**.
11. Click **OK** to save the changes you made to the **Global** policy and close the **Edit Policy** dialog box.
12. Click **Save Changes** above the navigation tree.

You have just edited the **Global** policy to enforce the **Business Hours** category set for all employees during business hours.

Once you click **Save Changes** to implement this policy, all requests for news and media sites made during business hours are blocked. There is no option to continue for work-related purposes.

Employees are free to view news and media sites during non-business hours, as the News and Media category is permitted by the **Default Settings** and **Basic Filtering** category sets.

Scenario 4: Assigning a Different Policy

You do not want to block or limit internet requests from the company's top executives. The quickest remedy is to add the CEO and the Management group via Websense Manager as clients, and assign them a separate policy. This ensures that internet sites are never blocked on machines where the executives are logged in, while everyone else continues to be filtered according to the **Global** policy.

Add Directory Objects

Add directory objects (also called “clients”) to Websense software when you want them to be filtered by a policy other than the **Global** policy. See [page 107](#) for more details about adding clients.

1. Right-click in the Websense Manager navigation tree, and then choose **Add Directory Objects**.
The **Add Directory Objects** dialog box appears.
2. Double-click the **LDAP directory service** or **Windows directory service** folder (in which the user is defined), to display its domain/context list.
3. Double-click a domain/context folder to display a list of its users.



Add Directory Objects dialog box

4. Select the CEO's user name and the Management group name from the list of available users.
To select multiple users, press the **Ctrl** key while clicking each group name. To select a range of users, hold down the **Shift** key while clicking the first and last users in the range.
5. Click **OK**.

Once you add the CEO user and the Management group, you can assign them a separate policy without affecting the **Global** policy that currently governs all other employees.



NOTE

For Websense software to properly filter internet requests from specific users, you may need to select **Prompt user for directory authentication** via **Server > Settings > User Identification** after you add groups via Websense Manager. See *Directory Service Access*, page 187 to make this determination.

Create a New Policy

Creating new policies provides added flexibility when managing employee internet access. Instead of editing the **Global** policy to fit everyone, create customized policies for those who should be filtered differently. See [page 396](#) for more details on adding policies.

1. Right-click in the Websense Manager navigation tree, and then choose **Add Policy**.

The **Add Policy** dialog box appears.

2. Name the new policy **Unlimited Access**.
3. Click **OK**. The **Policy Model** dialog box appears.
4. Select **Create Empty Policy**, and then click **OK**.
5. Expand **Filter Definitions > Policies** in the navigation tree.
6. Select the **Unlimited Access** policy, and then click **OK**.
7. Edit the policy, adding a single row with the following values:

Start Time—00:00 (midnight)

End Time—24:00 (midnight)

Days—Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Category Set—Never Block

8. Double-click in the **Protocol Set** column and select the **Never Block** protocol set. (For more information on configuring protocol-based filtering, see *Managing Protocols*, [page 337](#).)

The **Never Block** category set permits access to all sites, regardless of content. (This category set cannot be edited or deleted). The **Never Block** protocol set permits access to all protocols. The **Unlimited Access** policy uses the **Never Block** category set and protocol set 24 hours a day, seven days a week.

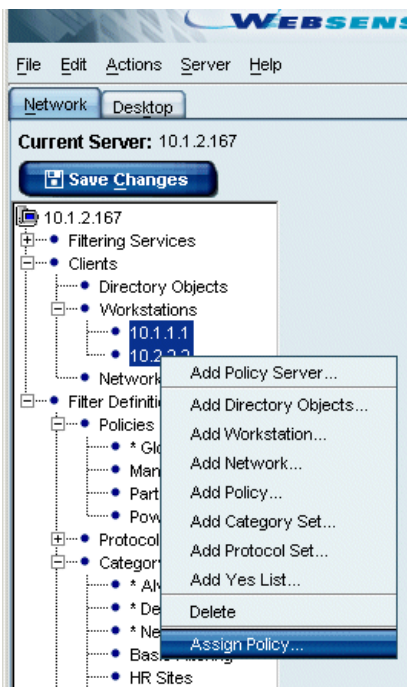
If you were to leave any times or days unscheduled (for example, by setting the times from 08:00 to 17:00 and the days of the week to Monday-Friday), Websense software would apply the **Global** policy during unscheduled times. If the **Global** policy had no category set scheduled at the time of a request, Websense software would apply the **Default Settings** category set.

