



# Deploying the Remote Filter Module

Forcepoint™ Web Filter & Security

v8.2.x, v8.3.x

©1996–2016, Forcepoint LLC  
All rights reserved.  
10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA  
Published 2016

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

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

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

### **Trademarks**

Forcepoint is a trademark of Forcepoint LLC. SureView, ThreatSeeker, TRITON, Sidewinder, and Stonesoft are registered trademarks of Forcepoint LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks are the property of their respective owners.

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

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).  
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

# Contents

<b>Topic 1</b>	<b>Introducing Remote Filtering</b> . . . . .	<b>5</b>
	System requirements . . . . .	6
	Deployment information . . . . .	6
	How remote filtering works . . . . .	8
	When server communication fails . . . . .	11
<b>Topic 2</b>	<b>Installing Remote Filtering Components</b> . . . . .	<b>13</b>
	Preparing for installation . . . . .	13
	Installing Remote Filtering Server on Windows . . . . .	14
	Installing Remote Filtering Server on Linux . . . . .	18
	Deploying Remote Filtering Client . . . . .	22
	Customizing the client installation package . . . . .	23
	Installing Remote Filtering Client manually . . . . .	25
	Using a third-party deployment tool for Windows . . . . .	26
	Uninstalling Remote Filtering Client . . . . .	27
<b>Topic 3</b>	<b>Configuring Remote Filtering Software</b> . . . . .	<b>29</b>
	Configuring remote filtering to ignore HTTPS or FTP . . . . .	30
	Configuring the Remote Filtering Client heartbeat interval . . . . .	31
<b>Topic 4</b>	<b>Upgrading Remote Filtering Components</b> . . . . .	<b>33</b>
	Upgrading Remote Filtering Server . . . . .	33
	Upgrading Remote Filtering Client . . . . .	34
	Upgrading Remote Filtering Client manually . . . . .	34
	Upgrading Remote Filtering Client with a third-party deployment tool . . . . .	35
<b>Appendix A</b>	<b>Troubleshooting remote filtering software</b> . . . . .	<b>37</b>
	Block pages are not being displayed . . . . .	37
	Reporting tools don't include remote filtering data . . . . .	38
	When client machines use a proxy server . . . . .	38
	General troubleshooting procedures . . . . .	38



# 1

## Introducing Remote Filtering

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Web Filter & Security customers who want to manage Internet requests made from outside their organization's network can optionally purchase the Remote Filter module. This allows administrators to deploy and configure remote filtering software:

- **Remote Filtering Client** is installed on each machine that will receive policy enforcement when it is outside the network.
- **Remote Filtering Server** resides inside your firewall, and acts as a proxy to Filtering Service.

All communication between remote filtering components is authenticated and encrypted.

This guide includes the following planning, installation, upgrade, configuration, and troubleshooting information for remote filtering software:

Planning	Installation
<ul style="list-style-type: none"><li>● <a href="#">System requirements</a></li><li>● <a href="#">Deployment information.</a></li><li>● <a href="#">How remote filtering works</a></li><li>● <a href="#">Differences between remote and local management of HTTPS and FTP traffic</a></li><li>● <a href="#">When server communication fails</a></li></ul>	<ul style="list-style-type: none"><li>● <a href="#">Preparing for installation</a></li><li>● <a href="#">Installing Remote Filtering Server on Windows</a></li><li>● <a href="#">Installing Remote Filtering Server on Linux</a></li><li>● <a href="#">Deploying Remote Filtering Client</a></li></ul>
Initial Setup	Upgrade
<ul style="list-style-type: none"><li>● <a href="#">Configuring Remote Filtering Software, page 29</a></li><li>● <a href="#">Configuring remote filtering to ignore HTTPS or FTP</a></li><li>● <a href="#">Configuring the Remote Filtering Client heartbeat interval</a></li></ul>	<ul style="list-style-type: none"><li>● <a href="#">Upgrading Remote Filtering Components</a></li><li>● <a href="#">Upgrading Remote Filtering Server</a></li><li>● <a href="#">Upgrading Remote Filtering Client</a></li></ul>
Troubleshooting	
<ul style="list-style-type: none"><li>● <a href="#">Block pages are not being displayed</a></li><li>● <a href="#">When client machines use a proxy server</a></li><li>● <a href="#">General troubleshooting procedures</a></li></ul>	

## System requirements

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Related topics:

- [Deployment information](#)
- [How remote filtering works](#)

Remote Filtering Client is supported on the following operating systems:

- Windows 10 (x64)
- Windows 8 (x64)
- 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)
- Windows Server 2012 (x64)
- Mac OS X 10.8 and later

Remote Filtering Server is supported on the following operating systems:

- Red Hat Enterprise Linux 6.x
- Windows Server 2008 R2 or R2 SP1 and Windows Server 2012 or 2012 R2

## Deployment information

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Related topics:

- [System requirements](#)
- [How remote filtering works](#)

When you install remote filtering components, 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 Filtering Service and with the remote machines outside the network firewall. The Remote Filtering Server machine need not be joined to a domain.

