Remote Filtering

Websense Enterprise®
Websense® Web Security Suite

v6.3.1

Published December 17, 2007
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.

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.

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**).

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.

Contents

CHAPTER 1

Introduction

The Remote Filtering feature allows Websense Web filtering software to filter URL requests on computers that are outside an organization's network. Remote Filtering requires the installation of client software on all machines that are used outside the network. This client, Remote Filtering Client, is configured to communicate with a Remote Filtering Server inside your firewall that acts as a proxy to Websense Filtering Service. All communication between Remote Filtering Client and Remote Filtering Server is authenticated and encrypted.

The Remote Filtering feature is offered with Websense Enterprise and Websense Web Security Suite.

Remote Filtering Client system requirements

Remote Filtering Client can only be installed on a supported Windows operating system.

Hardware Recommendations	Operating System Requirements
• Pentium 4 or greater • Free disk space: 25 MB for installation; 15 MB to run the application • 512 MB RAM	• Windows XP Professional with SP1 or SP2 • Windows Vista Ultimate • Windows Vista Enterprise • Windows Vista Business • Windows 2000 with SP3 or later (Professional, Server, Advanced Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)

Remote Filtering Server system requirements

Remote Filtering Server is supported on the following operating systems:

- Red Hat Enterprise Linux 3 or 4: AS, ES, and WS
- Solaris 9 or 10, with current patches
- Windows 2000 Server with SP3 or later
- Windows Server 2003, SP1 (Standard or Enterprise)
- Windows Server 2003, R2 (Standard or Enterprise)

Hardware recommendations

The following hardware recommendations are organized by network size.

Network Size	Hardware Recommendations
1-500 clients	**Windows** or **Linux** • Pentium 4, 2.0 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
500-2000 clients	**Windows** or **Linux** • Xeon, 3.2 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
2000-5000 clients	**Windows** or **Linux** • Dual Xeon, 3.2 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
5000-10000 clients	**Windows** or **Linux** • Quad Xeon, 3.2 GHz or greater *- or -* Static load balancing with Dual Xeon, 3.2 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, quad CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space

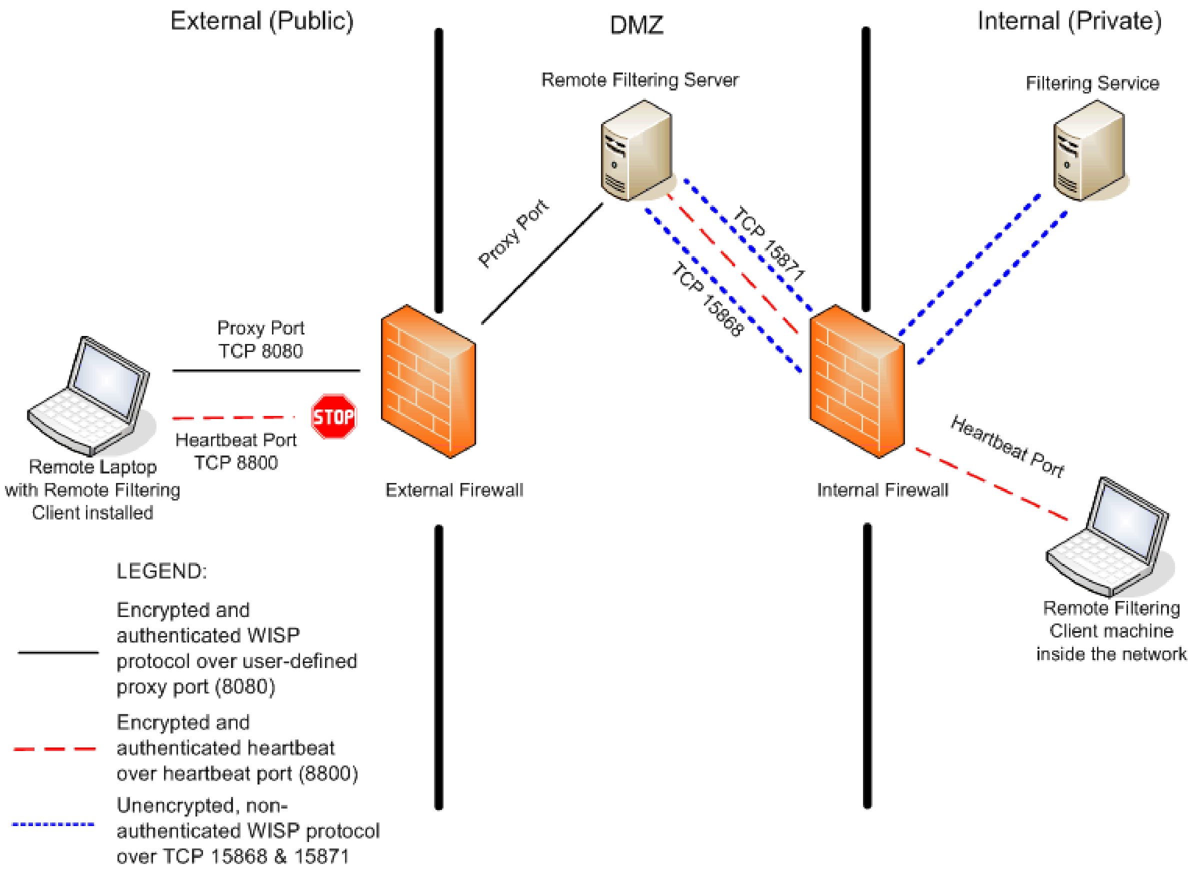
Network Size	Hardware Recommendations
10000+ clients	**Windows** or **Linux** • Static load balancing with Quad Xeon, 3.2 GHz or greater • 2 GB RAM • 20 GB of free disk space **Solaris** • Sun V490s, with 4 hyper-threaded CPUs, 1.593 GHz • 2 GB RAM • 20 GB of free disk space

Deployment information

Observe the following guidelines:

- Install Remote Filtering Server inside your organization’s outermost network firewall, but in the DMZ outside the firewall that protects the rest of the network.
- Install Remote Filtering Server on a separate, dedicated machine. This machine must be able to communicate with Websense Filtering Service and with the remote workstations outside the network firewall. The Remote Filtering Server machine need not be joined to a domain.
- Do not install Remote Filtering Server on the same machine as Websense Filtering Service or Network Agent.
- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- To provide failover capability for the primary Remote Filtering Server, install optional secondary and tertiary Remote Filtering Servers. Configure each Remote Filtering Server to communicate with the same Filtering Service. Configure each Remote Filtering Client to connect to the backup servers in case of server failure. Remote Filtering Clients connect to only one Remote Filtering Server at a time.

The following diagram shows a typical Remote Filtering deployment, including port assignments. This example does not include all Websense components. For more information about deploying Websense Web filtering software, see the Websense *Deployment Guide*.



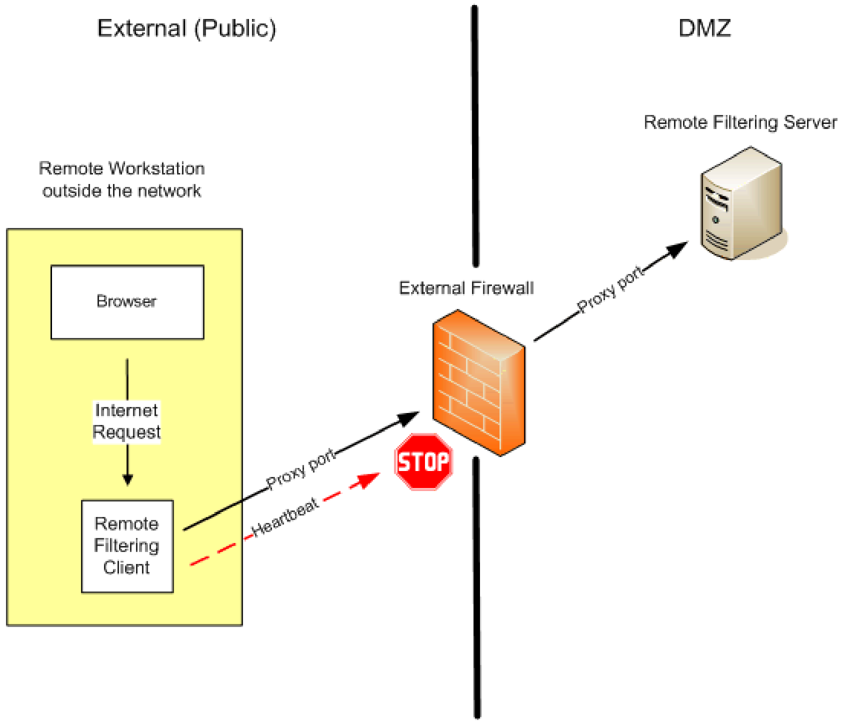
IMPORTANT

In this deployment, the heartbeat port, 8800, must be blocked at the external firewall, but opened on the internal firewall.