Now that you have created a new policy for the CEO and the Management group, you must assign the new policy to them.

Assign a Policy

Directory objects added via Websense Manager are automatically assigned the **Global** policy until a different policy is assigned to them. See [page 283](#) for more details on assigning policies.

1. In the navigation tree, expand **Clients > Directory Objects**.
2. Select both the CEO's user name and the Management group. (To select both, press the **Ctrl** key while clicking each name.)
3. Right-click one of the selected clients, and then choose **Assign Policy**.



Shortcut menu in navigation tree

The **Assign Policy** dialog box appears.

4. Select the **Unlimited Access** policy, and then click **OK**.
5. Click **Save Changes** above the navigation tree to implement the change from **Global** to **Unlimited Access** for the CEO and the Management group.

Any user or group recognized by your directory service can be added via Websense Manager and assigned its own policy.

Scenario 5: Using Yes Lists and Password Override

A manager finds that employees are using a shared computer in the shipping room to access permitted sites without supervision. Concerned about the lack of immediate supervision of this computer, you decide to add the workstation and give it a unique policy that restricts internet access to shipping-related sites only.

Add a Workstation

Individual computers can be added via Websense Manager as workstations and then assigned their own policies. See [page 113](#) for more details on adding workstations.

1. Right-click in the navigation tree, and then choose **Add Workstation**. The **Add Workstation** dialog box appears.
2. Enter the IP address of the workstation, and then click **OK** to add the computer via Websense Manager.

Set Up a Yes List

1. Create a yes list named **Shipping Room**, and add the URLs you would like to permit for users of the shipping room workstation (see [page 308](#) for instructions).
2. Add a policy called **Shipping** and base it on the **Unlimited Access** policy you created in *Scenario 4: Assigning a Different Policy*.
3. Edit the **Shipping** policy to use the **Shipping Room** yes list 24 hours a day, seven days a week. Using a yes list automatically blocks access to all sites except those you included on the yes list.
4. Select the newly-added IP address under **Workstations** in the navigation tree, and then select the **Shipping** policy from the policy list in the content pane.
5. Click **Save Changes** above the navigation tree.

Assign Password Override Privileges

A few hours after implementing the Shipping policy, the shipping manager calls to say he can't access a needed site. Realizing the difficulty of making sure every shipping site is on the **Shipping Room** yes list, you decide to give the manager password override privileges on this computer. Password override lets users enter a password to override Websense blocking and access requested sites.

The password override privilege can be assigned to individual users or workstations. See [page 115](#) for more details on password override.

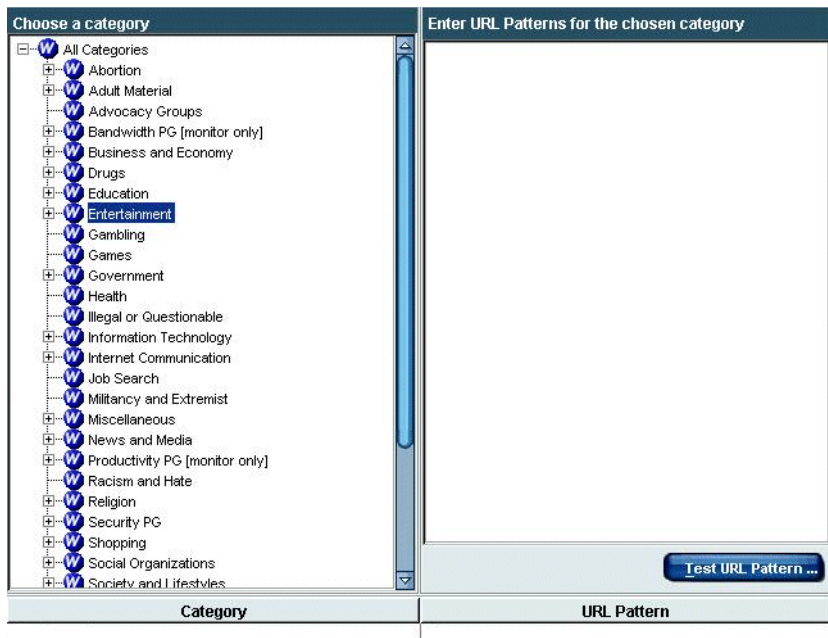
1. Expand **Workstations** in the navigation tree, and then select the IP address of the workstation to which you want to grant password override privileges. Details for this workstation appear in the content pane.
2. Check **Enable Password Override**. The **Enter Password** dialog box appears.
3. Enter a **New Password** for this workstation, and then confirm the spelling by entering it again in the **Confirm new password** field.
4. Click **OK**.
5. Click **Save Changes** above the navigation tree.

