Remote Filtering Software

Websense® Web Security
Websense Web Filter
Contents

Chapter 1  Introducing Remote Filtering Software ........................................... 5
  System requirements ................................................................. 6
  Deployment information ............................................................ 7
  How remote filtering works ......................................................... 8
    Identifying remote users ......................................................... 10
  Differences between remote and local filtering ................................. 11
  When server communication fails ............................................... 11
  Virtual Private Network (VPN) .................................................... 12

Chapter 2  Installing remote filtering software ........................................... 13
  Preparing for installation ........................................................... 13
  Installing remote filtering components on Windows .......................... 14
  Installing remote filtering components on Linux ............................... 18
  Deploying Remote Filtering Client .............................................. 22
    Customizing the client installation package ................................. 23
    Installing manually ............................................................... 25
    Installing with a third-party deployment tool ................................ 25
  Uninstalling Remote Filtering Client ......................................... 26

Chapter 3  Setting up remote filtering software .......................................... 27
  Configuring component communication ...................................... 27
  Configuring global remote filtering settings .................................. 28
  Configuring remote filtering to ignore HTTPS or FTP ......................... 29
  Configuring the Remote Filtering Client heartbeat interval .................. 29

Chapter 4  Upgrading remote filtering software ......................................... 31
  Preparing to upgrade Remote Filtering Server .................................. 31
  Upgrading Remote Filtering Server ............................................. 32
  Upgrading Remote Filtering Client ............................................. 32
    Upgrading Remote Filtering Client manually ................................ 33
    Upgrading Remote Filtering Client with a third-party deployment tool . 33

Appendix A  Troubleshooting remote filtering software ............................... 35
  Block pages are not being displayed .......................................... 35
  When client machines use a proxy server ..................................... 35
  General troubleshooting procedures .......................................... 36
Introducing Remote Filtering Software

Deploy Websense remote filtering software to filter Internet requests from machines outside the network. By default, remote filtering software monitors HTTP, HTTPS, and FTP traffic.


Note
In Websense Web Security Gateway Anywhere deployments, hybrid (in-the-cloud) filtering can also be used to filter Internet requests from users outside the network.

Remote filtering software includes 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.

This guide provides planning, installation, upgrade, configuration, and troubleshooting information for remote filtering software.

<table>
<thead>
<tr>
<th>Planning</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• System requirements</td>
<td>• Preparing for installation</td>
</tr>
<tr>
<td>• Deployment information</td>
<td>• Installing remote filtering components on Windows</td>
</tr>
<tr>
<td>• How remote filtering works</td>
<td>• Installing remote filtering components on Linux</td>
</tr>
<tr>
<td>• Differences between remote and local filtering</td>
<td>• Deploying Remote Filtering Client</td>
</tr>
<tr>
<td>• When server communication fails</td>
<td></td>
</tr>
<tr>
<td>• Virtual Private Network (VPN)</td>
<td></td>
</tr>
</tbody>
</table>
Introducing Remote Filtering Software

System requirements

Remote Filtering Client can be installed on the following supported Microsoft Windows operating systems.

**Hardware Recommendations**
- Pentium 4 1.8 GHz
- Free disk space: 25 MB for installation; 15 MB to run the application
- 512 MB RAM

**Operating System Requirements**
- Windows 7 (x86 and x64)
- Windows XP SP2 and above (x86 and x64)
- Windows Vista SP1 and above (x86 and x64)
- Windows Server 2003 SP2 and R2 SP2 and above (x86 and x64)
- Windows Server 2008 SP1 and above (x86 and x64)
- Windows Server 2008 R2 (x64)

Remote Filtering Server is supported on the following operating systems:
- Red Hat Enterprise Linux 4 and 5
- Windows Server 2003 and 2003 R2
- Windows Server 2008 and 2008 R2

Related topics:
- Deployment information
- How remote filtering works
Deployment information

When you install remote filtering software, 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 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 Server instances. Configure each of these Remote Filtering Server instances 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 software deployment, including port assignments. This example does not show all Websense components.
See the *Deployment Guide* for overall Websense Web Security deployment planning information.