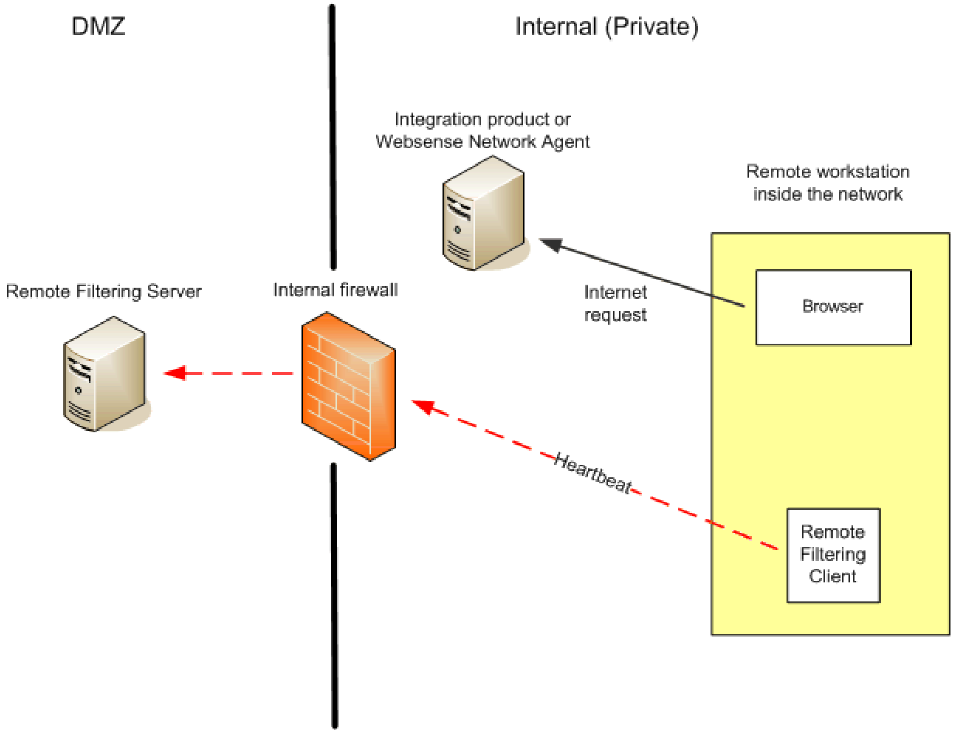
How Remote Filtering works

Websense Remote Filtering Client is an agent that controls the disposition of Internet requests on a workstation that is used outside an organization's network. When the browser on a machine running Remote Filtering Client makes an Internet request, Remote Filtering Client must decide whether to query Remote Filtering Server about the request. This determination is controlled by the location of the workstation relative to the network.

When the remote workstation is started *outside* the network, Remote Filtering Client attempts to send a *heartbeat* to Remote Filtering Server. Because the heartbeat port is blocked at the external firewall, the Remote Filtering Client cannot heartbeat to Remote Filtering Server. This heartbeat failure prompts Remote Filtering Client to send a query about each Internet request over proxy port 8080 to Remote Filtering Server in the DMZ. Each Internet request is delayed by Remote Filtering Client until a response is returned from Remote Filtering Server. Remote Filtering Server then forwards the filtering request to Websense Filtering Service installed on the inside network. Filtering Service evaluates each request and sends a response to Remote Filtering Server (including a block page, if needed). The response (containing the block page) is then served up to the remote workstation by Remote Filtering Server.



When the workstation is started *inside* the network, the Remote Filtering Client attempts to heartbeat back to the Remote Filtering Server in the DMZ. When Remote Filtering Client succeeds in heartbeating back to the Remote Filtering Server (the heartbeat port is open on the internal firewall), the Remote Filtering Client becomes passive and does not query Remote Filtering Server about Internet requests. Instead, requests from the browser are passed directly from the browser to an integration product (such as Cisco Pix, Microsoft ISA Server, or Websense Network Agent) installed on the internal network. The filtering of the request then proceeds as normal for an internal workstation.



Logon credentials

How a user logs on to a remote workstation affects the policy that is enforced. If a user logs on using cached domain credentials, Websense Filtering Service is able to resolve the user name and applies user and group-based policies to the remote machine. If the user logs on to the workstation with a local user account, Filtering Service cannot resolve the user name and applies the Global Policy instead.

When server communication fails

What action do you want Remote Filtering Client to take if it cannot contact Remote Filtering Server? Remote Filtering Client installs with a default *fail open* setting, which permits all Internet requests when communication between these components cannot be established. To change this setting to block all requests (*fail closed*), see *Fail closed option*, page 28.

When Remote Filtering Client is configured to fail closed, a default timeout value of 15 minutes is applied. The clock on this value begins running when the remote machine is started. Remote Filtering Client attempts to connect to Remote Filtering Server immediately and continues cycling through available Remote Filtering Servers until it is successful. If the user has Web access at startup, no filtering occurs (all requests are permitted) until Remote Filtering Client connects to the Remote Filtering Server machine. When this occurs, the Web filtering policy for remote machines is enforced.

If Remote Filtering Client cannot connect within the configured timeout limit, all Internet access is blocked (fail closed) until connection to Remote Filtering Server can be established.

NOTE

If Remote Filtering Server cannot connect to Websense Filtering Service for any reason, an error is returned to the Remote Filtering Client, and filtering fails open.

This timeout value allows users who pay for Internet access when travelling to start the machine and arrange for connection without being locked out. If Web access cannot be established before the 15 minute timeout period expires, no Web access can be established. When this occurs, restart the machine to begin the timeout interval again.

WARNING

Websense, Inc., does not recommend setting the fail closed timeout value to a low number or to zero. Zero disables the timeout, causing Remote Filtering Client to attempt to locate Remote Filtering Server continuously. Disabling the timeout or setting it too low can lock out a remote machine before the user can establish Internet connection from a hotel or other pay-for-use providers.

Virtual Private Network (VPN)

Websense Remote Filtering supports VPN connections, including split-tunneled VPN. When a client machine is connected to the internal network via VPN (non split-tunneled), Remote Filtering Client is able to heartbeat back to the Remote Filtering Server. As a result, Remote Filtering Client becomes passive, and all Internet requests from the remote workstation are filtered by the internal integration product using the internal filtering policy assigned to that workstation.

If the client workstation connects to the internal network via a split-tunneled VPN client, Remote Filtering Client detects this and does not heartbeat to the Remote Filtering Server. The Remote Filtering Client assumes that it is operating externally and sends a query to the Remote Filtering Server for instructions on handling the request. Remote Filtering Server checks with Filtering Service, which enforces the external filtering policy for the remote machine.

Websense software supports split-tunneling for the following VPN clients:

- Microsoft PPTP
- Checkpoint SecureClient
- Juniper/Netscreen
- SonicWALL
- Cisco
- Nokia
- Nortel

CHAPTER 2 Installation

You must have a functioning Websense Web filtering system installed before installing any Remote Filtering components. See the Websense *Installation Guide* for your integration product for instructions on installing and configuring your Websense Web filtering system. For Remote Filtering system requirements, see *Remote Filtering Client system requirements*, page 5. For deployment instructions, see *Deployment information*, page 7.

