Remote Filtering

Websense® Web Security
Websense Web Filter
Contents

Chapter 1  Introduction ................................................. 5
    Remote Filtering Client system requirements ................. 5
    Remote Filtering Server system requirements ................. 6
        Hardware recommendations .......................... 6
    Deployment information .................................. 7
    How Remote Filtering works .............................. 8
        Outside the network ................................ 8
        Inside the network .................................. 10
        Identifying remote users ............................. 10
        When server communication fails .................... 11
        Virtual Private Network (VPN) ....................... 11

Chapter 2  Installation .............................................. 13
    Preparing for installation .................................. 13
    Downloading and starting the installer .................... 14
    Installing Remote Filtering components ................... 16
        Installing Remote Filtering Client Pack separately .. 19
    Deploying Remote Filtering Client ......................... 19
        Preparing to install on Microsoft Windows Vista machines .. 20
        Installing manually ................................. 20
        Installing with a third-party deployment tool .......... 23

Chapter 3  Initial Setup ............................................. 27
    Firewall configuration and component communication ........ 27
        Remote Filtering Server and client computers .......... 27
        Remote Filtering Server and other filtering components .. 27
    Configuring Remote Filtering settings ...................... 28

Chapter 4  Upgrading ................................................. 31
    Preparing to upgrade Remote Filtering Server .............. 31
    Upgrading Remote Filtering Server ........................ 32
    Upgrading Remote Filtering Client ......................... 33
        Manual procedure ................................... 33
        Third-party deployment tool ......................... 34
        Upgrade syntax ..................................... 35

Appendix A  Troubleshooting ....................................... 37
    Block pages are not being displayed ....................... 37
Quota, Continue not offered for remote HTTPS or FTP requests ............37
When client machines use a proxy server ........................................38
Troubleshooting procedures for Remote Filtering .........................38
With Remote Filtering, Websense Web Security and Websense Web Filter can filter HTTP, HTTPS, and FTP requests from machines outside the network.

Remote Filtering requires the following components:

- **Remote Filtering Client** is installed on each machine that will be filtered when used outside the network. This client is configured to communicate with the Remote Filtering Server.
- **Remote Filtering Server** resides inside your firewall, and acts as a proxy to Websense Filtering Service.

All communication between Remote Filtering Client and Remote Filtering Server is authenticated and encrypted.

### Remote Filtering Client system requirements

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

<table>
<thead>
<tr>
<th>Hardware Recommendations</th>
<th>Operating System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Pentium 4 or greater</td>
<td>• Windows XP Professional with SP1, SP2, or SP3</td>
</tr>
<tr>
<td>• Free disk space: 25 MB for</td>
<td>• Windows Vista (Ultimate, Enterprise, or Business)</td>
</tr>
<tr>
<td>installation; 15 MB to</td>
<td>• Windows Server 2003 (Standard or Enterprise)</td>
</tr>
<tr>
<td>run the application</td>
<td>• Windows Server 2003, SP1 (Standard or Enterprise)</td>
</tr>
<tr>
<td>• 512 MB RAM</td>
<td>• Windows Server 2003, R2 (Standard or Enterprise)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 (x86), (Standard or Enterprise)</td>
</tr>
</tbody>
</table>
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
- Red Hat Enterprise Linux 5 (Standard, Advanced Platform, Desktop with Workstation option)
- 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.

<table>
<thead>
<tr>
<th>Network Size</th>
<th>Hardware Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-500 clients</td>
<td><strong>Windows</strong> or <strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td>• Quad-Core Intel Xeon, 2.5 GHz or greater</td>
</tr>
<tr>
<td></td>
<td>• 2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• 20 GB of free disk space</td>
</tr>
<tr>
<td>500-2000 clients</td>
<td><strong>Windows</strong> or <strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td>• Quad-Core Intel Xeon, 2.5 GHz or greater</td>
</tr>
<tr>
<td></td>
<td>• 2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• 20 GB of free disk space</td>
</tr>
<tr>
<td>2000-5000 clients</td>
<td><strong>Windows</strong> or <strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td>• Quad-Core Intel Xeon, 2.5 GHz or greater</td>
</tr>
<tr>
<td></td>
<td>• 2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• 20 GB of free disk space</td>
</tr>
<tr>
<td>5000-10000 clients</td>
<td><strong>Windows</strong> or <strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td>• Quad Xeon, 3.2 GHz or greater</td>
</tr>
<tr>
<td></td>
<td>• 1 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• 20 GB of free disk space</td>
</tr>
<tr>
<td></td>
<td>- or - Static load balancing with Dual Xeon, 3.2 GHz or greater</td>
</tr>
<tr>
<td>10000+ clients</td>
<td><strong>Windows</strong> or <strong>Linux</strong></td>
</tr>
<tr>
<td></td>
<td>• Static load balancing with Quad Xeon, 3.2 GHz or greater</td>
</tr>
<tr>
<td></td>
<td>• 2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• 20 GB of free disk space</td>
</tr>
</tbody>
</table>
Deployment information

When you install Remote Filtering, observe the following guidelines:

◆ Install Remote Filtering Server:
  ■ Inside your organization’s outermost network firewall
  ■ In the DMZ outside the firewall that protects the rest of the network
  ■ On its own, dedicated machine
    This machine must be able to communicate with Websense Filtering Service and with the remote machines 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 of these Remote Filtering Servers 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 software, see the Deployment Guide.