**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

Related topics:
- *Deployment information*
- *Differences between remote and local filtering*
- *When server communication fails*
- *Virtual Private Network (VPN)*

Websense Remote Filtering Client resides on client machines that are sometimes or always used outside your organization’s network. When a user makes a browser-based Internet request, Remote Filtering Client uses a heartbeat to determine whether it is...
within or outside the network. If the machine is outside the network, the request is forwarded to Remote Filtering Server.

You can configure how often Remote Filtering Client sends the heartbeat to see whether it is inside the network. See *Configuring the Remote Filtering Client heartbeat interval*, page 29.

**When the client is outside your network**

When a computer is started outside the network, Remote Filtering Client attempts to send a heartbeat to Remote Filtering Server, but the heartbeat port is blocked at the external firewall.

1. 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.
2. Remote Filtering Server then forwards the request to Filtering Service inside the network.
3. Filtering Service evaluates the request and sends a response to Remote Filtering Server.
4. Remote Filtering Server sends the response to the client.
5. 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.
Introducing Remote Filtering Software

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 global remote filtering settings, page 28.

When the client is inside your 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.

![Diagram showing the heartbeat process between the client and server](image)

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, Content Gateway, or an integrated proxy, cache, or firewall (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.
Introducing Remote Filtering Software

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.

---

Differences between remote and local filtering

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 or HTTPS 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 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.

You can configure what action Remote Filtering Client takes if it cannot contact Remote Filtering Server.

- By default, Remote Filtering Client **permits** all HTTP, HTTPS, and FTP requests (fails open).

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

---

Related topics:
- Deployment information
- How remote filtering works
Introducing Remote Filtering Software

- When Remote Filtering Client is configured **block** all requests when it cannot communicate with Remote Filtering Server (fail closed), users are not able to access the Internet until a successful connection to Remote Filtering Server has been established.

  In cases where users must pay for Internet access, such as in hotels or coffee shops, Remote Filtering Client detects and permits connection to the payment portal. As soon as Internet access has been paid for, Remote Filtering Client starts filtering requests.

  In earlier versions, users were given unfiltered Internet access for a limited timeout period, while Remote Filtering Client attempted to make a connection.

When Remote Filtering Server cannot communicate with Filtering Service, the server stops communicating with Remote Filtering Client. When this occurs, the client fails open or closed, as configured.

To change whether Remote Filtering Client blocks or permits all requests when it cannot communicate with Remote Filtering Server, see *Configuring global remote filtering settings*, page 28.

**Virtual Private Network (VPN)**

Websense Remote Filtering supports VPN connections, including split-tunneled VPN.

Remote Filtering Client filters all requests that go through a network adapter that is not connected to the internal network. The client identifies whether the adapter is connected to the internal network via its heartbeat.

Websense software has tested split-tunneling for the following VPN clients:

- Cisco Anyconnect 2.5 and 3.0
- Juniper/Netscreen
- Microsoft PPTP
You must have a functioning Websense Web Security deployment before installing any remote filtering components. See the Installation Guide for instructions on installing and configuring your Websense software.

- For remote filtering system requirements, see System requirements, page 6.
- For deployment instructions, see Deployment information, page 7.
- To get ready to install, see Preparing for installation, page 13.

### 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>55825</td>
<td>Enables communication from Policy Server to Remote Filtering Server during installation. Can be closed after installation is complete.</td>
</tr>
<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>
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>80 (or 8080)</td>
<td><strong>Open</strong> 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><strong>Close</strong> 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>

When your environment is prepared, continue with the appropriate topic:

- **Installing remote filtering components on Windows**
- **Installing remote filtering components on Linux**

## Installing remote filtering components on Windows

Make sure the installation machine meets the Remote Filtering Server hardware and software requirements, and then install the component as follows. If you plan to use additional Remote Filtering Server instances for failover purposes, perform this procedure for each Windows installation.

### Part I: Preparing to install

1. Make sure that Policy Broker, Policy Server, and Filtering Service are installed and running in the network.
2. Log on to the Remote Filtering Server installation machine with **domain** and **local** administrator privileges
   
   Close all applications and stop any anti-virus software on the machine.
3. Download the TRITON Unified Security Setup package:
   a. Log on to [MyWebsense.com](https://www.MyWebsense.com), and then go to the Downloads page. If you do not have an account, follow the instructions on the page to create one.
   b. Identify your product, and then download the setup program.
4. Double-click the downloaded file. If prompted, click Run to start the extraction program. The installation program starts automatically.