The installer package

Remote Filtering components install with the same download package that installs Websense Enterprise and Websense Web Security Suite. This package comes in two forms:

- **Dynamic**: An *online* installer package that requires Web access during installation. It downloads the necessary product files from the Websense Web site as needed, after product selections have been made. This package is smaller than the full (offline) version.
- **Full**: A complete *offline* installer. It is much larger than the online dynamic installer package, and contains all the files needed to install Websense Enterprise or Web Security Suite components. Use this package if you experience difficulties with the online connection.

Windows

To download and run the Windows installation package:

1. Log on to the installation machine with local administrator privileges.
2. Close all applications and stop any anti-virus software.
3. Go to the following download site and log on.

   https://www.websense.com/mywebsense/downloads/default.aspx

   If you do not have an account, you can create one on this page.
4. Select the product (Websense Enterprise or Web Security Suite), version, operating system, and language of the package you want.
5. Download the selected installer package (dynamic or full) to a folder on the installation machine, and double-click to extract the installer files.

   Websense Setup displays a file extraction dialog box.
6. Select a location in which to extract the installation files.

   If the path you enter does not exist, the installer creates it for you.
7. Click **Extract** to begin decompressing the files.
   - If Websense installation files already exist in that location, you may choose to overwrite the existing files.
   - A progress bar shows the status of the operation, and the view pane scrolls a list of the files as they are extracted.
   - `Setup.exe` runs automatically after the files are decompressed.

Linux and Solaris

To download and run the installation package for Linux and Solaris:

1. Log on to the installation machine as the **root** user.
2. Close all applications and stop any anti-virus software.
3. Create a setup directory for the installer files.

   For example: `/root/Websense_setup`
4. Go to the following download site and log on:

   https://www.websense.com/mywebsense/downloads/default.aspx

   If you do not have an account, you can create one on this page.
5. Select the product (Websense Enterprise or Web Security Suite), version, operating system, and language of the package you want.
6. Download the selected installer package (dynamic or full) to the setup directory you created.
7. In the setup directory, enter the following command to unzip the file:

   ```
   gunzip <download file name>
   ```

   For example: `gunzip Websense631Setup_Slr.tar.gz`
8. Expand the file into its components with the following command:

   ```
   tar xvf <unzipped file name>
   ```

   For example: `tar xvf Websense631Setup_Slr.tar`

   This places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.
Documentation	Release Notes: An HTML file containing release notes and last minute information about the Websense software. Read this file with any supported browser.

9. Run the installation program from the setup directory with the following command:

   ```
   ./install.sh
   ```

   To run the GUI version of the installer, use the following command:

   ```
   ./install.sh -g
   ```

✓ **NOTE**

If you are using a non-English based system, the installer displays an error message advising you that the GUI version is not supported.

Remote Filtering Server

To install Remote Filtering Server:

1. Download and run the installer, if not already done.

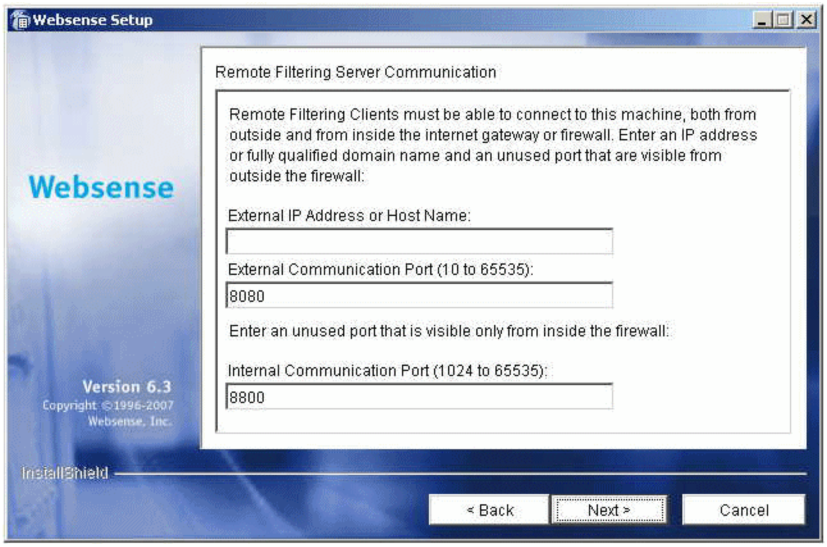
   For instructions on downloading the appropriate installer package for your operating system, see the previous sections.

2. Follow the onscreen instructions and select your Web filtering product.
3. Select a **Custom** installation.
4. Select **Remote Filtering Server**, and then click **Next**.

   If the installation machine is multihomed, all enabled network interface cards appear in a list.

5. Select the IP address of the card you want Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and then click **Next**.

   Remote Filtering Clients must be able to connect to Remote Filtering Server, both from inside and from outside the Internet gateway or network firewall. The installer asks you to provide connection information for this machine.



Remote Filtering Server Communication

Remote Filtering Clients must be able to connect to this machine, both from outside and from inside the internet gateway or firewall. Enter an IP address or fully qualified domain name and an unused port that are visible from outside the firewall:

External IP Address or Host Name:

External Communication Port (10 to 65535): 8080

Enter an unused port that is visible only from inside the firewall:

Internal Communication Port (1024 to 65535): 8800

6. In the **External IP Address or Host Name** field, enter an IP address or machine name (in the form of a fully qualified domain name) that is visible from *outside* the network firewall.

IMPORTANT

Remember which form you selected. You must use the same external address in *the same address format*—IP address or qualified domain name (FQDN)—when you install Remote Filtering Client.

7. In the **External Communication Port** field, enter a port number (from 10 to 65535) that is not in use, and that is accessible from *outside* the network firewall. The default value is 80. (If there is a Web server installed on the machine, port 80 may already in use, so you may need to change the default value.)

> **Important**
>
> The port entered as the **External Communication Port** must be opened on your network firewall to accept connections from Remote Filtering Clients on workstations located outside the firewall. For more information, see *Firewall configuration and component communication*, page 27.

8. In the **Internal Communication Port** field (*heartbeat* port), enter a port number (from 1024 to 65535) that is not in use, and that is accessible only from *inside* the network firewall. The default value is 8800.

> **Important**
>
> Be sure that your network firewall is configured to block connections to the **Internal Communication Port** from workstations located outside the firewall. For more information, see *Firewall configuration and component communication*, page 27.

9. Click **Next** to continue.

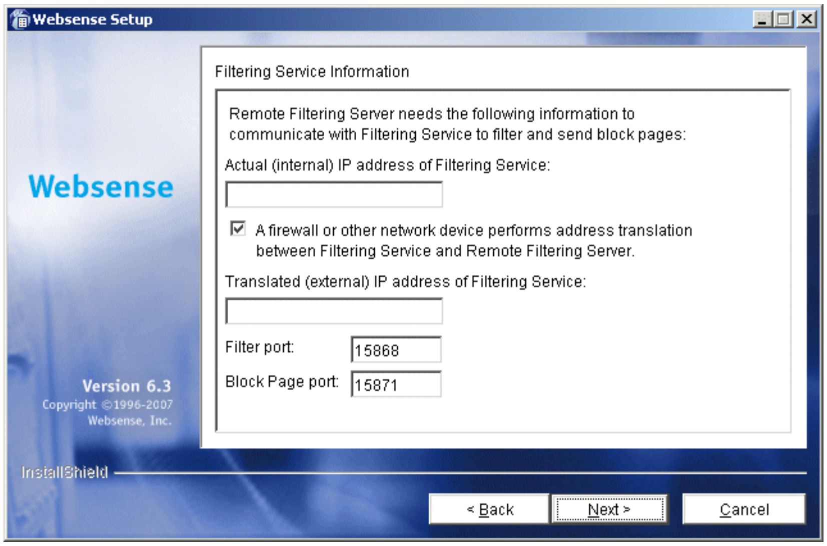
   The installer asks you to enter a *pass phrase* of any length for Remote Filtering Server. This pass phrase is combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.