Now the manager can enter this password to access any blocked site at the workstation in the shipping area. As the administrator, you can check to see if this password is being abused by generating relevant reports in Reporter or Explorer.

Scenario 6: Blocking Keywords

Several managers want to make sure their employees cannot view sites related to job hunting during working hours. The Job Search category is already blocked in both the **Business Hours** and **Default Settings** category sets, but you also decide to use the keywords feature to block search engine results and internet sites whose URLs contain the keywords “job,” “career,” and “resume.” See [page 332](#) for more details on blocking keywords.

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Common Filtering** at the left, and then set **Keyword search options** to **URL and CGI**.
3. Select **Keywords** in the navigation tree to open the keyword editor.



Keywords editor

4. Under **Choose a category**, select **Job Search**.
5. Under **Enter URL Patterns for the chosen category**, add the words **job**, **career**, and **resume** on separate lines. (Enter only one keyword per line.)

6. Click **Add Keywords**. The new keywords and their categories appear at the bottom of the keyword editor.

To alphabetize your keyword list, click on the **Keyword** title bar in the lower content pane. To reverse order the list, hold down the **Shift** key while you click the title bar.

7. Select the **Business Hours** category set in the navigation tree.
8. Click **Edit** to open the **Edit Category Set** dialog box.
9. Select the **Job Search** category, and then check the **Block Keyword** check box.
10. Click **OK**.
11. Click **Save Changes** above the navigation tree.

Clicking **Save Changes** immediately blocks access to sites such as <http://www.newcompany.com/jobs.htm> (via URL keyword blocking) and results from search engine requests such as “resume services” (via CGI keyword blocking). Using keyword blocking only slightly lengthens the time to filter site requests.

**NOTE**

Keyword blocking is in effect when the URL containing a keyword is in a blocked category, *and* when the keyword is in a permitted category.

Scenario 7: Recategorized Custom URLs

A local store is having a promotion where prizes are given to contestants who play a game on the store's website. You want to keep employees from accessing this site until after work, but the site is not currently part of the Master Database. You decide to add the site as a recategorized custom URL, and create a custom category for it so as not to interfere with the filtering options of other categories.

Create a Custom Category

Custom categories are useful for containing custom URLs, and for containing sites already residing in the Master Database that you want to reclassify. Custom categories can be added anywhere a category list is shown, and are added as subcategories under an existing Master Database category.

This scenario adds a custom category via the recategorized custom URLs list. See [page 328](#) for more details on recategorized URLs.

1. Expand **Filter Definitions > Custom URLs > Recategorized** in the navigation tree. The custom URLs editor appears in the content pane.
2. Under **Choose a category**, right-click **User-Defined**, and then choose **Add a Custom Category**. The **Add Category** dialog box appears.
3. Name the new category **Contests**, and then click **OK**.
4. Click **Save Changes** above the navigation tree.

The Contests category now appears in the category list as a subcategory under User-Defined. If no other filtering option is selected for a custom category, the filtering option defaults to Continue (see [Continue, page 48](#)).

Add Recategorized Custom URLs

After creating a custom category to contain the contest site, you must add the contest site to the recategorized custom URLs list. Recategorized custom URLs are added as follows:

1. Select **Custom URLs/Recategorized** in the navigation tree. The custom URLs editor appears in the content pane.
2. Under **Choose a category**, select the **Contests** category you created (it appears under User-Defined).
3. In the **Enter URLs for the chosen category** area, type the full URL for the contest site. For example:
<http://www.localcompany.com/contest>.
4. Click **Add URLs**.
5. Click **Save Changes** above the navigation tree.

Unlike sites on the Custom URLs/Not Filtered list, which are automatically permitted, recategorized custom URLs may be permitted, blocked, or limited by quota, based on the filtering setting for their categories in the active category set.