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

Part II: Selecting components

1. When the Welcome screen appears, click Start, then accept the subscription agreement and click Next.

2. On the Installation Type screen, select Custom, and then click Next, then click Next again on the Summary screen.

   The Summary screen will be blank, because you have not yet selected which components to install.

3. On the Custom Installation screen, click the Install link next to Web Security.


   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.

Part III: Defining the Remote Filtering Server initial configuration

These steps are only necessary if you are installing Remote Filtering Server. If you are installing only the Remote Filtering Client Pack, skip to Part IV: Completing the installation, page 17.

1. 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.

2. Enter the Policy Server IP address and Port (55806, by default).

   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.
3. 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 fully qualified domain name</td>
<td>IP address or fully qualified domain name visible from <em>outside</em> the network firewall. IMPORTANT: Remember which format you use for this address. You must use the same external address in the same address format—IP address or fully qualified domain name (FQDN)—when you install Remote Filtering Client.</td>
</tr>
<tr>
<td>External port</td>
<td>Port number (from 10 to 65535) that is not in use, and that is accessible from <em>outside</em> 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.) IMPORTANT: 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 Configuring component communication, page 27, for more information.</td>
</tr>
<tr>
<td>Internal port</td>
<td>Port number (from 1024 to 65535) that is not in use, and that is accessible only from <em>inside</em> the network firewall. The default value is 8800. This is the port over which heartbeats are sent. IMPORTANT: Be sure that your network firewall is configured to block connections to the Internal Communication Port from computers located outside the firewall. See Configuring component communication, page 27, for more information.</td>
</tr>
</tbody>
</table>

4. 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.
5. Enter and confirm your pass phrase, and then click Next.
6. 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>Internal IP address</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 IP address</td>
<td>Enter the translated (external) Filtering Service IP address only if the check box is marked.</td>
</tr>
<tr>
<td>Filtering port</td>
<td>Port Filtering Service uses for communication with other Websense services.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server. See Configuring component communication, page 27, for more information.</td>
</tr>
<tr>
<td>Block page port</td>
<td>Port Filtering Service uses to send block pages to client machines.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server. See Configuring component communication, page 27, for more information.</td>
</tr>
</tbody>
</table>

**Part IV: Completing the installation**

1. Accept the default installation path, or click **Browse** to locate another installation folder. Then, click **Next**.
2. 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**.
3. Review the installation summary, and then click **Next** to start the installation.
4. Click **Next** to exit the installer.
5. Restart any antivirus or other software that was stopped for the installation.
Installing remote filtering software

6. Install the Remote Filtering Client on computers to be filtered when outside the network. See Deploying Remote Filtering Client, page 22.

**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 TRITON - Web Security Help.

---

Installing remote filtering components on Linux

Make sure the installation machine meets the Remote Filtering Server hardware and software requirements, and then install the component as follows. If you plan to use additional Remote Filtering Server instances for failover purposes, perform this procedure for each Linux installation.

Note that you must install the Remote Filtering Client Pack on a Windows machine.

**Part I: Preparing to install**

1. Make sure that Policy Broker, Policy Server, and Filtering Service are installed and running in the network.
2. Log on to the Remote Filtering Server installation machine with root privileges.
3. Create a setup directory for the installer files:
   For example: `/root/Websense_setup`
4. Close all applications and stop any anti-virus software.
5. Download the Websense Web Security installer (Linux):
   a. Log on to MyWebsense.com, and then go to the Downloads page. If you do not have an account, follow the instructions on the page to create one.
   b. Identify your product, and then download the installer package to the installation machine.
6. Extract the installation program and launch the installer:
   a. In the setup directory, enter the following command to unzip the file:
      ```
gunzip <download_file_name>
```
      For example: `gunzip Websense76Setup_Lnx.tar.gz`
   b. Expand the file into its components with the following command:
      ```
tar xvf <unzipped_file_name>
```
      For example: `tar xvf Websense76Setup_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 to launch the installer.
   - Text-based install:
     ```bash
     ./install.sh
     ```
   - GUI-based install:
     ```bash
     ./install.sh -g
     ```