10. Before selecting a pass phrase, consider the following requirements:
    - If Websense Client Policy Manager (CPM) is already installed in your network, you must enter the same pass phrase used when installing CPM.
    - If you install Websense Client Policy Manager (CPM) in your network in the future, you must use the pass phrase you enter in this screen.
    - If you want this installation of Remote Filtering Server to function as a backup (secondary or tertiary) server for a primary Remote Filtering Server, you must enter the same pass phrase used when installing the primary Remote Filtering Server.
    - The pass phrase must include only ASCII characters. Do not use extended ASCII or double-byte characters.
    - You must use the pass phrase you enter in this screen when you install the Remote Filtering Clients that will connect with this server.

> **WARNING**
>
> Be sure to record your pass phrase and keep it in a safe place. You cannot retrieve it from the Websense system later.

11. Enter and confirm your pass phrase.
12. Click **Next** to continue.

Remote Filtering Server must be able to communicate with Websense Filtering Service. The installer asks you to identify the machine on which Filtering Service is installed.



Filtering Service Information

Remote Filtering Server needs the following information to communicate with Filtering Service to filter and send block pages:

Actual (internal) IP address of Filtering Service:

☑ A firewall or other network device performs address translation between Filtering Service and Remote Filtering Server.

Translated (external) IP address of Filtering Service:

Filter port: 15868

Block Page port: 15871

13. In the first field, enter the actual (internal) IP address of the Filtering Service machine.
14. Is there a firewall or other network device that performs network address translation between the Filtering Service machine and this machine?
    - If yes, enter the translated (external) IP address of the Filtering Service machine.
    - If no, clear the checkbox and disable the **Translated (external) IP address of Filtering Service** field.
15. Enter the filter port number for the Filtering Service machine, if it was changed from the default of 15868.

NOTE

The filter port is the default communication port used by the installer to install Filtering Service. If you installed Filtering Service using a different communication port, enter that port number.

16. Enter the block page port number for the Filtering Service machine, if it was changed from the default value of 15871.

Important

If there is a firewall between the Filtering Service machine and the Remote Filtering Server machine, be sure to open the filter port (15868) and block page port (15871) on that firewall. Filtering Service must be able to accept connections from Remote Filtering Server, and provide block pages for Remote Filtering Server to send to the remote machines. For more information, see *Firewall configuration and component communication*, page 27.

17. Click **Next**.

    The installer asks you to select an installation folder for the Websense components.

18. Accept the default path or click **Browse** to locate another installation folder, and then click **Next** to continue.

    The installer compares the system requirements for the installation you have selected with the resources of the installation machine.

    - If the installation machine has insufficient disk space, the installer quits.
    - If the installation machine has less than the recommended amount of memory, a warning is displayed, but the installation can continue.

    A summary list appears, showing the installation path, the installation size, and the components that are being installed.

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

    If you are using the online installer, the appropriate files are downloaded from the Websense Web site. Installation begins automatically when the download is complete.

20. If you chose an English language installer, click **Finish** to exit the installer.
21. If you chose a non-English language installer, click **Next** to continue.
22. If you stopped your anti-virus software, remember to start it again after Websense components have been installed.

Important

If Network Agent is configured to filter HTTP requests in your network, make sure that it is **not** filtering requests going to or from the Remote Filtering Server machine.

For information about configuring Network Agent, see the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Remote Filtering Client

Remote Filtering Client is installed on client machines that are used outside the network firewall. This component connects with a Remote Filtering Server located inside the network firewall to enable Web filtering on remote workstations. Remote Filtering Client installs on Windows only.

- **Deployment as part of CPM Client Agent** (**Websense Client Policy Manager™ users only**): If you purchased a subscription for Websense Client Policy Manager™ (CPM), it is not necessary to install Remote Filtering Client. The Remote Filtering Client application is included as part of CPM Client Agent, and is deployed automatically when you deploy the CPM Client Agent to user workstations. See your Websense Client Policy Manager documentation for more information.
- **Manual installation**: Use the Remote Filtering Client Pack to manually install Remote Filtering Client on individual workstations. See *Manual Installation*, page 20 for information.

- **Automatic deployment with third-party tool**: Use the Remote Filtering Client Pack and a third-party deployment tool to deploy Remote Filtering Client automatically to user workstations. See *Installing with a third-party deployment tool*, page 23 for information.

WARNING

Do not install the Remote Filtering Client on:

- Machines running Windows 2000, Service Pack 2 or earlier. The installation will fail.
- Machines on which you installed Remote Filtering Server. Remote Filtering Client running on the same machine as Remote Filtering Server eventually causes filtering to fail.

Remote Filtering Client Pack

The Remote Filtering Client Pack is an installer package. You download it and use it to deploy Remote Filtering Client to individual workstations or to multiple workstations using third-party network deployment tools. Load the Client Pack directly on individual workstations, or on a network server from which Remote Filtering Client can be deployed with third-party tools. The Remote Filtering Client Pack installs on Windows machines only.

To install the Remote Filtering Client Pack installer package on a Windows machine:

1. Download and start the Windows installer using the procedure in *The installer package*, page 13.
2. Follow the onscreen instructions and select your Web filtering product.
3. Select a **Custom** installation.
4. Select **Remote Filtering Client Pack**, and then click **Next**.

   If the installation machine is multihomed, all enabled network interface cards appear in a list.
5. Select the IP address of the card you want Remote Filtering Server to use to communicate with other Websense components inside the network firewall, and then click **Next**.

   The installer asks you to select an installation folder for the Websense components.
6. Accept the default path or click **Browse** to locate another installation folder, and then click **Next** to continue.

   The installer compares the system requirements for the installation you have selected with the resources of the installation machine.

   - If the installation machine has insufficient disk space, the installer quits.
   - If the installation machine has less than the recommended amount of memory, a warning is displayed, but the installation can continue.

   A summary list appears, showing the installation path, the installation size, and the components that are being installed.
7. Click **Next** to start the installation.

   If you are using the online installer, the appropriate files are downloaded from the Websense Web site. Installation begins automatically when the download is complete.
8. If you chose an English language installer, click **Finish** to exit the installer.
9. If you chose a non-English language installer, click **Next** to continue.

10. If you stopped your anti-virus software, remember to start it again after Websense components have been installed.

    You have now installed the Remote Filtering Client pack. The Remote Filtering Client Pack is called `CPMClient.msi` and can be found in the following default location:

    ```
    C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI
    ```

Manual Installation

To install the Remote Filtering Client manually on individual Windows workstations:

1. Make sure that the Remote Filtering Server to which this client will connect has been correctly installed on a separate machine. See *Deployment information*, page 7 for Remote Filtering Server deployment recommendations and *Remote Filtering Server*, page 15 for installation instructions.
2. Install the Remote Filtering Client Pack on the workstation as described in *Remote Filtering Client Pack*, page 19. Or, if you have already installed the Remote Filtering Client Pack on another machine, you can simply copy the `CPMClient.msi` file to a folder on the installation workstation. If you selected the default installation path of `C:\Program Files\Websense`, this file is located at:

    ```
    C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI
    ```

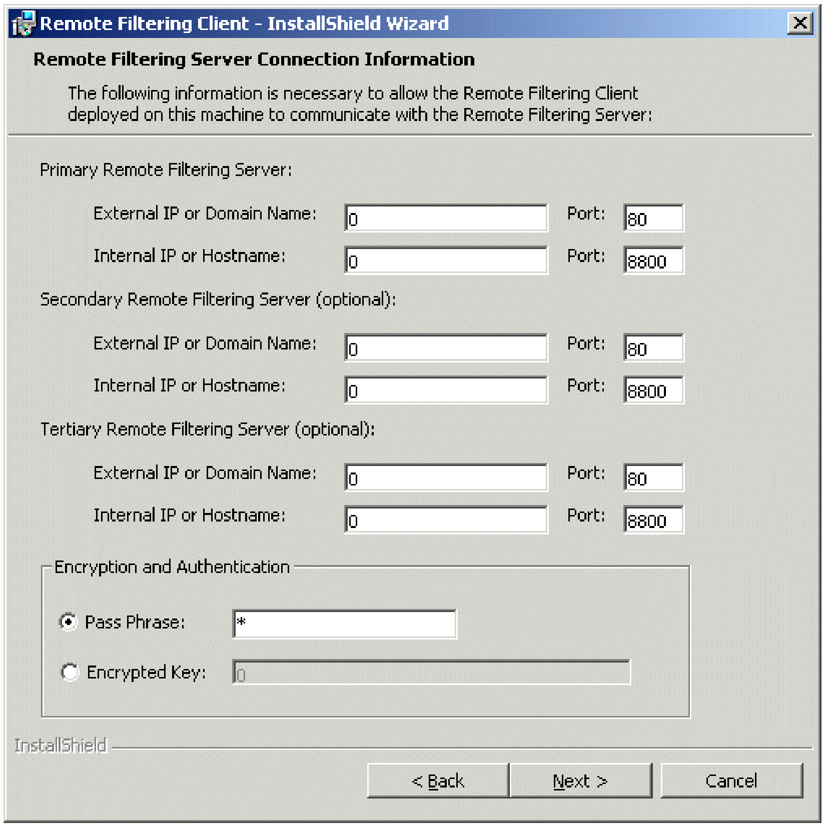
3. Double-click the `CPMClient.msi` file.

    The installer for Remote Filtering Client opens.

4. Click **Next** to continue.

    Remote Filtering Clients must be able to connect with a Remote Filtering Server from outside your organization’s Internet gateway or firewall.

5. Provide connection information for the Remote Filtering Servers that this client will use for Web filtering.



Remote Filtering Client - InstallShield Wizard

Remote Filtering Server Connection Information

The following information is necessary to allow the Remote Filtering Client deployed on this machine to communicate with the Remote Filtering Server:

Primary Remote Filtering Server:

External IP or Domain Name: 0 Port: 80

Internal IP or Hostname: 0 Port: 8800

Secondary Remote Filtering Server (optional):

External IP or Domain Name: 0 Port: 80

Internal IP or Hostname: 0 Port: 8800

Tertiary Remote Filtering Server (optional):

External IP or Domain Name: 0 Port: 80

Internal IP or Hostname: 0 Port: 8800

Encryption and Authentication

● Pass Phrase: *

○ Encrypted Key: 0

The Remote Filtering Client must be configured to connect with a primary Remote Filtering Server.

If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, Remote Filtering Client must be configured to connect with these as well. Remote Filtering Client attempts to connect with the primary Remote Filtering Server first, and then rotates through the list in order until a functioning server is located.

✓ **NOTE**

Remote Filtering Server has a timeout value of 2 minutes for inactivity. If the remote workstation does not send an Internet request to a Remoter Filtering Server to which it is connected in that time period, the server drops the connection. At the next Internet request, Remote Filtering Client attempts to connect with the primary Remote Filtering Server again. This protects server performance by constantly reducing the number of unused connections that might otherwise accumulate.

6. In the **Primary Remote Filtering Server** section of the screen, enter connection information for the Remote Filtering Server with which you want this client to attempt to connect first.

- Enter the externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine in the **External IP or Domain Name** field.

Important

You must use the same external address in *the same address format*—IP address or qualified domain name (FQDN)—that you entered when you installed this Remote Filtering Server. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing Remote Filtering Server, you enter the same IP address in this field. If you entered a machine name in the form of an FQDN, enter the same FQDN here.

- Enter the port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.
- Enter the internal IP address or the fully qualified domain name for the primary Remote Filtering Server machine in the **Internal IP or Hostname** field.
- Enter the port number for the internal communication port on the primary Remote Filtering Server that can be accessed only from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when this Remote Filtering Server was installed.

NOTE

If Remote Filtering Client is on a laptop computer that is used both inside and outside the network firewall, this port allows Websense software to determine where the machine is located and filter it appropriately. The machine is filtered in the same way as an internal client when it is used inside the organization’s network firewall, and by Remote Filtering Service when it is used remotely.

7. If you have installed the optional secondary and tertiary Remote Filtering Servers to provide failover protection, enter connection information for these servers in the **Secondary Remote Filtering Server** and **Tertiary Remote Filtering Server** sections of the screen.
8. In the **Encryption and Authentication** section, select **Pass Phrase** and enter the same pass phrase that was entered in the **Pass Phrase** field during installation of the primary Remote Filtering Server. (The secondary and tertiary Remote Filtering Servers must have the same pass phrase as their primary Remote Filtering Server.)

NOTE

If you forgot your pass phrase, you can enter the **Encrypted Key** (shared secret) that was derived from the pass phrase. To locate this key in your system, contact Websense Technical Support.

9. Click **Next** to continue.
10. Click **Install** to begin installation.

    When the installer is finished, a message appears advising you that the procedure was successful.

11. Click **Finish** to exit the installer.
12. If a message appears indicating that you must restart the machine, click **Yes** to restart now.
13. Proceed to *Chapter 3: Initial Setup*

Installing with a third-party deployment tool

Before deploying Remote Filtering Client to workstations, make sure that the Remote Filtering Server to which these clients will connect has been correctly installed on a separate machine. See *Remote Filtering Server*, page 15 for details.

To obtain the installer for Remote Filtering Client, install the Remote Filtering Client Pack on a Windows machine (see *Remote Filtering Client Pack*, page 19 for instructions). If you selected the default installation path of `C:\Program Files\Websense`, the installer (`CPMClient.msi)` is placed in the following location:

```
C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI\
```

To deploy the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

Command line parameters

This section provides the command line parameters required to install Remote Filtering Client using a third-party deployment tool.

Remote Filtering Clients are installed on user workstations or notebook computers that are used outside your organization's Internet gateway or firewall. These machines must be able to connect with a Remote Filtering Server that is located inside the Internet gateway or firewall.

Each Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If optional secondary and tertiary Remote Filtering Servers were installed to provide failover capability for the primary server, the Remote Filtering Client must be configured to connect with these as well. Remote Filtering Client attempts to connect with the primary Remote Filtering Server first, and then rotates through the list in order until a functioning server is located.

✓ **NOTE**
Command line parameters are *not* case sensitive.

Primary Remote Filtering Server

The following parameters identify the primary Remote Filtering Server:

- **PRIMARY_WISP_ADDRESS=**<*external IP address or FQDN of primary Remote Filtering Server*>

The externally visible address for the primary Remote Filtering Server machine, as entered in the **External IP Address or Host Name** field when the primary Remote Filtering Server was installed.

Important

This must be the same external address in *the same address format*—IP address or a fully qualified domain name (FQDN)—that was entered when this Remote Filtering Server was installed. That is, if you entered an IP address in the **External IP Address or Host Name** field when installing the Remote Filtering Server, you must enter the same IP address here. If you entered a machine name in the form of an FQDN, you must enter the same FQDN here.

- **PRIMARY_WISP_PORT=***<external port number of primary Remote Filtering Server>*

  The port number for the externally visible port used to communicate with the primary Remote Filtering Server from outside the network firewall. This must be the same port entered in the **External Communication Port** field when this Remote Filtering Server was installed.
- **PRIMARY_INTERNAL_WISP_ADDRESS=<***internal IP address or FQDN of primary Remote Filtering Server***>**

  The internal address, visible from inside the network firewall, for the machine on which the primary Remote Filtering Server is installed.
- **PRIMARY_INTERNAL_WISP_PORT=***<internal port number of primary Remote Filtering Server>*

  The port number for the internal communication port on the primary Remote Filtering Server that can only be accessed from inside the network firewall. This must be the same port entered in the **Internal Communication Port** field when the Remote Filtering Server was installed.