**How Remote Filtering works**

Websense Remote Filtering Client is an agent that handles Internet requests on machines used outside the organization’s network. When the user of a Remote Filtering Client machine makes a browser-based Internet request, Remote Filtering Client determines whether to query Remote Filtering Server about the request based on whether the machine is within or outside the network.

**Outside the network**

When a computer is started **outside** the network, Remote Filtering Client attempts to send a **heartbeat** to Remote Filtering Server. The heartbeat is unsuccessful because the heartbeat port is blocked at the external firewall.
This heartbeat failure prompts Remote Filtering Client to send a query about each HTTP, HTTPS, or FTP request over the configured port (default 80) to Remote Filtering Server in the DMZ. Remote Filtering Server then forwards the request to Filtering Service inside the network. Filtering Service evaluates the request and sends a response to Remote Filtering Server, which then sends the response to the remote computer. If the site is blocked, Remote Filtering Client requests and receives the appropriate block page, which is displayed to the user.

Remote Filtering Client delays each filtered request until it receives a response from Remote Filtering Server. Depending on the response received, Remote Filtering Client either permits the site or displays the block page.

A log file tracks Remote Filtering activities, such as entering and leaving the network, failing open or closed, and restarting the client. Remote Filtering Client creates the log file when it starts for the first time. You control the presence and size of this log file. See Configuring Remote Filtering settings, page 28.
Inside the network

When the filtered machine is started inside the network, the Remote Filtering Client attempts to send a heartbeat to the Remote Filtering Server in the DMZ. The heartbeat is successful because the heartbeat port is open on the internal firewall.

In this case, 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 Network Agent or an integrated product (such as Cisco Pix or Microsoft ISA Server). The request is filtered like any other internal request.

Identifying remote users

How a user logs on to the remote machine determines which policy is enforced.

If a user logs on using cached domain credentials (network directory logon information), Filtering Service is able to resolve the user name, and applies appropriate user and group-based policies to the remote computer. Additionally, Internet activity is logged under the network user name.

If the user logs on with a user account that is local to the computer, Filtering Service cannot resolve the user name. If manual authentication is enabled, the user receives a logon prompt when opening a browser. In this situation, Internet requests are filtered by the appropriate user or group policy.

If the user logs on with a user account that is local to the computer, and manual authentication is not enabled, Internet requests are filtered by the Default policy. Internet activity is logged under the local user name. Remote Filtering does not filter
on the basis of policies assigned to computers (IP addresses) or networks (IP address ranges).

**Note**

- Selective authentication settings do not apply to remote filtering users.

### When server communication fails

Filtering occurs when Remote Filtering Client, outside the network, successfully communicates with Remote Filtering Server in the network DMZ. However, there may be times when that communication is unsuccessful.

The action Remote Filtering Client takes if it cannot contact Remote Filtering Server is configurable. By default, Remote Filtering Client permits all HTTP, HTTPS, and FTP requests it cannot communicate with Remote Filtering Server (*fail open*).

Remote Filtering Client continues attempting to contact Remote Filtering Server. When communication is established, the appropriate filtering policy is enforced.

When Remote Filtering Client is configured to *fail closed*, a timeout value is applied (default 15 minutes). The clock begins running when the remote computer 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. When this occurs, the appropriate filtering policy is enforced.
- If Remote Filtering Client cannot connect within the configured timeout period, all Internet access is blocked until connection to Remote Filtering Server can be established.

**Note**

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

This timeout period allows users who pay for Internet access when travelling to start the computer and arrange for connection without being locked out. If the user does not establish Web access before the 15 minute timeout period expires, Web access cannot be established during that session. When this occurs, the user must restart the computer to begin the timeout interval again.

To change the *fail open/fail closed* setting, and change the timeout value, see *Configuring Remote Filtering settings, page 28*.

### Virtual Private Network (VPN)

Websense Remote Filtering supports VPN connections, including split-tunneled VPN. When a remote computer connects to the internal network via VPN (non-split-
tunneled), Remote Filtering Client is able to send a heartbeat to Remote Filtering Server. As a result, Remote Filtering Client becomes passive and all HTTP, HTTPS, and FTP requests from the remote computer are filtered by Network Agent or an integration product, like other in-network computers.

If the remote computer connects to the internal network via a split-tunneled VPN client, Remote Filtering Client detects this and does not send a heartbeat to Remote Filtering Server. Remote Filtering Client assumes that it is operating externally and submits requests to Remote Filtering Server for filtering.

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

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL
You must have a functioning Websense Web filtering deployment before installing any Remote Filtering components. See the Installation Guide, and the Installation Supplement for your integration product, if needed, for instructions on installing and configuring your Websense software.