---

**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.

---

**Part II: Installing Remote Filtering Server.**

1. Follow the instructions to initiate the installer and accept the Websense Subscription Agreement.
2. Select **Remote Filtering Server** as the component to install, and then confirm your selection, if prompted.
3. 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.
4. 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.
5. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| External IP address or fully qualified domain name | 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 format you use for this address. You must use the same external address in the same address format—IP address or fully qualified domain name (FQDN)—when you install Remote Filtering Client. |
| External port | 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.)  
**IMPORTANT**: 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. |
| Internal port | 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.  
**IMPORTANT**: Be sure that your network firewall is configured to block connections to the Internal Communication Port from computers located outside the firewall. |

6. When asked for a **pass phrase**, consider the following information, and then enter and confirm the pass phrase.

- 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.
7. When asked for Filtering Service information, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal IP address</td>
<td>IP address of the machine running Filtering Service.</td>
</tr>
<tr>
<td>A firewall or other network device...</td>
<td>Indicate whether a firewall or other network device performs network address translation between the Filtering Service machine and the Remote Filtering Server machine.</td>
</tr>
<tr>
<td>Translated IP address</td>
<td>Enter the translated Filtering Service IP address only if network address translation occurs between the Filtering Service and Remote Filtering Server machines.</td>
</tr>
<tr>
<td>Filtering port</td>
<td>Port Filtering Service uses for communication with other Websense services.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server.</td>
</tr>
<tr>
<td>Block page port</td>
<td>Port Filtering Service uses to send block pages to client machines.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong>: Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server.</td>
</tr>
</tbody>
</table>

**Part III: Completing the installation**

1. Accept the default installation path, or enter a new path.
2. 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.
   - If the installation machine has less than the recommended amount of memory, a warning is displayed, but the installation can continue.
   Review the installation summary, and then start the installation.
3. When installation is complete, exit the installer.
4. Restart any antivirus or other software that was stopped for the installation.

**Part IV: Next steps**

In order to start using your remote filtering software, you must also:

- Install the Remote Filtering Client Pack on a Windows machine.
- Create one or more client profiles.
- Install Remote Filtering Client on computers to be filtered when outside the network.
Installing remote filtering software

See Deploying Remote Filtering Client, page 22.

**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 TRITON - Web Security Help.

---

**Deploying Remote Filtering Client**

Remote Filtering Client must be deployed to all Windows client machines that are used outside the network firewall.

The Remote Filtering Client Pack includes an installation program (**setup.exe**) and several supporting files, as well as a client configuration tool:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0409.ini</td>
<td>Support file containing Remote Filtering Client installation messages</td>
</tr>
<tr>
<td>RF.cab</td>
<td>Cabinet file containing files needed for installation</td>
</tr>
<tr>
<td>RFCClientConfig.hsw</td>
<td>Configuration file</td>
</tr>
<tr>
<td>setup.exe</td>
<td>The program used to install and uninstall Remote Filtering Client on end user machines.</td>
</tr>
<tr>
<td>Setup.ini</td>
<td>Support file containing installer configuration information</td>
</tr>
<tr>
<td>Websense Endpoint.msi</td>
<td>Windows installer file for Remote Filtering Client.</td>
</tr>
<tr>
<td>WEP.cab</td>
<td>Cabinet file containing files needed for installation</td>
</tr>
<tr>
<td>WRFEUtil_platform_version.exe</td>
<td>Self-extracting executable file containing the Remote Filtering Client Configuration tool and its supporting files.</td>
</tr>
<tr>
<td></td>
<td>The <em>platform</em> section of the file name indicates whether the tool is used to create installation packages for 32-bit or 64-bit clients.</td>
</tr>
<tr>
<td></td>
<td><em>Version</em> is 3 or 4-digit number.</td>
</tr>
<tr>
<td></td>
<td>See Customizing the client installation package, page 23.</td>
</tr>
</tbody>
</table>

By default, the client pack files are installed in the 32-bit and 64-bit subfolders under:

```
Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\
```
Before deploying Remote Filtering Client to end user machines, use the Remote Filtering Client Configuration tool to create one or more profiles, used to configure remote filtering behavior. Each profile is saved as part of a separate Remote Filtering Client installation package. See *Customizing the client installation package*, page 23.

Once you have created one or more profiles and its accompanying installation package:

- If you plan to install the client manually, copy the installation package to any directory on individual computers (see *Installing manually*, page 25).
- If you plan to automatically deploy the client via third-party tools, copy the installation package to the appropriate directory on a network server (see *Installing with a third-party deployment tool*, page 25)

Remote Filtering Client can be installed only on Windows machines.