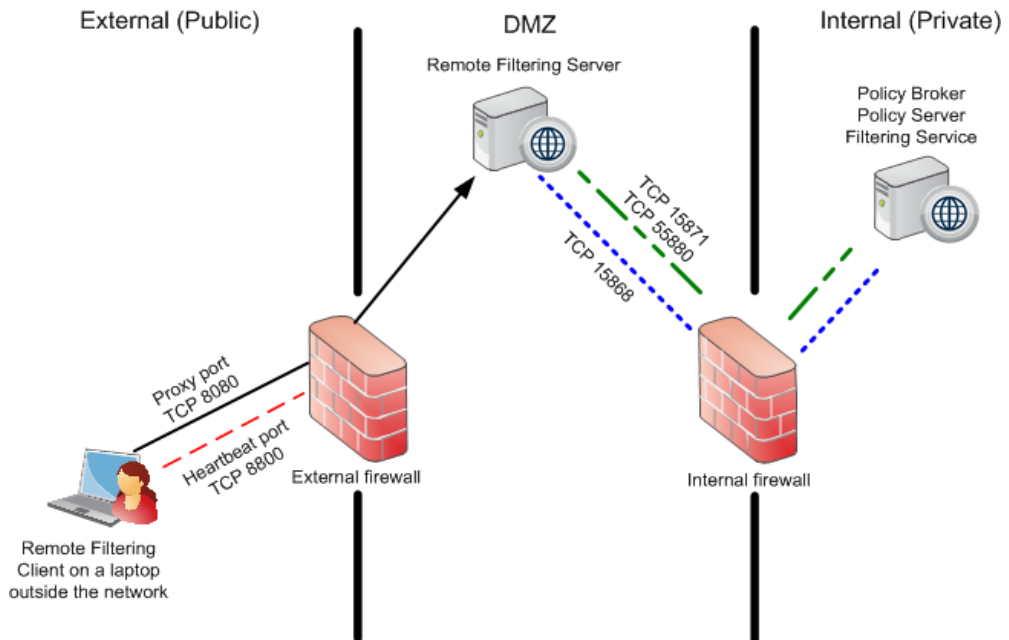
- Do not install Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Make sure that Network Agent or your third-party integration product is configured to **ignore** (not filter) requests going to or from the Remote Filtering Server machine.
- Make sure that Network Agent is **not** configured to “Log HTTP requests” (configured on the **Settings > Network Agent > Local Settings > NIC Settings** page in the Web module of the TRITON Manager).
- Install only one primary Remote Filtering Server for each Filtering Service in your network.
  - To provide a failover option 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.

Remote filtering software supports VPN connections, including split-tunneled VPN.

- Remote Filtering Client manages all requests that go through a network adapter that is not connected to the internal network.
- Your web protection software has tested split-tunneling for the following VPN clients: Cisco Anyconnect 2.5 and 3.0, Juniper/Netscreen, Microsoft PPTP.

The following diagram provides a rough sketch of a typical remote filtering software deployment, including port assignments (does not show all web protection

components). See the *Deployment and Installation Center* for your version ([v8.2.x](#) or [v8.3.x](#)) for comprehensive deployment information for all TRITON solutions.



**Important**

The heartbeat port, 8800, must be blocked at the external firewall.

## How remote filtering works

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Related topics:

- [Deployment information](#)
- [Differences between remote and local management of HTTPS and FTP traffic](#)
- [Identifying remote users](#)
- [When server communication fails](#)

Forcepoint Remote Filtering Client resides on client machines that are 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.