- For Remote Filtering system requirements, see Remote Filtering Client system requirements, page 5.
- For deployment instructions, see Deployment information, page 7.

### Preparing for installation

Before installing Remote Filtering components, determine whether a firewall exists between the machine where Remote Filtering Server will be installed and the machine or machines where Policy Broker, Policy Server, and Filtering Service are installed.

If so, configure that firewall to permit communication over the following ports (or the alternate ports you configured when you installed primary Websense components). Some of these ports must be open for installation, but can be closed after that, as noted. Others must stay open for Remote Filtering to function properly.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>55880</td>
<td>Enables communication from Remote Filtering Server to Policy Broker.</td>
</tr>
<tr>
<td>55806</td>
<td>Enable communication from Remote Filtering Server to Policy Server during installation. Can be closed after installation is complete.</td>
</tr>
<tr>
<td>40000</td>
<td></td>
</tr>
<tr>
<td>55825</td>
<td>Enables communication from Policy Server to Remote Filtering Server during installation. Can be closed after installation is complete.</td>
</tr>
</tbody>
</table>
Most environments also include a firewall between the Remote Filtering Server and the Remote Filtering Clients that operate outside the network. This firewall must be configured as follows to enable Remote Filtering to function properly. You can configure this firewall before or after installing Remote Filtering Server and deploying Remote Filtering Clients.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15868</td>
<td>Filtering Service Port. Enables communication between Filtering Service and Remote Filtering Server.</td>
</tr>
<tr>
<td>15871</td>
<td>Block Page Port. Enables Filtering Service to send block messages to users. If this port is not open on the firewall, users are still blocked, but do not receive a block message.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 (or 8080)</td>
<td>Open this external communication port on the external firewall. This enables Remote Filtering Server to accept connections from Remote Filtering Clients on computers located outside the network firewall. The default is 80, but many installations set it to port 8080 during installation of Remote Filtering Server.</td>
</tr>
<tr>
<td>8800</td>
<td>Close access to this internal communication port on the external firewall from computers located outside the network firewall. This default may have been changed when Remote Filtering Server was installed.</td>
</tr>
</tbody>
</table>

**Downloading and starting the installer**

The Websense Web Security and Websense Web Filter installer includes the Remote Filtering components. If the installer has already been downloaded to the machine where you plan to install Remote Filtering Server, go directly to step 5.

Otherwise, follow these instructions to download and extract the installer.

1. Log on to the Remote Filtering Server installation machine with administrative privileges:
   - **Linux**: Log on as root.
   - **Windows**: Use an account with domain and local administrator privileges.
2. Close all applications and stop any anti-virus software.
3. On Linux machines, create a setup directory for the installer files:
   - For example: /root/Websense_setup
4. Download the installer package for your product:
Installation

a. Log on to MyWebsense.com, and then click the Downloads link. If you do not have an account, follow the instructions on the page to create one.

b. Scroll through the Product Filter list and select either Web Security Suite - Web Security or Websense Enterprise - Web Filter as the product.

c. Download the installer package to a folder on the installation machine.

5. Extract the installation program and launch the installer:

Windows

a. Double-click the downloaded file. If prompted, click Run to start the extraction program. The installation program should start automatically.

If the installer does not start automatically, go to the temporary directory for the current user account (by default, C:\Documents and Settings\<user name>\Local Settings\Temp\<generated name>.tmp) and run Setup.exe.

If another program, such as Internet Explorer, is running, the installation screens may be hidden behind that program’s window.


Linux

a. In the setup directory, enter the following command to unzip the file:

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

For example: `gunzip Websense70Setup_Lnx.tar.gz`

b. Expand the file into its components with the following command:

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

For example: `tar xvf Websense70Setup_Lnx.tar`

This command places the following files into the setup directory:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.sh</td>
<td>Installation program.</td>
</tr>
<tr>
<td>Setup</td>
<td>Archive file containing related installation files and documents.</td>
</tr>
</tbody>
</table>

c. Enter one of the following commands, depending on whether you want to run the text or GUI installer.

- Text-based install:
  ```
  ./install.sh
  ```
- GUI-based install:
  ```
  ./install.sh -g
  ```

The GUI-based installer is available on English versions of Linux only.

Note

If a firewall is running on the installation machine, turn it off before installing. Otherwise, the installation program displays error messages that it is having difficulty locating other machines.

## Installing Remote Filtering components

Make sure the installation machine meets the hardware and software requirements. Then, use the following procedure to install Remote Filtering Server. If you plan to use a secondary and/or tertiary Remote Filtering Server for failover purposes, perform this procedure for each installation.