To keep employees from viewing the contest site you just added, you must now edit the **Business Hours** category set you created in [Scenario 3: Deferring News and Media Sites](#), page 390. Apply the **Block** filtering option to the **Contests** category.

Once you have edited the **Business Hours** category set and clicked **Save Changes**, all employees assigned policies using **Business Hours** will see a block message when they try to access the contest site during working hours.

Scenario 8: Quotas

You want to allow employees to do banking and other personal errands online, but want control over the total amount of time they are web surfing, the categories they are accessing, and the duration of each session.

By default, Websense software is configured to use the **Limit by Quota** filtering option for several selected categories. Do the following to ensure that Websense software is configured properly for your environment.

- ◆ Review the filtering options in the **Default Settings** category set and make any appropriate changes. Instructions are given under [Editing a Category Set, page 314](#).
- ◆ Review the length of time each quota session should be (default is 10 minutes), and make appropriate changes. Instructions are given in the next section.
- ◆ Review the number of minutes every client should be allocated per day (default quota time is 60 minutes) to view sites in quota categories, and make appropriate changes. Instructions are given in the next section.
- ◆ If a user, group, workstation, or network should be allocated a different amount of quota time than the other clients, add the client via Websense Manager and specifically allocate time to that client (see [page 119](#)).

Configure Quota Session and Default Quota Time

1. In Websense Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **Common Filtering** at the left.
3. Notice that **10** minutes is entered in the **Quota session length** field.
This amount of time is configured by default, and gives employees a 10-minute window in which to take care of personal business. To change the time, enter a new number.
4. Notice that **60** minutes are configured in the **Default quota time per day** field.
This gives employees sufficient time to have several quota sessions during the day, if no additional quota time is configured. To change the time, enter a new number.
5. Click **OK**.

Allocate Quota Time to Specific Clients

1. Add a user to which you want to allocate quota time via Websense Manager (see [page 107](#)).



NOTE

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

2. Expand **Clients** in the navigation tree.
3. Select the desired client name. The client editor appears.
4. Select the **Set quota time for this user to...minutes** option.
5. Enter an appropriate number of minutes in the field that appears (default is 0 minutes). The user will be allocated this amount of quota time daily.

User: dlowejoy Domain: NIS1

Set quota time for this user to minutes

No specific quota time for this user

Policy: * Global

Enable Password Override

Change Password

Client editor

6. Click **Save Changes** above the navigation tree.
7. Repeat steps 1-5 for each user, group, workstation or network to which you want to allocate quota time other than the default amount (10 minutes).

Your employees can now access the internet for personal business, but you have control over the amount of time they spend, and the sites they can visit.

Scenario 9: Filtering Video and Audio Internet Media

Employees are spending work time playing audio and video files they have acquired via email or other transfer methods. Websense Dynamic Protocol Management is designed to give you control over user access to such media.

To implement a full filtering solution for audio and video internet media, you can combine protocol-based filtering with file type filtering (see [File Types](#), page 297). This way, protocol filtering handles streaming media, while file type filtering handles files that can be downloaded and then played.

Customize the **Global** policy (provided with Websense software) to limit access to internet audio and video media for all users governed by this policy. To do this, edit the **Global** policy so the **Default Settings** protocol set blocks streaming media, and the **Business Hours** category set blocks audio and video file types.

If you do not want to modify the **Global** policy, alternatively create a new protocol set (see [Adding a Protocol Set](#), page 357) and a new category set (see [page 390](#)), and then create and assign a policy that uses the new filtering settings you have specified. See [Scenario 4: Assigning a Different Policy](#) for instructions.

Block File Types

In Scenario 3, you edited the **Global** policy to use the **Business Hours** category set during working hours. Now you want to modify the **Business Hours** category set so that audio and video files are blocked during working hours.

1. Select the **Business Hours** category set in the navigation tree.
2. Click **Edit**. The **Edit Category Set** dialog box appears.
3. Select **All Categories** in the list of categories.
4. Under **Advanced Filters**, check **Block File Types**.
5. In the list of file types, check both **Audio Files** and **Video Files**, and then click **OK**.
6. To apply the same filtering option to the subcategories associated with the category, click **Apply to Subcategories**.