---

**Warning**

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

---

**Customizing the client installation package**

Before deploying Remote Filtering Client to users’ machines, create one or more configuration profiles to specify how the client connects to one or more Remote Filtering Server instances, whether filtering activity is logged for the client, and so on.

Each profile is saved as part of a complete Remote Filtering Client installation package.

You must create at least one profile (customized installation package) to successfully deploy Remote Filtering Client, and can create multiple profiles (both 32 and 64-bit) as required by your network environment.

**Extract the configuration tool**

1. Navigate to the 32-bit or 64-bit subdirectory of the Remote Filtering Client Pack installation directory (by default, `\Program Files\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack`).

2. Double-click the `WRFEUtil_platform_version.exe` self-extracting executable and specify a path for the configuration tool files.

   As a best practice, install the tool in its own folder.

**Configure an installation profile**

1. Navigate to the folder containing the configuration tool and double-click `RFClient_Config.exe`.

2. Browse to the location of the existing Remote Filtering Client installation package (see step 1 for the default path), and then click **Next**.
After creating a profile, you can choose where to save your customized installation package.

3. On the Internal Connections screen, enter the internal **IP address or name** and internal **Port** of each Remote Filtering Server to which this client will connect. Use the > button to move the information to the selected list. When you are finished, click **Next**.

Remote Filtering Client sends its heartbeat to these IP addresses and ports to determine whether or not it is inside the network.

If you have multiple Remote Filtering Server instances, Remote Filtering Client rotates through the list in order until a functioning server is located.

Remote Filtering Server has a 2-minute inactivity timeout period. If the client connects, and then does not send an Internet request in the timeout period, the server drops the connection. When the next request is made, Remote Filtering Client goes through its list to connect again. This protects server performance by reducing the number of unused connections that might otherwise accumulate.

4. On the External Connections screen, enter the external **IP address or name** and **Port** of each Remote Filtering Server listed on the previous screen. Use the > button to move the information to the selected list.

Each server must be identified by an externally visible IP address or fully qualified domain name (FQDN).

---

**Important**

Be sure to use the **same format** (IP address or FQDN) that you used when installing Remote Filtering Server.

When Remote Filtering Client is outside the network, filtering requests are sent to Remote Filtering Server via the specified IP address or FQDN and port.

5. Indicate whether or not to **Log user Internet activity** seen by Remote Filtering Client instances installed using this customized installation package, and then click **Next**.

6. Use the **Close feedback message...** field to indicate how long (in seconds) to display a pop-up notification when remote filtering software blocks FTP or HTTPS traffic. If you do not want the user to see a pop-up notification, mark the **Do not notify end user...** check box.

7. Indicate whether or not to **Enable tamper protection**. This helps prevent Remote Filtering Client files from being renamed or deleted.

8. Enter and confirm an **Administrator password** used for communication with Remote Filtering Server. This must match the pass phrase created when Remote Filtering Server was installed.

When you are finished, click **Next**.

9. Indicate whether to **Save customized installation package to a new location** (recommended) or **Overwrite the existing installation package**.
Installing remote filtering software

If selecting a new location, indicate where the installation package will be saved.

10. Click Finish.

The new installation package can now be used to deploy Remote Filtering Client to users’ machines.

Installing manually

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

1. Make sure that Remote Filtering Server has been correctly installed. See Installing remote filtering components on Windows, page 14.

2. Use the Remote Filtering Client Configuration tool to create one or more client profiles. Each profile is associated with a separate installation package. See Customizing the client installation package, page 23.

3. Copy all of the files from a configured installation package to a temporary folder on the client machine.
   - If you chose to overwrite the default client pack files when you created your custom installation package, note that you should not copy the configuration tool file (WRFEUtil_platform_version.exe) to the client machine.
   - If you use the default installation package without configuring a profile, the client will not be able to connect to Remote Filtering Server.


5. When the installer finishes launching, click Next.

6. Accept the subscription agreement, and then click Next.

7. Review and accept or change the installation path, and then click Next.

8. Review the summary screen, and then click Install.

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

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 on Windows, page 14.