Failover servers

The following parameters identify the optional secondary and tertiary Remote Filtering Servers:

- **SECONDARY_WISP_ADDRESS=***<external IP address or FQDN of secondary Remote Filtering Server>*
- **SECONDARY_WISP_PORT=***<external IP address or FQDN of secondary Remote Filtering Server>*
- **SECONDARY_INTERNAL_WISP_ADDRESS=***<internal IP address or FQDN of secondary Remote Filtering Server>*
- **SECONDARY_INTERNAL_WISP_PORT=***<internal IP address or FQDN of secondary Remote Filtering Server>*
- **TERTIARY_WISP_ADDRESS=***<external IP address or FQDN of tertiary Remote Filtering Server>*
- **TERTIARY_WISP_PORT=***<external IP address or FQDN of tertiary Remote Filtering Server>*
- **TERTIARY_INTERNAL_WISP_ADDRESS=***<internal IP address or FQDN of tertiary Remote Filtering Server>*
- **TERTIARY_INTERNAL_WISP_PORT=***<internal IP address or FQDN of tertiary Remote Filtering Server>*

These addresses and port numbers must match those entered during installation of the Remote Filtering Servers, as noted above for the primary Remote Filtering Server.

Installation options

- **PATH=**<*installation path*>

  Directory in which Remote Filtering Client is installed on each client workstation. If this parameter is not specified, the default installation path is `C:\PROGRAM FILES\Websense\WDC.` The `WDC` directory is hidden by default.

- **PASSPHRASE=**<*pass phrase for Remote Filtering Server*>

  The **Pass Phrase** entered when the primary Remote Filtering Server was installed. Note that all Remote Filtering Servers in the same failover group (primary, secondary, and tertiary) must have the same pass phrase.

- **REBOOT=YES | NO | PROMPT | IF_NEEDED_PROMPT**

  This parameter defines whether the client workstation is automatically restarted after Remote Filtering Client is installed (or uninstalled). Values for this parameter are:

  - **YES**: Machines are restarted, and employees are not prompted to restart.
  - **NO**: Machines are not restarted, and employees are not prompted to restart.
  - **PROMPT**: Employees are prompted to restart their machines.
  - **IF_NEEDED_PROMPT**: Employees are prompted to restart their machines only if a restart is required. (Default.)

> **Important**
>
> You must restart the workstation after installing Remote Filtering Client if:
>
> - The workstation's operating system is Windows 2000.
> - Check Point® VPN-1® is running on the workstation.
> - You have uninstalled, upgraded, or repaired Remote Filtering Client

- **REINSTALL=ALL**

  This parameter is used only for repairing or upgrading an existing installation of Remote Filtering Client. It indicates the components to remove and reinstall. The value should always be set to `ALL`.

- **REINSTALLMODE=veums | voums**

  This parameter is used only for repairing or upgrading an existing installation of Remote Filtering Client. It defines either a repair or an upgrade. The possible values are:

  - **veums**: for repairs only
  - **voums**: for upgrades only

- **/qn**

  This is the switch for quiet installation mode. When you use this option, Remote Filtering Client installs without displaying information to the employee at the workstation. If you do not use **`/qn`**, the installer launches in interactive mode, and installation dialog boxes display to the employee during installation. Most organizations choose the quiet mode, as interactive mass deployment has little value.

Installation syntax

Replace the variables in angle brackets with appropriate values for your network. Type the command on a single line with no returns.

msiexec /i cpmclient.msi PASSPHRASE=<*pass phrase for Remote Filtering Server*> **PRIMARY_WISP_ADDRESS=**<*external IP Address or FQDN of primary Remote Filtering Server*> **PRIMARY_WISP_PORT=**<*external port number of primary Remote Filtering Server*> **PRIMARY_INTERNAL_WISP_ADDRESS=<***internal IP address or host name of primary Remote Filtering Server***>** **PRIMARY_INTERNAL_WISP_PORT=**<*internal port number of primary Remote Filtering Server***>** **REBOOT=**<*reboot parameter*> **/qn**

For example, the installation command might look like this:

```
msiexec /i cpmclient.msi PASSPHRASE=2gbatfm PRIMARY_WISP_ADDRESS=63.16.200.232
PRIMARY_WISP_PORT=80 PRIMARY_INTERNAL_WISP_ADDRESS=10.218.5.60
PRIMARY_INTERNAL_WISP_PORT=9000 REBOOT=IF_NEEDED_PROMPT /qn
```

If you are using secondary or tertiary Remote Filtering Servers, you must enter parameters for those machines as well.

Repair syntax

The following example shows the syntax to repair an existing installation of Remote Filtering Client using a third-party deployment tool. Type it on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL REINSTALLMODE=veums /qn
```

When the installer repairs an installation of Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command.

Uninstall command

The following is the actual command that can be used to uninstall Remote Filtering Client with a third-party deployment tool. Type it on a single line with no returns.