7. Click **OK** to close the **Edit Category Set** dialog box.
8. Click **Save Changes** above the navigation tree.

Block a Protocol

Next, customize the **Global** policy to block streaming media by following these steps:

1. Expand **Filter Definitions > Policies** in the navigation tree.
2. Select **Global**. Its start and end times, days, category set and protocol set are displayed in the content pane.
3. In the **Protocol Set** area, click **Edit**. The **Edit Protocol Set** dialog box appears for the **Default Settings** protocol set.
4. Select the first protocol under **Streaming Media**, and then select **Block** (under **Protocol Set Options**).
5. Click **Apply to Entire Group** to block all streaming media protocols, and then click **OK**.
6. Click **Save Changes** above the navigation tree.

The **Global** policy will block audio and video internet media, whether they are accessed live from an external web server, or downloaded to a client machine.

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.

Before Contacting Websense Technical Support

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.
- ◆ Familiarity with your network's architecture, or access to a person who has this familiarity.
- ◆ Specifications of the machines running Filtering Service and Websense Manager.
- ◆ A list of other applications running on the Filtering Service machine.

Check the Top 10 FAQs at <http://www.websense.com/global/en/SupportAndKB/> for solutions to common questions.

Websense Technical Support Services

Technical information about Websense is available 24 hours a day via the internet at:

<http://www.websense.com/global/en/SupportAndKB/>

You will find the latest release information, Frequently Asked Questions (FAQs), Knowledge Base, and other information.

Premium Support

Websense offers two premium fee-based support options: Priority One 24x7 Support and Platinum Support.

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 a complete list of Priority One 24x7 and Platinum Support services, please visit our website at:

<http://www.websense.com/global/en/ProductsServices/Services/PriorityOne24x7Support.php>

For additional information, please contact our Sales Department at **800.723.1166** or **858.320.8000**, or send an email to **sales@websense.com**.

Support Options

Websense Technical Support can be requested 24 hours a day, 7 days a week.

Web Portal

You can submit support tickets through the Web Portal 24 hours a day, 7 days a week. 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:

<http://www.websense.com/global/en/SupportAndKB/CreateRequest/>

Email Questions

You can email your questions to us at the addresses listed below. Make sure you include your subscription key. This option is available 24 hours a day, 7 days a week. We will respond during business hours Monday through Friday.

- ◆ **support@websense.com**—San Diego, California, USA
- ◆ **uksupport@websense.com**—London, England

Customers in Japan should contact their distributors for the most rapid service.

Email support can take up to 24 hours or more for a response. If you need a quicker turnaround, submit your issues through the Web Portal.

Telephone Assistance

Before you call a Websense Technical Support representative, please be ready with the following:

- ◆ Websense subscription key.
- ◆ Access to the configuration files for your Websense products
- ◆ Access to the machine running the Filtering Service, the Websense Reporting components, and the database (MSDE or SQL Server).
- ◆ Permission to access the Websense Log Database.
- ◆ Familiarity with your network's architecture, or access to a person who has this familiarity.
- ◆ Specifications of the machines running the Filtering Service and the Websense configuration files
- ◆ A list of other applications running on the Filtering Service machine.

For severe problems, additional information may be needed.

Telephone assistance is available during normal business hours Monday through Friday at the following numbers:

- ◆ U.S. Technical Services in San Diego, California: **1-858.458.2940**
- ◆ U.K. Technical Services in London, England: **+44 (0) 1932 796244**

Customer Care

Not sure who to call? Contact Customer Care for assistance with:

- ◆ General concerns
- ◆ Subscription key renewals
- ◆ 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: **1 866 355 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

A

Active Directory Server
 about, 124
adding
 category sets, 313
 directory objects, 107
 file types, 301
 policies, 280
 Policy Server, 212
 protocol sets, 357
 protocols, 352
 roles, 252
 workstations, 113
 yes lists, 308
adding networks, 114
address bar, searching from, 368
administration, change history for, 237
administration, roles for, 247
alerting, 227
alternate block messages, 64
Always Block category set, 303
Anonymous Logging, 79
Apply to Subcategories button, 315
assigning policies, 283, 397
audit log, 237
authentication
 manual, 208