Locate a customized Remote Filtering Client installation package (see Customizing the client installation package, page 23).
Installing remote filtering software

To deploy the Remote Filtering Client to Windows computers, use the custom installation package files 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.

Uninstalling Remote Filtering Client

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 {<product_code>} XPSWDRF=<password> /qn
```

- **product_code** is a unique identifier (GUID) that can be found in the setup.ini file of each installation package.
- **password** is the administrator password that you entered when creating the installation package.

To uninstall Remote Filtering Client manually:

1. Go to Start > Control Panel > **Add/Remove Programs** on the client machine.
2. Select **Websense Endpoint**, and then click **Remove**.
Setting up remote filtering software

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

- Configuring component communication, page 27.
- Configuring global remote filtering settings, page 28.
- (optional) Configuring remote filtering to ignore HTTPS or FTP, page 29.

Configuring 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.

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.

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 filtering port (default 15868) to accept connections from the Remote Filtering Server.
- 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 TRITON - Web Security.

See the documentation for your firewall product for configuration instructions.
Configuring global remote filtering settings

Use the Settings > General > Remote Filtering page in TRITON - Web Security to configure options that affect all Remote Filtering Clients associated with this installation.

1. Mark the Block all requests... check box to block off-site users from all Internet access unless their computer is communicating with Remote Filtering Server (fail closed).
   By default, users have unfiltered access to the Internet when their computers cannot communicate with the Remote Filtering Server (fail open).

2. If you have any v7.5 Remote Filtering Client instances deployed, and marked the “Block all requests” option, use the Timeout interval field to select a number of minutes up to 60 (default 15).
   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).

   **Warning**
   Choosing at timeout value of 0 may lock out a remote computer before the user can establish Internet connection from a hotel or other pay-for-use-provider.
   Websense, Inc., does not recommend choosing 0 or setting the timeout period to another low number.

3. Select a Maximum size for log file (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.

4. Click OK to cache your changes. Changes are not saved until you click Save All.
Configuring remote filtering to ignore HTTPS or FTP

You can configure remote filtering software to ignore FTP traffic, HTTPS traffic, or both. HTTP traffic is always monitored.

If you have multiple Remote Filtering Servers, repeat these steps for each instance.

1. Navigate to the Websense bin directory (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin, by default) on the Remote Filtering Server machine.
2. Open the securewispproxy.ini file in a text editor.
3. To disable FTP filtering for this Remote Filtering Server instance, add the following line to the file:
   
   FilterFTP=0

   If you want to later turn FTP filtering back on, change the parameter value from “0” to “1”.
4. To disable HTTPS filtering for this Remote Filtering Server instance, add the following line to the file:
   
   FilterHTTPS=0

   If you want to later turn HTTPS filtering back on, change the parameter value from “0” to “1”.
5. Save and close the file.
6. Restart the Remote Filtering Server service or daemon.

Configuring the Remote Filtering Client heartbeat interval

In order to determine whether it is inside or outside of the network, Remote Filtering Client sends a heartbeat to Remote Filtering Server. If the heartbeat connection succeeds, Remote Filtering Client knows that it is inside the network. By default, Remote Filtering Client continues to send the heartbeat every 15 minutes to ensure that its status has not changed.

If you would prefer that Remote Filtering Client send the heartbeat less frequently once it has determined that it is inside the network, you can increase the heartbeat interval. In this case, Remote Filtering Client will only send a more frequent heartbeat if it registers a change in network.

To change the heartbeat interval:

1. Navigate to the Websense bin directory (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/) on the Remote Filtering Server machine.
2. Open the securewispproxy.ini file in a text editor.
3. Find the HeartbeatRetryInterval parameter and change its value. For example:
HeartbeatRetryInterval=360

In this example, the heartbeat will be sent every 360 minutes, or 6 hours.

- The value can be any number of minutes between 0 and 1440 (24 hours).
- The default is 15 minutes.

4. Save and close the file.

5. Restart the Remote Filtering Server service or daemon.
Upgrading remote filtering software

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 on Windows, page 14, for details.

This guide provides instructions for:
- Preparing to upgrade Remote Filtering Server
- Upgrading Remote Filtering Server
- Upgrading Remote Filtering Client

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 global remote filtering settings, page 28, for details.
If you employ secondary and tertiary Remote Filtering Servers, they should be configured to communicate with the same Filtering Service as the primary Remote Filtering Server. If they communicate with different Filtering Services, failover filtering occurs during the upgrade, but quota and continue time may not operate as expected.