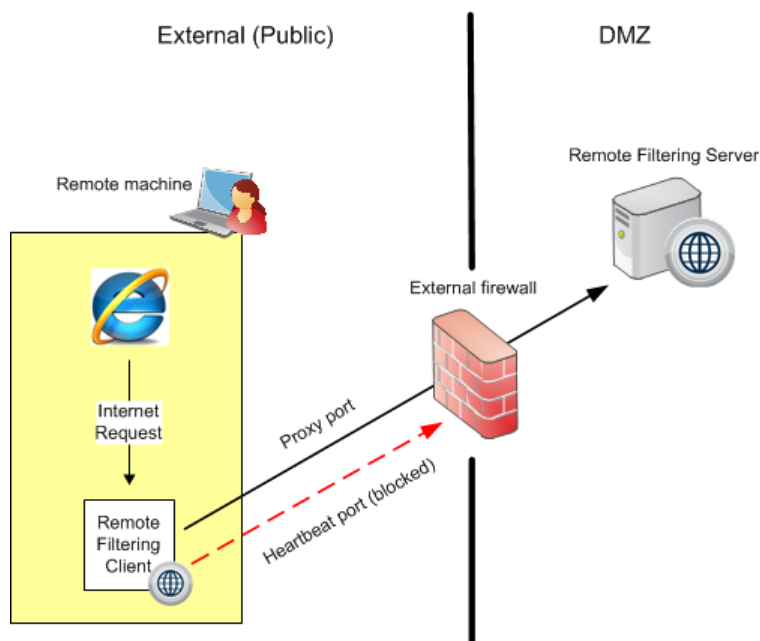


You can configure how often Remote Filtering Client sends the heartbeat to see whether it is inside the network. See [Configuring the Remote Filtering Client heartbeat interval](#), page 31.

## 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.

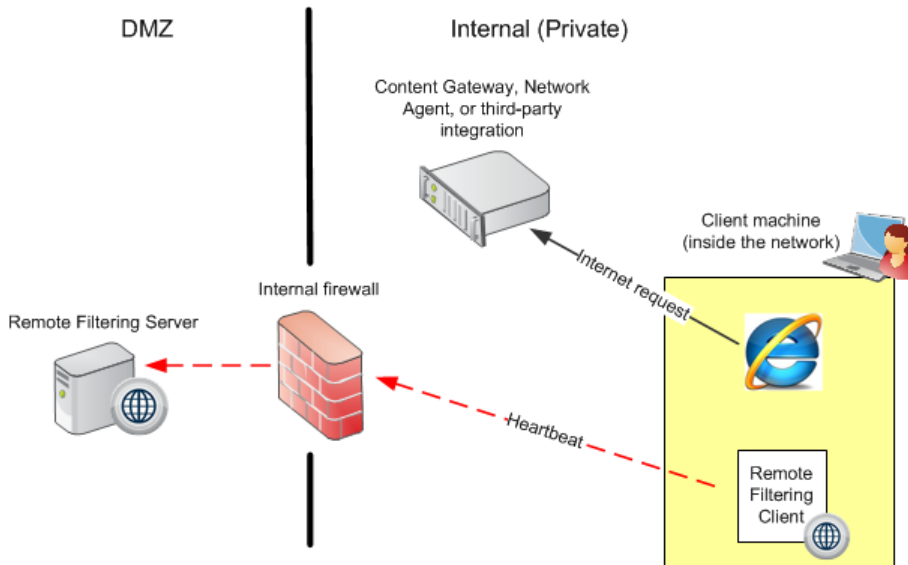


Remote Filtering Client delays each request until it receives a response from Remote Filtering Server. Depending on the response received, Remote Filtering Client either permits the site or displays the block page.

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 [Global remote filtering settings](#), page 30.

## When the client is inside your network

When the client 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.



Remote Filtering Client does not query Remote Filtering Server about Internet requests. Instead, requests are passed directly from the browser to Network Agent, or an integrated proxy, cache, or firewall and managed like any other request.

## Identifying remote users

The policy applied to requests from a remote machine depends on how the user logs on to the machine.

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

If the user logs on with a local account, Filtering Service cannot resolve the user name.

- If manual authentication **is** enabled, the user receives an in-browser logon prompt, and Internet requests are managed according to the user or group policy and Internet activity is logged under the network user name.
- If manual authentication is **not** enabled, the Default policy is applied to Internet requests and Internet activity is logged under the local user name.



### Note

Selective authentication settings do not apply to remote filtering users.

## Differences between remote and local management of HTTPS and FTP traffic

When a remote user requests an HTTP site in a category that is set to the Quota or Confirm action, remote filtering software 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 software does not support the Quota and Confirm actions for these protocols.

## When server communication fails

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Related topics:

- [Deployment information](#)
- [How remote filtering works](#)

Policy enforcement 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.

- When Remote Filtering Client is configured to **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 managing requests.