1. Make sure that Policy Broker, Policy Server, and Filtering Service are installed and running in the network.
2. Download and launch the installer on the Remote Filtering machine, as described in *Downloading and starting the installer, page 14*.
3. Follow the onscreen instructions and select a **Custom** installation.
4. Select **Remote Filtering Server**. If you are installing on a Windows machine, also select **Remote Filtering Client Pack**. Then click **Next**.
   The Remote Filtering Client Pack is used to install Remote Filtering Client on the target computers. It can only be installed on a Windows machine. If you are installing Remote Filtering Server on Linux, see *Installing Remote Filtering Client Pack separately, page 19*.
5. If a list displays IP addresses for multiple network cards (NICs), select the IP address for the NIC that Remote Filtering Server will use to communicate with other Websense components inside the network firewall, and then click **Next**.
6. Enter the **Policy Server IP address** and **Configuration Port**.

---

**Important**

Be sure that any firewall between Remote Filtering Server and Policy Broker, Policy Server, and Filtering Service have been configured to permit traffic over the ports needed for installation and operation. See *Preparing for installation, page 13*. 

---
7. To enable Remote Filtering Clients to connect to Remote Filtering Server both from inside and from outside the Internet gateway or network firewall, provide the following information, and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External IP Address or Host Name</td>
<td>IP address or machine name (in the form of a fully qualified domain name) that is visible from outside the network firewall. <strong>IMPORTANT</strong>: Remember which format you use for this address. 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.</td>
</tr>
<tr>
<td>External Communication Port</td>
<td>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 choose a different port.) <strong>IMPORTANT</strong>: The port entered as the External Communication Port must be opened on your network firewall to accept connections from Remote Filtering Clients on computers located outside the firewall. See <em>Firewall configuration and component communication, page 27</em>, for more information.</td>
</tr>
<tr>
<td>Internal Communication Port</td>
<td>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. This is the port over which heartbeats are sent. <strong>IMPORTANT</strong>: Be sure that your network firewall is configured to block connections to the Internal Communication Port from computers located outside the firewall. See <em>Firewall configuration and component communication, page 27</em>, for more information.</td>
</tr>
</tbody>
</table>

8. When asked for a **pass phrase**, consider the following information:

- The pass phrase can be any length. This pass phrase is combined with unpublished keys to create an encrypted authentication key (shared secret) for secure client/server communication.
- 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, but can not include spaces. Do not use extended ASCII or double-byte characters.
- You must use this pass phrase when you install the Remote Filtering Clients that will connect with this server.

**Warning**

Record your pass phrase and keep it in a safe place. Websense software cannot be used to retrieve it later.
9. Enter and confirm your pass phrase, and then click **Next**.

10. When asked for Filtering Service information, provide the following, and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual (internal) IP address of Filtering Service</td>
<td>IP address of the machine running Filtering Service.</td>
</tr>
<tr>
<td>A firewall or other network device...</td>
<td>Mark this check box if a firewall or other network device performs network address translation between the Filtering Service machine and the Remote Filtering Server machine. Otherwise, clear this check box.</td>
</tr>
<tr>
<td>Translated (external) IP address of Filtering Service</td>
<td>Enter the translated IP address only if the check box is marked.</td>
</tr>
<tr>
<td>Filter port</td>
<td>Port Filtering Service uses for communication with other Websense services.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server. See <em>Firewall configuration and component communication</em>, page 27, for more information.</td>
<td></td>
</tr>
<tr>
<td>Block Page port</td>
<td>Port Filtering Service uses to send block pages to client machines.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server. See <em>Firewall configuration and component communication</em>, page 27, for more information.</td>
<td></td>
</tr>
</tbody>
</table>

11. Accept the default installation path, or click **Browse** to locate another installation folder. Then, click **Next**.

12. 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 displays a message that it must exit. Click **Exit Setup**, and install Remote Filtering Server on a different machine.
   - If the installation machine has less than the recommended amount of memory, a warning is displayed, but the installation can continue. Click **Next**.

13. Review the installation summary, and then click **Next** to start the installation.

14. Click **Next** to exit the installer.

15. Restart any anti-virus or other software that was stopped for the installation.
16. Install the Remote Filtering Client on computers to be filtered when outside the network. See *Deploying Remote Filtering Client*, page 19.

**Important**

If Network Agent or an integration product 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 Websense Manager Help system.

---

**Installing Remote Filtering Client Pack separately**

The Remote Filtering Client Pack, which must be installed on a Windows machine, is used to install Remote Filtering Client on the target computers. If you installed Remote Filtering Server on Windows, you should have installed Remote Filtering Client Pack at the same time.

If you did not, or if you installed Remote Filtering Server on Linux, use the following procedure to install the Remote Filtering Client Pack.

1. On a Windows server machine, download and launch the installer, as described in *Downloading and starting the installer*, page 14.
2. Follow the onscreen instructions and select a **Custom** installation.
3. Select **Remote Filtering Client Pack**, and then click **Next**.
4. Review the installation summary, and then click **Next** to start the installation.
5. Click **Next** to exit the installer.
6. Install the Remote Filtering Client on computers to be filtered when outside the network. See *Deploying Remote Filtering Client*, page 19.

---

**Deploying Remote Filtering Client**

Remote Filtering Client must be deployed to 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 computers. Remote Filtering Client installs on machines running a Windows operating system only.