### 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 *Part I: Preparing to install*, 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 TRITON - Web Security.
6. Go to the **Settings > General > 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**.

### Upgrading Remote Filtering Client

You can upgrade v7.5 Remote Filtering Client instances in your network with either of the following methods:

- **Manual upgrade**: Use a customized v7.6 Remote Filtering Client installation package on each client machine to upgrade the Remote Filtering Client. See *Upgrading Remote Filtering Client manually*, page 33.
- **Automatic upgrade with third-party tool**: Use a customized v7.6 Remote Filtering Client installation package with a third-party deployment tool to upgrade the Remote Filtering Client on client computers. See *Upgrading Remote Filtering Client with a third-party deployment tool*, page 33.
To create a custom installation package, see *Customizing the client installation package, page 23.*

### Upgrading Remote Filtering Client manually

To manually upgrade the Remote Filtering Client on a Windows machine:

1. Create a custom installation package as described in *Customizing the client installation package, page 23.*
2. Run `setup.exe` as described in *Installing manually, page 25.*

The Remote Filtering Client installer detects the existence of a previous version and performs the upgrade automatically.

After upgrading the Remote Filtering Client on remote computers, configure Remote Filtering settings in TRITON - Web Security.

1. Click **Settings > General > Remote Filtering**.
2. Review and update the settings on this page, as needed.
3. Click **OK** to cache your changes.
4. Click **Main > Policy Management > Filters**.
5. Review and update category filters, as needed, to account for the fact that remote clients are filtered for HTTPS and FTP, as well as HTTP sites, by default.
   
   If you do not want remote filtering software to filter HTTPS requests, FTP requests, or both, see *Configuring remote filtering to ignore HTTPS or FTP, page 29,* for instructions on disabling this functionality.
6. Click **OK** to cache any changes. Changes are not implemented until you click **Save All**.

### Upgrading Remote Filtering Client with a third-party deployment tool

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

To create the installation package, see *Customizing the client installation package, page 23.*

After upgrading the Remote Filtering Client on remote computers:

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.

   If you do not want remote filtering software to filter HTTPS requests, FTP requests, or both, see Configuring remote filtering to ignore HTTPS or FTP, page 29, for instructions on disabling this functionality.

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

Use the sections that follow to diagnose and address remote filtering software issues:

- Block pages are not being displayed, page 35
- When client machines use a proxy server, page 35
- General troubleshooting procedures, page 36

Block pages are not being displayed

If Remote Filtering Clients are being filtered correctly, but are not receiving Websense block pages, make sure that:

- The firewall between the Filtering Service machine and the Remote Filtering Server machine is properly configured, as described in Configuring component communication, 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.


- Any client machines configured to send requests through a proxy server have been configured to communicate with the Remote Filtering Server machine directly. See When client machines use a proxy server, page 35.

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 fully qualified domain name (use the exact value entered when you installed Remote Filtering Client) to the list of addresses for which no proxy should be used.

**General troubleshooting procedures**

1. Verify that your subscription key includes remote filtering.
2. Make sure that Remote Filtering Server is running.
   - Windows: Use the Windows Services dialog box to verify that Websense Remote Filtering Server is running.
   - Linux:
     a. Go to the `/opt/Websense` directory and enter the following command:
        
        ```
        ./WebsenseAdmin status
        ```
     b. Remote Filtering Server 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 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 *Configuring component communication*, page 27.
   - Make sure the Filtering Service’s **filtering 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 Configuring component communication, page 27.

- The Remote Filtering Server’s external communication port on these firewalls must be able to accept connections from Remote Filtering Clients on machines 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 machines 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, and that it is not monitoring the machine on which Remote Filtering Server is installed.

See the Network Agent Quick Start for more information about configuring Network Agent 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.

  To solve this problem, 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 2 is not installed.

  To solve this problem, 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 on Windows, page 14, 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:
     ```
     ./WebsenseAdmin stop
     ```

b. Open the securewispproxy.ini file.

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

d. Save and close the securewispproxy.ini file.

e. Start the Remote Filtering Server.
   - **Windows**: Use the Windows Services dialog box.
   - **Linux**: Enter the following command:
     ```
     ./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.