In earlier versions, users were given open 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 [Global remote filtering settings](#), page 30.

# 2

## Installing Remote Filtering Components

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Installation of remote filtering software components requires a functioning Forcepoint Web Filter & Security deployment. You must also purchase the Remote Filter module to enable remote filtering.

- For remote filtering system requirements, see [System requirements](#), page 6.
- For general deployment guidelines, see [Deployment information](#), page 6.
- To get ready to install, see [Preparing for installation](#), page 13.

### Preparing for installation

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Before installing remote filtering components, configure the firewall between the machine intended for Remote Filtering Server and the Policy Broker, Policy Server, and Filtering Service machine or machines to permit communication over the following ports.

Some of these ports must be open for installation, but can be closed afterward, as noted. Others must stay open for remote filtering to function properly.

Port	Description
55880	Enables communication from Remote Filtering Server to Policy Broker.
55806 40000	Enable communication from Remote Filtering Server to Policy Server during installation. Can be closed after installation is complete.
55825	Enables communication from Policy Server to Remote Filtering Server during installation. Can be closed after installation is complete.

Port	Description
15868	Filtering Service Port. Enables communication between Filtering Service and Remote Filtering Server.
15871	Block Page Port. Enables Filtering Service to send block messages to users. If this port is not open, requests are still blocked, but users do not receive a block message.

Most organizations also have a firewall between Remote Filtering Server and Remote Filtering Clients outside the network. This firewall must be configured as follows to enable remote filtering to function properly.

You can configure the external firewall before or after installing Remote Filtering Server and deploying Remote Filtering Clients.

Port	Description
80 (or 8080)	<b>Open</b> this external communication port on the external firewall. This enables Remote Filtering Server to accept requests from Remote Filtering Clients outside the network.
8800	<b>Close</b> access to the internal communication (heartbeat) port on the external firewall.

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

- [Installing Remote Filtering Server on Windows](#)
- [Installing Remote Filtering Server on Linux](#)

## Installing Remote Filtering Server on Windows

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Make sure the installation machine meets the Remote Filtering Server hardware and software requirements, then install the component as follows. If you plan to use additional Remote Filtering Server instances for failover purposes, perform this procedure on each 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 **domain** and **local** administrator privileges.
3. Close all applications and stop any anti-virus software on the machine.

4. If you do not have a local copy of the TRITON Setup package to reuse, download the setup package:
  - a. Log on to the [My Account](#) page at forcepoint.com, and then go to the Downloads tab. If you do not have an account, follow the instructions on the page to create one.
  - b. Identify your product, navigate to the Windows installation package, and then click **download**.
5. 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, 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.
3. On the Custom Installation screen, click the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
4. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
5. Accept the subscription agreement, then click **Next**.
6. 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 web protection components inside the network firewall, and then click **Next**.
7. Select the **Custom** installation type, then click **Next**.
8. On the Select Components screen, select **Remote Filtering Server**.

When Remote Filtering Server is installed on a Windows machine, the Forcepoint Endpoint Package Builder, used to create Remote Filtering Client installation packages, is installed automatically on the same machine.

## Part III: Defining the Remote Filtering Server initial configuration

1. 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.

---

2. 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**.

Field	Description
External IP address or fully qualified domain name	IP address or fully qualified domain name visible from <b>outside</b> the network firewall. <b>IMPORTANT:</b> Remember which format you use for this address. You must use the same external address <b>in the same address format</b> —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 <b>outside</b> 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.) <b>IMPORTANT:</b> The port entered as the <b>External Communication Port</b> 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 <b>inside</b> the network firewall. The default value is 8800. This is the port over which heartbeats are sent. <b>IMPORTANT:</b> Be sure that your network firewall is configured to block connections to the <b>Internal Communication Port</b> from computers located outside the firewall.

3. When asked for a **pass phrase**, consider the following information:
  - The pass phrase can be up to 32 characters in 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. Your web protection software cannot be used to retrieve it later.

4. Enter and confirm your pass phrase, and then click **Next**.



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

Field	Description
Internal IP address	IP address of the machine running Filtering Service.
A firewall or other network device...	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.
Translated IP address	Enter the translated (external) Filtering Service IP address only if the check box is marked.
Filtering port	Port Filtering Service uses for communication with other Forcepoint services. <b>IMPORTANT:</b> Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server.
Block page port	Port Filtering Service uses to send block pages to client machines. <b>IMPORTANT:</b> Be sure this port is open on the firewall that separates Filtering Service and Remote Filtering Server.