**Note**

If you are running Remote Filtering in conjunction with Client Policy Manager, do not install Websense Web Security or Websense Web Filter v7.x. It does not support Client Policy Manager functionality.
The Remote Filtering Client Pack is an installer package (*CPMClient.msi*) that was placed on the Remote Filtering Server machine during installation. By default, it is located at:

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

On Microsoft Windows Vista machines, ensure that User Account Control (UAC) is disabled before using either of the methods below to install the Remote Filtering Client (see *Preparing to install on Microsoft Windows Vista machines*, page 20).

- If you plan to install the client manually, copy the Remote Filtering Client Pack to any directory on individual computers (see *Installing manually*, page 20).
- If you plan to automatically deploy the client via third-party tools, copy the Remote Filtering Client Pack to the appropriate directory on a network server (see *Installing with a third-party deployment tool*, page 23)

The Remote Filtering Client Pack installs on Windows machines only.

---

**Warning**

Do NOT install Remote Filtering Client on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

---

**Preparing to install on Microsoft Windows Vista machines**

Before the Remote Filtering Client can be installed and run on Vista machines, you must disable User Account Control (UAC).

1. Open the Windows Control Panel (Start > Control Panel) on the Vista machine.
2. Under User Account and Family settings, click *Add or remove user account*.
3. Select a user account, such as Guest, and then click *Go to the main User Account page*.
4. Under Make changes to your user account, click *Change security settings*.
5. Deselect the *Use User Account Control (UAC) to help protect your computer* check box, and then click *OK*.
6. Restart the machine.

---

**Installing manually**

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

1. Make sure that the Remote Filtering Server to which this client will connect has been correctly installed. See *Installing Remote Filtering components*, page 16, for installation instructions.
2. Copy the *CPMClient.msi* file from the machine where it was installed (see *Installing Remote Filtering components*, page 16) to a folder on the client computer.
   
   If you selected the default installation path, this file is located at:
3. Double-click the CPMClient.msi file on the client computer.

**Warning**

Do NOT install Remote Filtering Client on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

4. When the installer for Remote Filtering Client opens, click Next.
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](image)

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, 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 machine connects to a Remote Filtering server, and then does not send an Internet request 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 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 to which this client should attempt to connect first.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External IP or Domain Name</td>
<td>Externally visible IP address or fully qualified domain name (FQDN) of the primary Remote Filtering Server machine. <strong>IMPORTANT:</strong> You must use the same address format (either IP address or FQDN) as when you installed this Remote Filtering Server.</td>
</tr>
<tr>
<td>Port</td>
<td>Externally visible port used to communicate with the primary Remote Filtering Server. This must match the external port number entered when installing the primary Remote Filtering Server.</td>
</tr>
<tr>
<td>Internal IP or Hostname</td>
<td>Internal IP address or the fully qualified domain name for the primary Remote Filtering Server machine,</td>
</tr>
<tr>
<td>Port</td>
<td>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 <strong>Internal Communication Port</strong> field when this Remote Filtering Server was installed. <strong>NOTE:</strong> If Remote Filtering Client is on a laptop that is used both inside and outside the network firewall, this allows Websense software to determine where the machine is located and filter it appropriately. See <em>How Remote Filtering works</em>, page 8.</td>
</tr>
</tbody>
</table>

7. If you have installed 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. Do one of the following, and then click **Next**.
- In the **Encryption and Authentication** section, select **Pass Phrase** and enter the same pass phrase that was entered during installation of the primary Remote Filtering Server. (The secondary and tertiary Remote Filtering Servers must have the same pass phrase as the primary Remote Filtering Server.)

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

9. Click **Install** to begin installation.

10. After receiving the successful installation message, click **Finish** to exit the installer.

11. If a message appears indicating that you must restart the machine, click **Yes** to restart now.

12. Proceed to **Initial Setup**.

**Installing with a third-party deployment tool**

Before deploying Remote Filtering Client, make sure that the Remote Filtering Server to which these clients will connect has been correctly installed on a separate machine. See **Installing Remote Filtering components**, page 16 for details.

Locate the Remote Filtering Client Pack (**CPMClient.msi**). If Remote Filtering Server is installed on a Windows machine, the client pack is typically installed on the same machine (see **Installing Remote Filtering components**, page 16). The default installation path is:

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

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

---

**Warning**

Do NOT install Remote Filtering Client on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

---

**Command line parameters**

The command line parameters described in this section are used when installing Remote Filtering Client with a third-party deployment tool.

Keep in mind that Remote Filtering Clients are installed on machines used outside your organization’s Internet gateway or firewall. These machines must be able to connect with a Remote Filtering Server located inside the Internet gateway or firewall.

Additionally, each Remote Filtering Client must be configured to connect with a primary Remote Filtering Server. If secondary and tertiary Remote Filtering Servers
were installed to provide failover capability, the Remote Filtering Client must be configured to connect with these as well.

---

**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>
  
  This is the externally visible IP address for the primary Remote Filtering Server machine, as entered in the **External IP Address or Host Name** field during installation.