B

bandwidth, 67
 managing, 103
Block keywords filtering option, 314
block messages
 customized, 56

 default, 55
 for file types, 298
 for old subscriptions, 19
 for protocols, 342
 for quota sites, 50
 for yes list users, 304
 illustrated, 55
 troubleshooting, 371, 373
Block Messages settings, 54, 215
blocking
 by file type, 333
 Use more restrictive option, 41, 51

C

categories
 adding custom, 328
 creating custom, 402
 deleting custom, 330
category sets
 adding, 313, 390
 Always Block, 303
 Basic Filtering, 303
 Default Settings, 22, 303
 defined, 26
 deleting, 317
 editing, 314, 387
 Monitor Only, 303
 Never Block, 303, 396
 permanent, 303
 Yes List Only, 320
CGI (Common Gateway Interface)
 requests via, 78
clients
 adding workstations, 113

- and policy priority, 106
- assigning policies to, 283
- defined, 25
- viewing policy assignment for, 286

Common Filtering settings, 216

components

- removing, 242

components, of Websense, 31

configuration

- interface for See Websense Manager
- of distribution settings, 291
- port for, 212

connections

- between servers and Network Agent, 88
- to Policy Server, 212

content pane, 23

custom categories

- about, 402
- adding, 328
- deleting, 330

custom object class types, 205

custom URLs, 74, 319

- adding, 320
- adding recategorized, 403
- and custom categories, 328
- and redirected sites, 323
- deleting, 328
- recategorized, defined, 26
- unfiltered, defined, 26

Customer Care, 412

customizing block messages, 59

D

- database download
 - manual, 65
- database updates, 65
- DC Agent, 129
- Default Settings category set, 22
 - described, 303
- Default Settings protocol set
 - described, 351
- Delegated Administrator, 247
- deleting

- category sets, 317
- custom categories, 330
- custom URLs, 328
- keywords, 336
- policies, 295
- Policy Server, 220
- protocols, 355

Directory Service settings, 215

directory services

- Active Directory, 124
- described, 123
- LDAP, 124, 192
- Novell Directory Services, 124
- Sun ONE Directory Server, 124
- Windows-based, 123

Distributed Administration, 245

distribution

- of configuration data, 269

domain administrator privileges, 131

Download settings, 215

downloading Master Database, 65

E

- eDirectory Agent, 169
- Edit Category Set dialog box, 265, 315
- Edit Policy dialog box, 282
- email notification, 19, 227
- email questions
 - technical services, 411
- error messages, 66, 367

F

- file extensions
 - filtering by, 297
- file types
 - adding, 301
 - blocking by, 333
 - defined, 27
- filtered custom URLs
 - defined, 26, 319
 - deleting, 328
- filtering

- of remote clients, 34, 53, 120
- of URLs not in Master Database, 403
- order of, 39
- filtering options, 26
 - bandwidth-based, 102
 - block, 314
 - block keywords, 26, 314
 - continue, 48
 - limit by quota, 49, 314
 - permit, 314
 - setting, 265, 315, 389
- Filtering Service, 211
 - and filtering site requests, 16
 - connecting to, 211
 - described, 33
 - starting/stopping, 33
- filtering, restrictions on, 261

G

- Global policy, 22
 - about, 15, 279, 386
- groups
 - adding, 394
 - defined, 25

I

- identifying users, 123
- installation
 - troubleshooting, 367
- Instant Messaging Attachment Manager, 346
- integration partners
 - and Filtering Service, 33
 - examples of, 14
- IP addresses
 - changing, 222
 - matching of, 77
 - problems with, 383

K

- keys, for subscription, 68
- keyword blocking
 - troubleshooting, 369

- keywords
 - adding, 333
 - blocking, 27, 314, 331, 400
 - deleting, 336

L

- LDAP, 124
- lockouts, 260
- Log Server, 14, 37, 79, 386
 - described, 37
- Logging settings, 79, 215
- logging, anonymously, 79
- Logon Agent, 142

M

- manual authentication
 - enabling, 208
- Master Database
 - about, 33
 - adding sites to, 74
 - matching sites by IP address, 77
 - matching sites by URL, 76
- menus
 - main, 24
- Monitor Only, 296
- monitoring
 - Internet access, 33
 - network activity, 33