## Part IV: Completing the installation

- Accept the default installation path, or click **Browse** to locate another installation folder. Then, click **Next**.
- 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**.
- Review the installation summary, and then click **Next** to start the installation.
- Click **Next** to exit the installer.
- Restart any antivirus or other software that was stopped for the installation.

6. Create one or more Remote Filtering Client installation packages and deploy Remote Filtering Client to the machines you want to filter when outside the network. See [Deploying Remote Filtering Client](#), page 22.



### Important

If Network Agent or an integration product is configured to manage HTTP requests in your network, make sure that it is **not** monitoring requests going to or from the Remote Filtering Server machine.

For information about configuring Network Agent, see the [Network Agent Quick Start](#) paper.

---

## Installing Remote Filtering Server on Linux

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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 the Endpoint Package Builder, used to create Remote Filtering Client installation packages, is a Windows-only tool. The Package Builder can be found on any Windows machine that includes web protection components, such as the TRITON management server or the Log Server 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 web module installer for Linux:
  - a. Log on to the [My Account](#) page at forcepoint.com, and then go to the Downloads tab. If you do not have an account, follow the instructions on the page to create one.
  - b. Identify your product, and then download the Linux installer.
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 Web82xSetup\_Lnx.tar.gz**

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

```
tar xvf <unzipped_file_name>
```

For example: **tar xvf Web82xSetup\_Lnx.tar**

This command places the following files into the setup directory:

File	Description
install.sh	Installation program.
Setup	Archive file containing related installation files and documents.

- c. Launch the installer.

To use the command-line installer, enter:

```
./install.sh
```

To use the graphical installer, enter:

```
./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 Forcepoint Subscription Agreement.
2. 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 web protection components inside the network firewall.
3. Select **Remote Filtering Server** as the component to install, and then confirm your selection, if prompted.
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:

Field	Description
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 <i>outside</i> the network firewall. <b>IMPORTANT:</b> Remember which format you use for this address. You must use the same external address <b>in the same address format</b> —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 <b>outside</b> 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.) <b>IMPORTANT:</b> The port entered as the <b>External Communication Port</b> 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 <b>inside</b> the network firewall. The default value is 8800. This is the port over which heartbeats are sent. <b>IMPORTANT:</b> Be sure that your network firewall is configured to block connections to the <b>Internal Communication Port</b> 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 up to 32 characters long. 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. Your web protection software cannot be used to retrieve it later.

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

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

## Part III: Completing the installation

- Accept the default installation path, or enter a new path.
- 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.
- When installation is complete, exit the installer.
- 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:

- Locate the Endpoint Package Builder on a Windows machine.  
The Package Builder is automatically included when any Web Filter & Security component is installed on a Windows machine. You can copy the client pack files from, for example, the Log Server or TRITON management server machine, then perform client configuration on any Windows machine (server or workstation).
- Create one or more Remote Filtering Client installation packages.
- Install Remote Filtering Client on client machines that reside (or move) outside the network. See [Deploying Remote Filtering Client](#), page 22.

## Deploying Remote Filtering Client

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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

Remote Filtering Client installation packages are created with the Endpoint Package Builder, which can also be used to create and configure installation packages for TRITON AP-ENDPOINT Web and TRITON AP-ENDPOINT DLP.

By default, the Package Builder files are installed in the following directory:

```
Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\
```

Note that not all of the files and directories are used for all clients, so you may see directories for client operating systems that are not currently supported by Remote Filtering Client.

Before deploying Remote Filtering Client to end user machines, use the Endpoint Package Builder tool to create one or more installation packages.

- The installation package is used to both deploy Remote Filtering Client to client machines and to configure Remote Filtering Client behavior.
- You can create multiple installation packages if you need multiple Remote Filtering Client configurations.

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 client machines (see [Installing Remote Filtering Client 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 [Using a third-party deployment tool for Windows, page 26](#)).

Remote Filtering Client can be installed on Windows or Mac OS X client machines.



### Warning

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

---

## Customizing the client installation package

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Before deploying Remote Filtering Client to users' machines, create one or more **installation packages**. An installation package includes configuration information to specify how the client connects to one or more Remote Filtering Server instances, whether Internet activity is logged for the client, and so on.

You must create at least one customized installation package to successfully deploy Remote Filtering Client, and can create multiple installation packages.

To create an installation package:

1. Navigate to the folder containing the configuration tool (by default, Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\) and double-click **EndpointPackage82x.exe**.

The Endpoint Package Builder opens.

2. Mark the **Endpoint web protection** check box, then select **Remote Filtering Client**. Also select a language from the drop-down list at the bottom of the page. This is the language used to display messages to the end user (if any such messages are enabled).

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

3. Select one or more operating systems (**Windows 32-bit**, **Windows 64-bit**, or **Mac OS X**) for which to create an installation package, then enter and confirm the anti-tampering **Password** that administrators may use to modify or uninstall the Remote Filtering Client. Also specify whether or not to **Protect the installation directory from modification or deletion**.

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

4. If you selected one or more Windows operating systems, specify the installation path for Remote Filtering Client on end user machines.
  - Select **Use the default location** to install Remote Filtering Client in the directory displayed in the tool.
  - Select **Use this location** to enter a custom installation path.

If you selected only Mac OS X as your client operating system, this screen is not displayed. On Mac OS X machines, Remote Filtering Client is installed in the Applications directory.

5. On the Internal Connections screen, enter the internal **IP address or hostname** 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.

6. On the External Connections screen, enter the external **IP address or hostname** 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.

7. 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**.
8. Use the **Trusted Sites** list to enter up to 4 URLs, IP addresses, or regular expressions for sites that Remote Filtering Client users can access directly, without being filtered or logged. Click **Add** to enter a URL, IP address, or regular expression.

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

9. Indicate whether or not to **Notify users when HTTPS or FTP traffic is blocked**, then, if notification is enabled, specify how long (in seconds) the message is displayed.
10. Enter and confirm the **Pass phrase** 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**.

11. Specify a **Save location** for the new installation package. Enter a valid directory path or click **Browse** to navigate to the path.
12. Click **Finish**.

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



## Installing Remote Filtering Client manually

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

### Windows

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 Server on Windows, page 14](#).
2. Use the Endpoint Package Builder to create one or more installation packages. See [Customizing the client installation package, page 23](#).
3. Each installation package is a single executable file. The name depends on the operating system you selected during configuration:
  - TRITONAP-ENDPOINT-x32.exe
  - TRITONAP-ENDPOINT-x64.exe
4. Double-click the installation package executable on the client machine.



#### Warning

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

---

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.

### Mac OS X

To install Remote Filtering Client on Mac client machines:

1. Copy the Mac installation package (ZIP file) to the client machine and unzip the package.
2. To start the installation, double-click **WebsenseEndpoint.pkg**.
  - The **RFAdmin.hsw** and **RFClient.hsw** settings files must reside in the same directory as the installer package (pkg) file in order to install Remote Filtering Client.
  - Local administrator permissions are required to install the client software.
3. Follow the onscreen instructions to install Remote Filtering Client.

## Using a third-party deployment tool for Windows

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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 Server on Windows, page 14](#).

1. Locate a customized Remote Filtering Client installation package (see [Customizing the client installation package, page 23](#)).
2. If you are using a tool like GPO and want to deploy a MSI file rather than an EXE file, use a file compression tool like 7-Zip, WinZip, or WinRAR to extract the contents of the installation package.

This exposes the **Websense Endpoint.msi** file and its support files.

3. Use a third-party deployment tool (such as Microsoft GPO or SMS) to deploy the installation package to Windows clients. For example:

- EXE file:

```
TRITONAP-ENDPOINT-x32.exe /v"/quiet /norestart"
```

- MSI file:

```
msiexec /package /v"\\path\Websense Endpoint.msi" /quiet /norestart
```

Here, “path” is the full path to the directory containing the MSI and its support files.



### Warning

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

---

Supported installation parameters include:

/v	Used to pass arguments that affect endpoint client deployment. Note that the arguments must be enclosed in straight quotes.
/quiet	Install the endpoint client in the background, without prompting the end user.
/norestart	Do not restart the client machine when the endpoint client has finished installing.

## Uninstalling Remote Filtering Client

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

### Windows

On Windows clients, 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. (You must extract the contents of the installation package as explained in [Using a third-party deployment tool for Windows](#), page 26, to locate the setup.ini file.)
- **<password>** is the anti-tampering password that you entered when creating the installation package.

To uninstall Remote Filtering Client from Windows clients manually:

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

### Mac OS X

To uninstall Remote Filtering Client from Mac OS X clients:

1. Open **System Preferences** and locate the Forcepoint preference pane (in the **Other** section).
2. Click **Uninstall Endpoint**.
  - Local administrator permissions are required to remove the client software.
  - If an anti-tampering password was set in the Package Builder, the administrator must enter the password to uninstall the client software.



# 3

## Configuring Remote Filtering Software

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Use the instructions in this document to:

- Configure your network firewall to handle communication between Remote Filtering Client, Remote Filtering Server, and Filtering Service appropriately.
- Determine whether user requests are permitted or blocked when Remote Filtering Client is unable to contact Remote Filtering Server from outside your organization's network.

### Firewall configuration

---

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 the Web module of the TRITON Manager.

See the documentation for your firewall product for configuration instructions.

## Global remote filtering settings

---

Use the **Settings > General > Remote Filtering** page in the Web module of the TRITON Manager to configure whether users receive Internet access when Remote Filtering Client cannot contact Remote Filtering Server from outside the network.

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 unrestricted access to the Internet when their computers cannot communicate with the Remote Filtering Server (fail open).

Optionally, you can also configure your remote filtering software to ignore HTTPS or FTP traffic, or change the Remote Filtering Client heartbeat interval. For instructions, see:

- [Configuring remote filtering to ignore HTTPS or FTP, page 30](#)
- [Configuring the Remote Filtering Client heartbeat interval, page 31](#)

## Configuring remote filtering to ignore HTTPS or FTP

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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 Server instances, repeat these steps for each one.

1. Navigate to the Forcepoint **bin** directory (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin, by default) on the Remote Filtering Server machine.
2. Open the **securewisproxy.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. Use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to restart Remote Filtering Server.

## Configuring the Remote Filtering Client heartbeat interval

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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 Forcepoint **bin** directory (`C:\Program Files\Websense\Web Security\bin` or `/opt/Websense/bin/`) on the Remote Filtering Server machine.
2. Open the **securewisproxy.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.





# 4

## Upgrading Remote Filtering Components

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

When you upgrade Web protection solutions, you must also upgrade Remote Filtering Server by running the new installer on the machine where Remote Filtering Server is installed. See [Installing Remote Filtering Server on Windows](#), page 14, for details.



### Note

Remote Filtering Server is backward compatible with the previous version of Remote Filtering Client.

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.

Upgrade each Remote Filtering Server instance **after** Filtering Service has been upgraded. If your network uses a single Remote Filtering Server, policy enforcement for remote machines is disrupted during the upgrade process. Plan for this by configuring an appropriate fail open/fail closed option. See [Global remote filtering settings](#), page 30, 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 policy enforcement occurs during the upgrade, but quota and continue time may not operate as expected.

For instructions, see:

- [Upgrading Remote Filtering Server](#)
- [Upgrading Remote Filtering Client](#)

## Upgrading Remote Filtering Server

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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 **Start the Upgrade** when prompted.
4. Follow the onscreen instructions to complete the upgrade process.
5. After the upgrade is complete, open the Web module of the TRITON Manager and navigate to the **Settings > General > Remote Filtering** page to verify your Remote Filtering configuration.

## Upgrading Remote Filtering Client

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

Related topics:

- [Upgrading Remote Filtering Server](#)

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

- **Manual upgrade:** Use a customized Remote Filtering Client installation package on each client machine to upgrade the Remote Filtering Client for Windows or Mac OS X. See [Upgrading Remote Filtering Client manually](#), page 34.
- **Automatic upgrade with third-party tool:** Use a customized Remote Filtering Client installation package with a third-party deployment tool to upgrade the Remote Filtering Client on Windows client machines. See [Upgrading Remote Filtering Client with a third-party deployment tool](#), page 35.

To create a custom installation package, see [Customizing the client installation package](#), page 23.

## Upgrading Remote Filtering Client manually

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

To manually upgrade the Remote Filtering Client:

1. Create a custom installation package as described in [Customizing the client installation package](#), page 23.
2. Run the installation package created for the target operating system as described in [Installing Remote Filtering Client 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 the Web module of the TRITON Manager.

1. Go to the **Settings > General > Remote Filtering** page.

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 30, for instructions on disabling this functionality.
6. Click **OK** to cache any changes. Changes are not implemented until you click **Save and Deploy**.

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

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

To deploy the new version of the Remote Filtering Client to Windows client machines:

1. Create the installation package as described in [Customizing the client installation package](#), page 23.
2. If you are using a tool like GPO and want to deploy a MSI file rather than an EXE file, use a file compression tool like 7-Zip, WinZip, or WinRAR to extract the contents of the installation package.

This exposes the **Websense Endpoint.msi** file and its support files.

3. Use a third-party deployment tool (such as Microsoft GPO or SMS) to deploy the uncompressed installation package to the client machines. For example:

- EXE file:

```
TRITONAP-ENDPOINT-x32.exe /v"/quiet /norestart"
```

- MSI file:

```
msiexec /package /v"XPSWDRF=<password> \\path\Websense  
Endpoint.msi" /quiet /norestart
```

Here, “<password>” is the anti-tampering password specified during installation of the previous Remote Filtering Client version, and “path” is the full path to the directory containing the MSI and its support files.

Supported upgrade parameters and arguments include:

/v	Used to pass arguments that affect endpoint client deployment. Note that the arguments must be enclosed in straight quotes.
/quiet	Upgrade the endpoint client in the background, without prompting the end user.
/norestart	Do not restart the client machine when the endpoint client has finished being upgraded.

After upgrading the Remote Filtering Client on remote computers:

1. Open the Web module of the TRITON Manager.
2. Go to the **Settings > General > Remote Filtering** page.
3. Review and update the settings on this page, as needed.
4. Click **OK** to cache your 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 30, for instructions on disabling this functionality.

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

# A

## Troubleshooting remote filtering software

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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

- [Block pages are not being displayed, page 37](#)
- [When client machines use a proxy server, page 38](#)
- [General troubleshooting procedures, page 38](#)

### Block pages are not being displayed

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

If Remote Filtering Clients are receiving the correct policies, but users get an error instead of the expected block pages, make sure that:

- The firewall between the Filtering Service machine and the Remote Filtering Server machine is properly configured, as described in [Firewall configuration, page 29](#). 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.
- Remote Filtering Client is not installed on the Remote Filtering Server machine. An instance of Remote Filtering Client running on the Remote Filtering Server machine eventually uses all available connections to the server. When no connections are available, remote computers cannot connect to Remote Filtering Server and are not filtered. Uninstall any Remote Filtering Client running on the Remote Filtering Server machine.
- 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 38](#).

---

## Reporting tools don't include remote filtering data

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

If Network Agent is configured to log HTTP requests, reporting data from machines with Remote Filtering Client does not appear in Real-Time Monitor or TestLogServer.

To address this issue:

1. Log on to the Web module of the TRITON Manager.
2. Navigate to the **Settings > Network Agent > <IP address>** page for a Network Agent instance.
3. Select a Network Agent NIC.
4. In the **Integrations** section, clear the check box next to **Log HTTP requests**.
5. Click **OK**, then click **OK** again to cache your changes.
6. Repeat steps 2-5 for each Network Agent instance and NIC.
7. Click **Save and Deploy** to implement your changes.

## When client machines use a proxy server

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

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

---

Deploying the Remote Filter Module | Web Filter & Security | v8.2.x, v8.3.x

1. Verify that your subscription key includes remote filtering.
2. Make sure that Remote Filtering Server is running.
  - Windows: Use the Windows Services tool to find the status of **Remote Filtering Server**.
  - Linux: Use the `/opt/Websense/WebsenseDaemonControl` command to review service status.
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 web protection components, check that they have been properly configured, as described in [Firewall configuration, page 29](#).

- 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 [Firewall configuration, page 29](#).
    - 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** monitoring 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\Web Security\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.

- 
9. Check that communication settings 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 Server on Windows](#), page 14, for more information.

- a. On the Remote Filtering Server machine, navigate to the product **bin** directory (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default), and open the **securewisproxy.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 hostname 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 the **ipconfig** (Windows) or **ifconfig -a** (Linux) command to get the IP addresses for each network interface card (NIC) in that machine.

Verify that these IP address values match the Proxy Server parameters found in the **securewisproxy.ini** file.
  - e. Check the values on the Remote Filtering Client machines. Contact Forcepoint 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. Use the Windows Services tool or /opt/WebSense/WebSenseDaemonControl command to stop Remote Filtering Server.
    - b. Open the **securewisproxy.ini** file.
    - c. Add or edit the **TraceType** entry to read:

```
TraceType=All
```
    - d. Save and close the **securewisproxy.ini** file.
    - e. Start Remote Filtering Server.
    - f. Go to a remote client computer and browse the Internet.



- 
- g. On the Remote Filtering Server machine, navigate to the product **bin** directory (C:\Program Files\WebSense\Web Security\bin or /opt/WebSense/bin/, by default) and open the **traceFile.log** file.

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

- If the client and server pass phrases do not match, 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**.
- If you do not know the correct pass phrase, reinstall the Remote Filtering Server and enter a new proper pass phrase. Then, reinstall the Remote Filtering Clients, using the same pass phrase.

If the same error occurs, contact Forcepoint 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.