  **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.

- **PRIMARY_WISP_PORT**=<external port number>
  
  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 during installation.

- **PRIMARY_INTERNAL_WISP_ADDRESS**=<internal IP address or FQDN>
  
  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>
  
  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 during installation.

### Failover servers

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDARY_WISP_ADDRESS</td>
<td>external IP address or FQDN of secondary Remote Filtering Server</td>
</tr>
<tr>
<td>SECONDARY_WISP_PORT</td>
<td>external port number of secondary Remote Filtering Server</td>
</tr>
<tr>
<td>SECONDARY_INTERNAL_WISP_ADDRESS</td>
<td>internal IP address or FQDN of secondary Remote Filtering Server</td>
</tr>
</tbody>
</table>
These IP addresses and port numbers must match those entered during installation of the Remote Filtering Servers.

### 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
  ```

  This 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 computer 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.

- **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**

### Table: Parameter Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECONDARY_INTERNAL_WISP_PORT</td>
<td>internal port number of secondary Remote Filtering Server</td>
</tr>
<tr>
<td>TERTIARY_WISP_ADDRESS</td>
<td>external IP address or FQDN of tertiary Remote Filtering Server</td>
</tr>
<tr>
<td>TERTIARY_WISP_PORT</td>
<td>external port number of tertiary Remote Filtering Server</td>
</tr>
<tr>
<td>TERTIARY_INTERNAL_WISP_ADDR</td>
<td>internal IP address or FQDN of tertiary Remote Filtering Server</td>
</tr>
<tr>
<td>TERTIARY_INTERNAL_WISP_PORT</td>
<td>internal port number of tertiary Remote Filtering Server</td>
</tr>
</tbody>
</table>
This is the switch for quiet installation mode. When you use this option, Remote Filtering Client installs without displaying information to the user of the client machine. If you do not use this parameter, the installer launches in interactive mode, and installation dialog boxes display to the user during installation. Most organizations choose the quiet mode for a mass deployment.

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>
PRIMARY_WISP_ADDRESS=<external IP address or FQDN>
PRIMARY_WISP_PORT=<external port number>
PRIMARY_INTERNAL_WISP_ADDRESS=<internal IP address or host name>
PRIMARY_INTERNAL_WISP_PORT=<internal port number>
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=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.

Uninstall command

The following command 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
```

To uninstall manually, double-click the CPMClient.msi file on the client machine. The installer asks if you want to uninstall the existing Remote Filtering Client. Respond appropriately to uninstall the client software.
Initial Setup

Review the following setup tasks before attempting to filter remote computers:

- 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 computers. Firewalls must be configured to allow Remote Filtering Server to communicate with the remote computers and with Filtering Service.

Remote Filtering Server and client computers

The external network firewall and any additional firewalls located between the Remote Filtering Server machine and the remote computers 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 computers located outside the network firewall. The default is 80, but this is often changed to port 8080 during Remote Filtering Server installation.
- Block connections to the Remote Filtering Server’s Internal Communication Port from computers located outside the network firewall. The default is 8800.

See the documentation for your firewall product for configuration instructions.

Remote Filtering Server and other filtering components

If there is a firewall between the Remote Filtering Server machine and the machines running Policy Broker, Policy Server, and Filtering Service, configure it as follows.

- Open the Filtering Service filter port (default 15868) to accept connections from the Remote Filtering Server.
Initial Setup

- Open the Filtering Service **block page port** (default 15871) to allow Filtering Service to send block pages to remote users.
- Open the Policy Broker **communication port** (default 55880) to allow Remote Filtering Server to receive configuration updates made in Websense Manager.

See the documentation for your firewall product for configuration instructions.

### Configuring Remote Filtering settings

Unconditional Super Administrators can use the **Settings > General > Remote Filtering** page in Websense Manager to configure options that affect all Remote Filtering Clients associated with this installation.

For details on how Remote Filtering operates, see *How Remote Filtering works*, page 8. For information on the fail closed settings, see *When server communication fails*, page 11.

1. Mark the **Fail closed** check box to block Remote Filtering Clients from all Internet access unless their computer is communicating with Remote Filtering Server.
   
   Be default, this is not selected, which means remote users have unfiltered access to the Internet when their computers cannot communicate with the Remote Filtering Server.

2. If you marked the Fail closed option, use the **Fail closed timeout** field to select a number of minutes up to 60 (default 15), or choose **No timeout**.
   
   During the timeout period, all HTTP, HTTPS, and FTP requests are permitted.
   
   If the Remote Filtering Client cannot communicate with Remote Filtering Server during the timeout interval, all Internet access will be blocked (fail closed).
   
   Choosing **No timeout** may lock out a remote computer before the user can establish Internet connection from a hotel or other pay-for-use-provider. Additionally, Remote Filtering Client attempts to communicate with Remote Filtering Server continuously.

   **Warning**

   Websense, Inc., does not recommend choosing **No timeout** or setting the timeout period to a very low number.

3. Select a **Maximum size for the local log cache** size (in megabytes), up to 10. Choose **No Log** to disable logging.
   