```
msiexec.exe /x - {14D74337-01C2-4F8F-B44B-67FC613E5B1F} /qn
```

CHAPTER 3 Initial Setup

Review the following setup tasks before attempting to filter workstations remotely:

- Firewall configuration
- Filtering behavior when Remote Filtering Server unavailable
- Remote Filtering Client log

Firewall configuration and component communication

Some firewall configuration is necessary to enable Web filtering on remote workstations. Firewalls must be configured to allow Remote Filtering Server to communicate with the remote workstations and with Filtering Service.

Client workstations and Remote Filtering Server

The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations should be configured as follows:

- Open the Remote Filtering Server's **External Communication Port** on these firewalls to accept connections from Remote Filtering Clients on workstations located outside the network firewall. Typically, this is port 8080, which was defined during installation of Remote Filtering Server. The default is 80.
- Block connections to the Remote Filtering Server's **Internal Communication Port** from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of Remote Filtering Server.

See the documentation for your firewall product for configuration instructions.

Filtering Service and Remote Filtering Server

If there is a firewall between the Remote Filtering Server machine and the Filtering Service machine, configure it as follows:

- Open the Filtering Service's **Filter port** (by default, 15868) on this firewall to accept connections from the Remote Filtering Server.
- Open the Filtering Service's **Block Page port** (by default, 15871) on this firewall to allow Filtering Service to serve block pages to remote users.

See the documentation for your firewall product for configuration instructions.

Fail closed option

You can configure Remote Filtering Server to block remote users' Internet access when they are unable to connect with Remote Filtering Server. You can also configure the length of time that Remote Filtering Client attempts to connect with a Remote Filtering Server before failing closed and blocking access to all Web sites.

This behavior is controlled by the following two parameters in the `securewispproxy.ini` file on the Remote Filtering Server machine:

- **FailClose**: The `FailClose` parameter specifies whether a Remote Filtering Client fails open or closed when connectivity with Remote Filtering Server is lost.
  - When set to **false**, Remote Filtering Client fails open and all HTTP traffic is allowed. The default value is `false`.
  - When set to **true**, Remote Filtering Client fails closed and all HTTP traffic is blocked.
- **FailCloseTimeout**: The `FailCloseTimeout` parameter applies only when Remote Filtering clients are set to fail closed (`FailClose=true`). `FailCloseTimeout` specifies the amount of time, in minutes, that Remote Filtering Client is given to connect with Remote Filtering Server before failing closed and blocking all HTTP traffic. During the connection attempt, all HTTP traffic is permitted. The default value is 15, but can be set to any integer from 0 to 60. A value of 0 disables the timeout. If any value outside the acceptable range (or any invalid input) is entered, the timeout defaults to 15 minutes.

To set fail closed parameters:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the following default locations:
   - Windows: `\Program Files\Websense\bin`
   - Linux and Solaris: `/opt/Websense/bin`
2. Open the `securewispproxy.ini` file in a text editor.
3. Change the value of the `FailClose` parameter to `true`.
4. If you leave the `FailCloseTimeout` set to its default value of 15, Remote Filtering Client tries to connect to Remote Filtering Server for 15 minutes before failing closed and blocking all HTTP traffic.
   - To change the length of time, in minutes, that the Remote Filtering Client tries to connect, change the value of `FailCloseTimeout` to an integer from 1 to 60.
   - To disable the timeout, change the value of `FailCloseTimeout` to 0. The Remote Filtering Client keeps trying to establish a connection.
5. Save your changes.
6. Restart Remote Filtering Server.

The new settings are applied to all Remote Filtering Clients that connect with Remote Filtering Server.

✓ **NOTE**

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `FailClose` and `FailCloseTimeout` parameters in the `securewispproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

Remote Filtering Client log

Each Remote Filtering Client installed on a workstation maintains a local log file that records the following events:

- Each activation after the machine leaves the corporate network
- Each deactivation after the machine enters the corporate network
- When Remote Filtering Client is restarted
- When filtering fails open (allows access to all Web sites when connectivity with Remote Filtering Server is lost)
- When filtering fails closed (blocks access to all Web sites when connectivity with Remote Filtering Server is lost)
- When Remote Filtering Client receives a policy update

You can change the maximum size of this local log file by editing the `LocalLogSize` parameter in the `securewispproxy.ini` file on the Remote Filtering Server machine. The `LocalLogSize` parameter defines the maximum size, in MB, of the log file. Once the maximum file size is reached, the log file name is stamped with the current date and time and is saved. A maximum of two log files are maintained; the oldest log is deleted when a third log is started. The default value of `LocalLogSize` is 1, but it can be set to any integer from 0 to 10. To disable the log, enter a value of 0.

To change the maximum size of the Remote Filtering Client's local log file:

1. On the Remote Filtering Server machine, locate the `securewispproxy.ini` file in the `bin` subdirectory in the Websense installation directory.

   The default location of this file is:

   - Windows: `\Program Files\Websense\bin`
   - Linux and Solaris: `/opt/Websense/bin`
2. Open the `securewispproxy.ini` file in a text editor.
3. Change the value of the `LocalLogSize` parameter to any integer from 0 to 10.

   This integer defines the maximum size of the log in megabytes. A value of 0 disables the log.
4. Save your changes.
5. Restart Remote Filtering Server.

The new maximum log size setting is applied to all Remote Filtering Clients that connect with the Remote Filtering Server.

✓ **NOTE**

If you are using Websense Client Policy Manager (CPM) in your network, Remote Filtering parameters are configured in the Desktop tab of Websense Manager. If the CPM Server is present, values set for the `LocalLogSize` parameter in the `securewispproxy.ini` file are ignored.

For information about configuring Remote Filtering features when you are using CPM, see your Websense Client Policy Manager documentation.

CHAPTER 4 Upgrading

When you upgrade your Websense Enterprise or Web Security Suite components, you must also upgrade the Remote Filtering components to the same version. Upgrade Remote Filtering Server in the same manner as the rest of the Websense components—by running the v6.3.1 Websense installer on the machine where Remote Filtering Server is installed. Upgrade the Remote Filtering Client Pack by running the main installer on that machine as well. See *Remote Filtering Client Pack*, page 19 for details.

✓ **NOTE**

Remote Filtering Server 6.3.1 is backwards compatible with Remote Filtering Client 6.2. You do not have to upgrade your v6.2 Remote Filtering Clients to v6.3.1, but be aware that they cannot access any Remote Filtering enhancements added after your version of Remote Filtering Client was released.

Remote Filtering Server

Upgrade your Remote Filtering Servers after upgrading Filtering Service. If your network uses a single Remote Filtering Server, filtering for remote machines is disrupted during the upgrade process. Plan for this by configuring an appropriate fail open/fail close option. See *Fail closed option*, page 28 for details. If you employ secondary and tertiary Remote Filtering Servers, they must be configured to communicate with the same Filtering Service as the primary Remote Filtering Server for proper failover filtering to occur.

To upgrade Remote Filtering Server:

1. Log on to the Remote Filtering Server machine with local admin rights.
2. Download the installer package from the Websense download site onto the Remote Filtering Server machine, and then extract the files.

   See *The installer package*, page 13 for instructions.
3. Run the installer and select **Upgrade** when prompted.
4. Follow the onscreen instructions to complete the upgrade process.

Remote Filtering Client

You can upgrade Remote Filtering Clients in your network with either of the following methods:

- **Manual upgrade**: Use the v6.3.1 Remote Filtering Client Pack installer package to uninstall the existing version of Remote Filtering Client on an individual workstation, and then install the new version. This upgrade method does *not* preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

- **Automatic upgrade with third-party tool**: Use the v6.3.1 Remote Filtering Client Pack and a third-party deployment tool to uninstall the existing version of Remote Filtering Client on client workstations, and replace it with the new version. See *Third-party deployment tool*, page 33 for information.

NOTE
If you add Websense Client Policy Manager (CPM) to your network when you upgrade, you do not have to upgrade your Remote Filtering Clients as described in this section. Because the Remote Filtering Client is included as part of the CPM Client Agent, deploy Client Agent with the appropriate remote filtering settings. For more information, see your Websense Client Policy Manager documentation.

Manual procedure

To manually upgrade Remote Filtering Client on a single Windows workstation to v6.3.1:

NOTE
This upgrade method does not preserve existing Remote Filtering Client configuration settings; communication information for Remote Filtering Server must be re-entered.

1. Run the v6.3.1 Websense installer on the Remote Filtering Client workstation to upgrade or install the Remote Filtering Client Pack:
   - If a previous version of the Remote Filtering Client Pack is installed on the machine, the Websense installer detects it. Follow the onscreen instructions to upgrade it to v6.3.1.
   - If no previous version of the Remote Filtering Client Pack exists on the machine, follow the installation instructions in *Remote Filtering Client Pack*, page 19.
2. Navigate to the default installation location of the Client Pack file (`CPMClient.msi`).

   `C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI`
3. Double-click the `CPMClient.msi` file to run the new Remote Filtering Client installer.
4. When the application detects an existing installation of Remote Filtering Client, it asks if you want to remove it.
5. Click **Next** to continue.
6. When the **Remove the Program** dialog box appears, click **Remove**.
7. When the **InstallShield Wizard Completed** dialog box opens, click **Finish** to complete removal of the existing Remote Filtering Client.
8. Restart the machine.
9. Double-click the `CPMClient.msi` file to run the Remote Filtering Client installer again.
10. Click **Next** to continue.
11. Re-enter the connection information for the primary Remote Filtering Server that this client uses for Web filtering. If you are not certain of these values, you can view them in Websense files on the Remote Filtering Server machine:
    a. Navigate to the `securewispproxy.ini` file, located in the `Websense\bin` directory on the Remote Filtering Server machine.

b. Open the `securewispproxy.ini` file with a text editor to view the values of the following Remote Filtering Server parameters:

- External IP address or host name: `ProxyPublicAddress`
- External communication port: `ProxyPort`
- Internal IP address or host name: `ProxyIP`
- Internal communication port: `HeartBeatPort`

c. If you do not remember the pass phrase you defined when installing the Remote Filtering Server, enter the encrypted key instead. The Websense software generates this key automatically by combining the pass phrase you defined with unpublished Websense keys. To locate this key in your system, contact Websense Technical Support.

12. If secondary and tertiary Remote Filtering Servers are being used, re-enter communication parameters for each of these servers as well.
13. Click **Next** to continue.
14. Click **Install** to begin installation.

    When the installer is finished, a message appears advising you that the procedure was successful.
15. Click **Finish** to exit the installer.
16. If a message appears indicating that you must restart the machine, click **Yes** to restart now.

    Remote filtering cannot function until the machine is restarted.

Third-party deployment tool

This upgrade method allows you to deploy version 6.3.1 of Remote Filtering Client to client workstations, while preserving the existing configuration settings.

To obtain the installer for version 6.3.1 of Remote Filtering Client, you can do one of the following:

- Upgrade an existing version of the Remote Filtering Client Pack to version 6.3.1
- Install version 6.3.1 of the Remote Filtering Client Pack on a Windows machine (see *Remote Filtering Client Pack*, page 19 for instructions).

If you selected the default installation path of `C:\Program Files\Websense`, the installer (`CPMClient.msi`) is placed in the following location:

```
C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI
```

To deploy the new version of the Remote Filtering Client to Windows workstations, use this installer with a third-party deployment tool, such as Microsoft® Systems Management Server (SMS) or Novell® ZENworks®.

Upgrade syntax

Following is an example of the syntax to upgrade Remote Filtering Client using a third-party deployment tool. This command must be typed on a single line with no returns.