N

- navigation tree, 23
 - about, 24
 - illustrated, 25
- network, 105
- network activity, monitoring, 33
- Network Agent, 83
- network interface cards, 85
- networks, 25
- Never Block category set, 303, 396
- Never Block protocol set, 351
- Novell Directory Services
 - configuring, 202

Novell eDirectory, 124
NTLM, 124

O

object classes
 custom types for, 205
online Help
 troubleshooting, 369

P

password override, 53, 115, 399
 disabling, 117
 setting timeouts for, 116
permitted custom URLs, 319
 defined, 26
 deleting, 328
policies, 277
 adding, 280, 396
 and multiple groups, 41
 assigning, 283, 397
 creating new, 396
 custom, 15, 280
 defined, 27
 deleting, 295
 determining which applies, 40
 distributing to other servers, 265, 287
 editing, 391
 Global, 279
 priorities for, 106
 samples of, 279
Policy Server
 adding, 212
 configuring, 215
 connecting to, 213
 connections, 24
 deleting, 220
 distributing data to, 265, 287
 machine ID, 133
 password for, 368
 starting/stopping, 217
 using multiple, 47
port numbers

 Policy Server, 133
port spanning, 85
ports
 blocking, 340
 for configuration, 212
protocol sets
 Basic Filtering, 351
 creating, 351, 357
 Default Settings, 351
 editing, 357
 Monitor Only, 351
 Never Block, 351
 using in policies, 359
protocols
 adding, 351
 customizing, 351
 defined, 27
 filtering, 346
 managing access to, 337
proxy servers
 and avoidance systems, 22, 386
 and database download, 218

Q

quota block message, illustrated, 50
quota time
 allocating, 119, 406
 configuring, 405
 defined, 50, 52
 priority list, 51
 setting defaults for, 52, 118, 405
quotas, 16, 49

R

RADIUS Agent, 150
real-time security updates, 72
recategorized custom URLs, 403
 adding, 324
recategorized custom URLs, deleting, 328
regular expressions, 308, 322, 326, 335
Remote Administrator, 247
Remote Filtering, 34, 53, 120

Reporter

See Websense Enterprise Reporter

risk classes, 81

roles, 247

roles, creating, 252

S

searching from address bar, 368

security

updates to database, 72

Servers See Log Server

sessions, for Policy Server, 258

Settings dialog box, 211

block message options in, 54

logging options in, 79

shortcut menus, 24

subscription, 17

compliance with, 39

expiration of, 39

upgrading, 39

subscription key, 17, 68

Sun Java System Directory Server, 124

configuring, 198

Super Administrator, 247

support

email questions, 411

options, 410

web portal, 410

T

technical services

web portal, 410

technical support, 409

documentation feedback, 412

email, 411

fee-based, 410

telephone assistance, 411

Web portal, 410

telephone assistance, 411

timeouts

for password override, 116

transparent identification agents, 129, 150, 169, 182

tutorials

adding category sets, 390

adding custom categories, 402

adding groups, 394

adding policies, 396

adding recategorized custom URLs, 403

adding users, 394

adding workstations, 398

assigning policies, 397

editing category sets, 387

editing policies, 391

for keyword blocking, 400

for password override, 399

U

upstream proxy servers, 218

URL matching, 76

URLs

custom, 319

of redirected sites, 323

Use more restrictive blocking, 41, 51

Use quota time button, 50

User Service, 35

required privileges, 131

User Service settings, 215

users

adding, 394

defined, 25, 105

V

virtual hosts

about, 78

W

Web Filter Lock, 261

web portal

support, 410

Websense

removing, 242

Websense DC Agent, 129

Websense eDirectory Agent, 169
Websense Enterprise Reporter, 14, 37, 79
Websense Filtering Service, 33
Websense Logon Agent, 142
Websense Manager, 34
 content pane in, 23
 illustrated, 23
 managing Internet access with, 21
 menus in, 23
 navigation tree in, 23
 starting, 23, 28
Websense Master Database, 33
 troubleshooting download of, 364, 367

Websense Network Agent, 83
Websense Policy Server, 32
Websense RADIUS Agent, 150
Websense User Service, 35
workstations, 25
 adding, 113, 398

Y

Yes List Only category set, 320
yes lists
 behavior of, 398
 creating, 308
 defined, 26