   This controls the size and existence of the log file the remote computer creates when it is initially disconnected from the Remote Filtering Server. This log file tracks the following events:

   - The computer leaves the network
   - The computer rejoins the network
   - The Remote Filtering Client is restarted
- Fail open condition occurs
- Fail closed condition occurs
- Remote Filtering Client receives a policy update

The computer retains the 2 most recent logs. These logs can be used to troubleshoot connection issues or other problems with Remote Filtering.
Upgrading

When you upgrade Websense software, you must also upgrade Remote Filtering Server. Upgrade Remote Filtering Server just like other Websense components—by running the installer on the machine where Remote Filtering Server is installed. You can upgrade the Remote Filtering Client Pack at the same time. See Installing Remote Filtering components, page 16, for details.

Note
Remote Filtering Server is backwards compatible with the previous 2 versions of Remote Filtering Client. For example, v7.0 Remote Filtering Server is compatible with Remote Filtering Client versions v6.3.2 and 6.3.1.

Although you do not have to upgrade your compatible Remote Filtering Clients, be aware that they cannot use any of the Remote Filtering enhancements available in the new version.

Preparing to upgrade Remote Filtering Server

Upgrade each Remote Filtering Server 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 closed option. See Configuring Remote Filtering settings, page 28 for details.

If you are upgrading from version 7.0.x, use the Settings > Remote Filtering page in Websense Manager to configure the fail open/fail closed behavior.

If you are upgrading from version 6.x:

1. On the v6.x Remote Filtering Server machine, stop the service.
   - **Windows:** Use the Windows Services dialog box (Start > Programs > Administrative Tools > Services) to stop the Websense Remote Filtering Server service.
   - **Linux:** Go to the Websense installation directory (by default, /opt/Websense) and enter the following command:
Upgrading Remote Filtering Server

1. Log on to the Remote Filtering Server machine with local administrator rights.
2. Download and run the installer package. See Downloading and starting the installer, page 14, for instructions.
3. Select Upgrade when prompted.
4. Follow the onscreen instructions to complete the upgrade process.
5. After the upgrade is complete, open Websense Manager.
6. Go to the Settings > Remote Filtering page, and change the fail closed options, as needed.
7. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

---

**Note**

There is no need to stop and restart the v7.x Remote Filtering Server after making changes in Websense Manager.

---

### Upgrading Remote Filtering Client

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

- **Manual upgrade**: Use the v7.x Remote Filtering Client Pack installer on each client machine to upgrade the Remote Filtering Client. This upgrade method preserves existing Remote Filtering Client configuration settings.

- **Automatic upgrade with third-party tool**: Use the v7.x Remote Filtering Client Pack and a third-party deployment tool to upgrade the Remote Filtering Client on client computers. See *Third-party deployment tool, page 34* for information.

### Manual procedure

Use the following procedure to manually upgrade the Remote Filtering Client on a Windows machine.

---

**Warning**

Do NOT install Remote Filtering Client on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

---

1. Copy the `CPMCli**ent.msi` file from the machine where it was installed (see *Installing Remote Filtering components, page 16*) to any folder on the client computer.

   By default, this file is located at:
   ```
   C:\Program Files\Websense\bin\RemoteFilteringAgentPack\NO_MSI
   ```

2. Go to **Start > Run** and enter `cmd` to open a command window.

3. Navigate to the location where you placed the `CPMCli**ent.msi` file.

4. Enter the following command:

   ```
   msiexec /i cpmclient.msi REINSTALLMODE="vaums" REINSTALL="ALL"
   ```

   If Error 2734 appears, ensure that the 0x22 ASCII character is used for the double quotes. The Windows Character Map utility can be used to verify this.

5. Close any open applications if you are prompted to do so.
Upgrading

6. Choose **Next** to continue.
7. Choose **Install** to begin installation.
   When the installer is finished, a message appears advising you that the procedure was successful.
8. Choose **Finish** to exit the installer.
9. When prompted to restart the machine, click **Yes** to restart now.
   Remote Filtering cannot function until the machine is restarted.

After upgrading the Remote Filtering Client on remote computers, configure Remote Filtering settings in Websense Manager.

1. Open Websense Manager.
2. Click **Settings > Remote Filtering**.
3. Review and update the settings on this page, as needed.
4. Click **OK** to save any changes.
5. Click **Main > Policy Management > Filters**.
6. Review and update category filters, as needed, to account for the fact that remote clients are now filtered for HTTPS and FTP, as well as HTTP sites.
7. Click **OK** to cache any changes. Changes are not implemented until you click **Save All**.

**Third-party deployment tool**

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

The Client Pack installer is called **CPMClient.msi**. By default, it is located in the following directory:

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

After upgrading the Remote Filtering Client on remote computers:

1. Open Websense Manager.
2. Click **Settings > Remote Filtering**.
3. Review and update the settings on this page, as needed.
4. Click **OK** to save any changes.
5. Click **Main > Policy Management > Filters**.