```
msiexec /i cpmclient.msi REINSTALL=ALL REINSTALLMODE=voums /qn
```

When the installer upgrades an installation of Remote Filtering Client, the current configuration settings are used. If your remote filtering configuration *has not* changed, no additional parameters are necessary. However, if you have changed your configuration, you must include the appropriate parameters and new values in the command. For a complete list of command line parameters, see *Command line parameters*, page 23.

APPENDIX A Troubleshooting

Block pages are not displaying

If Remote Filtering Clients are being filtered correctly, but are not receiving Websense block pages, check the following:

- If there is a firewall between the Websense Filtering Service machine and the Remote Filtering Server machine, ensure that it is properly configured, as described in *Filtering Service and Remote Filtering Server*, page 27. Make sure the **Block Page port** (by default, 15871) has been opened on the firewall. This allows Filtering Service to send block pages to remote users.

  See the documentation for your firewall product if you need information about how to configure your firewall.
- Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. An instance of Remote Filtering Client running on the Remote Filtering Server machine eventually uses all available connections to the server. When the connections are not available, remote workstations cannot connect to the Remote Filtering Server and are not filtered. Uninstall the Remote Filtering Client from the Remote Filtering Server machine.

Troubleshooting procedures for Remote Filtering

Follow these procedures to troubleshoot filtering issues with Remote Filtering Clients:

1. Check that your subscription key includes Remote Filtering.
2. Check that Remote Filtering Server is running.
   - Windows: Use the Windows Services Control Panel to check that Websense Remote Filtering Service is running.
   - Linux and Solaris:
     a. Go to the `/opt/Websense` directory.
     b. From a command prompt, run `./WebsenseAdmin status`
     c. The Remote Filtering Server service should be running. If not, run `./WebsenseAdmin start`
3. Make sure Remote Filtering Server is *not* installed on the same machine as Filtering Service.

   Installing these components on the same machine causes a serious drain on resources on the machine. Filtering becomes very slow, and may eventually fail and allow all requests.
4. Check that any firewalls located between Websense Filtering Service and Remote Filtering Server are correctly configured.

   If there are one or more firewalls between the Filtering Service machine and the Remote Filtering Server machine, check that they have been properly configured, as described in *Filtering Service and Remote Filtering Server*, page 27.

- Make sure the Filtering Service's **Filter port** (by default, 15868) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot accept connections from the Remote Filtering Server.
- Make sure that the **Block Page port** (by default, 15871) has been opened on all firewalls between the Filtering Service and Remote Filtering Server. If this port is not open, Filtering Service cannot send block pages to remote clients through Remote Filtering Server.

5. Check that the external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote workstations have been properly configured, as described in *Client workstations and Remote Filtering Server*, page 27.
    - The Remote Filtering Server's **External Communication Port** on these firewalls must be able to accept connections from Remote Filtering Clients on workstations located outside the network firewall. By default, this is port 80, unless it was changed during installation of the Remote Filtering Server.
    - Access to the Remote Filtering Server's **Internal Communication Port** must be blocked from workstations located outside the network firewall. By default, this is port 8800, unless it was changed during installation of the Remote Filtering Server.
6. Make sure Network Agent is *not* filtering responses to Remote Filtering requests.

    Check that Network Agent is *not* monitoring the machine on which Remote Filtering Server is installed:

    a. Open Websense Manager and connect to the Policy Server.
    b. Select **Server > Settings**.
    c. The **Settings** dialog box appears.
    d. In the **Settings** pane, click **Global Settings** under **Network Agent**.
    e. In the **Internal Network Definition** section of the window, ensure that the IP address for the machine running Remote Filtering Server is *not* included.
        - If the server's IP address is listed individually, select the address from the list and click **Delete**.
        - If the server's IP address is in a range, delete the range and add two ranges around that IP address.
    f. When you are finished, click **OK** at the bottom of the screen to save your changes.

    See the Network Agent chapter in the *Administrator's Guide* for Websense Enterprise and Web Security Suite for more information about configuring Network Agent's global settings.
7. Check that connections are working properly.
    - Check that the remote workstations on which Remote Filtering Client has been installed are able to communicate with the Remote Filtering Server machine. The ping command can be used to verify this connection.
    - Check that the Remote Filtering Server machine is communicating properly with the network. Try to ping the Filtering Service machine and other machines on the local network.
8. Check the `RFSErrors.log` file on the Remote Filtering Server machine.
    a. Open the `RFSErrors.log` file in a text editor. The default location of the file is:
        - Windows: `\Program Files\Websense\bin`
        - Linux and Solaris: `/opt/Websense/bin`
    b. Check for error 64.

This error might indicate that DHCP is enabled for the machine running the Remote Filtering Server.

Solution: Acquire a static IP address and disable DHCP on this machine.

c. Check for error 121.

This error occurs in a Windows Server 2003 environment, and might indicate that Service Pack 1 is not installed. This service pack is required to run Remote Filtering Server.

Solution: Download and install the service pack from the Microsoft Web site.

9. Check that communications are properly configured for Remote Filtering Server and Remote Filtering Clients.

Remote Filtering Clients must be able to connect to Remote Filtering Server from both inside and outside the Internet gateway or network firewall. The correct communication information—IP addresses and port numbers for internal and external communications—must be entered during installation. See *Remote Filtering Server*, page 15 for more information.

a. On the Remote Filtering Server machine, open the `securewispproxy.ini` file in a text editor. The default location of this file is:

- Windows: `\Program Files\Websense\bin`
- Linux and Solaris: `/opt/Websense/bin`

b. Under `Proxy Server parameters`, make note of these settings:

- **ProxyIP**: Must match the IP address of the network interface card (NIC) on the Remote Filtering Server machine that is used for internal communications.
- **ProxyPort**: The port on the Remote Filtering Server machine used for external communications. Typically, this is 8080. The default is 80.
- **ProxyPublicAddress**: The IP address or host name used for external access to the Remote Filtering Server machine from outside the external network firewall or internet gateway.

c. Under `HeartBeat Server Parameters`, make note of the **HeartBeatPort** setting. This is the Internal Communication Port on the Remote Filtering Server machine, used for communication with Remote Filtering Client machines that have been moved inside the external network firewall. The default setting is 8800.

d. Open a command prompt and run an IP configuration command on the Remote Filtering Server machine to get the IP addresses for each network interface card (NIC) in that machine:

- Windows: `ipconfig`
- Linux and Solaris: `ifconfig -a`

e. Check that these IP address values match the Proxy Server parameters found in the `securewispproxy.ini` file.

f. Checked the values on the Remote Filtering Client machines. Contact Websense Technical Support for assistance. The technician needs the information gathered in the previous steps to verify that communications are properly configured.

10. Check that the pass phrases match.

The pass phrase for Remote Filtering Server and the Remote Filtering Clients must match. Checking to see if they match requires access to configuration and registry files. Incorrect changes to these files can interfere with machine operation. Contact Websense Technical Support for assistance.

If the pass phrase used for all Remote Filtering Clients does not match the pass phrase configured for the Remote Filtering Server:

a. Reinstall the Remote Filtering Server and enter the proper pass phrase when prompted.

b. Reinstall the Remote Filtering Clients, using the same pass phrase.

If Websense Client Policy Manager (CPM) is installed, or will be installed in the future, note the following:

- If Websense Client Policy Manager (CPM) is already installed in your network, enter the same pass phrase used to install CPM.
- If you install CPM in your network in the future, use the same pass phrase you used to install the Remote Filtering components.

11. Ensure that the load balancer is forwarding packets to the Remote Filtering Server.

If you are using a load balancer, ensure that it is forwarding packets to the Remote Filtering Server. See your load balancing appliance or software documentation for configuration information.