---

**Warning**

Do NOT install Remote Filtering Client on machines running Remote Filtering Server. That combination eventually causes filtering to fail.

---

34 © Websense, Inc.
6. Review and update category filters, as needed, to account for the fact that remote clients are now filtered for HTTPS and FTP, as well as HTTP sites.

7. Click OK to cache any changes. Changes are not implemented until you click Save All.

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 REINSTALLMODE="vaums"
REINSTALL="ALL" /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.
Block pages are not being displayed

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 *Remote Filtering Server and other filtering components*, page 27. Make sure the **Block Page port** (by default, 15871) has been opened on the internal firewall. This allows Filtering Service to send block pages to remote users.

  See the documentation for your firewall product for information on configuring your firewall.


Quota, Continue not offered for remote HTTPS or FTP requests

When a remote user requests an HTTP site in a category that is set to the Quota or Confirm action, Remote Filtering offers the appropriate block message, including the Quota or Continue button.

However, if a remote user requests an FTP, HTTPS or other SSL site in a category that is set to Quota or Confirm, Remote Filtering presents only a block page. Remote Filtering does not support the Quota and Confirm actions for these protocols.
When client machines use a proxy server

Remote Filtering Server and Remote Filtering Client cannot communicate through a proxy server. Block messages could not be displayed in the remote user’s browser.

If client machines are required to use a proxy server for HTTP, FTP, and SSL (such as HTTPS) communications, update each client machine to add the Remote Filtering Server IP address or hostname (use the exact value entered when you installed Remote Filtering Client) to the list of addresses for which no proxy should be used.

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 dialog box to check that Websense Remote Filtering Service is running.
   - Linux:
     a. Go to the /opt/Websense directory.
     b. Enter the following command:
        
        ./WebsenseAdmin status
     c. The Remote Filtering Server service should be running. If not, enter:
        
        ./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 the machine’s resources. Filtering becomes very slow, and may eventually fail, permitting all Internet requests.
4. Check that any firewalls located between Websense Filtering Service and Remote Filtering Server are correctly configured.
   
   If one or more firewalls sit between the Remote Filtering Server machine and the machines running other Websense components, check that they have been properly configured, as described in Remote Filtering Server and other filtering components, 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 computers have been properly configured, as described in Remote Filtering Server and client computers, 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. Log on to Websense Manager, selecting the Policy Server configured to communicate with this Remote Filtering Server.

b. Go to Settings > Network Agent > Global.

c. In the Internal Network Definition area, 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.

d. When you are finished, click OK to cache your changes. Changes are not implemented until you click Save All.

See the Websense Manager Help system for more information about configuring Network Agent’s global settings.

7. Check that connections are working properly.

- If your firewall allows ICMP, use the ping command to verify that the remote computers on which Remote Filtering Client has been installed are able to communicate with the Remote Filtering Server machine.

- Verify 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. Use a text editor to check the RFSErrors.log file on the Remote Filtering Server machine (located in the C:\Program Files\Websense\bin or /opt/Websense/bin directory, by default).

- 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.

- 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 Installing Remote Filtering components, page 16 for more information.

   a. On the Remote Filtering Server machine, navigate to the Websense bin directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default), and open the securewispproxy.ini file in a text editor.

   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. The default is 80, but many installations set it to port 8080 during installation of Remote Filtering Server.
      • 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 is 8800.

   d. On the Remote Filtering Server machine, open a command prompt and run an IP configuration command to get the IP addresses for each network interface card (NIC) in that machine:
      • Windows: ipconfig
      • Linux: ifconfig -a

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

   f. Check 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 for Remote Filtering Server and all Remote Filtering Clients match.

   a. Stop the Remote Filtering Server service:
      • Windows: Use the Windows Services dialog box.
• **Linux**: Enter the following command:
  ```bash
  ./WebsenseAdmin stop
  ```

b. Open the `securewispproxy.ini` file.

c. Add or edit the `TraceType` entry to read:
  ```ini
  TraceType=All
  ```

d. Save and close the `securewispproxy.ini` file.

e. Start the Remote Filtering Server.
  ```bash
  ./WebsenseAdmin start
  ```

f. Go to a remote client computer and browse the Internet.

g. On the Remote Filtering Server machine, navigate to the Websense `bin` directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default) and open the `traceFile.log` file.

   If it contains errors indicating that “HandShake failed”, the pass phrases set for Remote Filtering Client and Remote Filtering Server most likely do not match.

h. If the pass phrase used for all Remote Filtering Clients does not match the pass phrase configured for the Remote Filtering Server, and you know the pass phrase, reinstall the Remote Filtering Clients with the correct pass phrase.

   If this resolves the problem, repeat steps a) through e) to disable tracing. Either remove the `TraceType` entry, or edit it to read `TraceType=none`.

i. If you do not know the correct pass phrase, reinstall the Remote Filtering Server and enter the proper pass phrase when prompted. Then, reinstall the Remote Filtering Clients, using the same pass phrase.

j. If the same error occurs, contact Websense Technical Support.

11. 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.