smoothwall®

The Web You Want

Smoothwall Connect Filter

Smoothwall Connect Filter for Windows Installation and Administration Guide

Smoothwall® Smoothwall Connect Filter, Installation and Administration Guide, July 2014

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Smoothwall Connect Filter.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Smoothwall.

For more information, contact: docs@smoothwall.net

© 2001 – 2014 Smoothwall Ltd. All rights reserved.

Trademark notice

Smoothwall and the Smoothwall logo are registered trademarks of Smoothwall Ltd.

Linux is a registered trademark of Linus Torvalds. Snort is a registered trademark of Sourcefire INC. DansGuardian is a registered trademark of Daniel Barron. Microsoft, Internet Explorer, Window 95, Windows 98, Windows NT, Windows 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. Apple and Mac are registered trademarks of Apple Computer Inc. Intel is a registered trademark of Intel Corporation. Core is a trademark of Intel Corporation.

All other products, services, companies, events and publications mentioned in this document, associated documents and in Smoothwall software may be trademarks, registered trademarks or service marks of their respective owners in the UK, US and/or other countries.

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Smoothwall Connect Filter contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada: United Kingdom: All other countries:	1 800 959 3760 0870 1 999 500 +44 870 1 999 500
Fax	USA and Canada: United Kingdom: All other countries:	1 888 899 9164 0870 1 991 399 +44 870 1 991 399

Contents

About This Guide 1
Audience and Scope 1
Organization and Use 1
Conventions 2
Related Documentation 2

Chapter 1 Introduction to Smoothwall Connect Filter 3
About Smoothwall Connect Filter 3
About Smoothwall Connect Filter Locations 4
Supported Operating Systems 6

Chapter 2 Preparing Your Smoothwall System 7
Enabling and Configuring MobileProxy 7
Configuring MobileProxy Servers 8
Managing MobileProxy Servers 8
Generating Client Keys 9
Generating Server Keys 9
Installing a Server Key on the MobileProxy Server 9
Configuring Network Guardian User Credentials 10

Chapter 3 Installing Smoothwall Connect Filter 11
Installing Smoothwall Connect Filter 11
Removing Smoothwall Connect Filter 12

Chapter 4 Using Smoothwall Connect Filter 13
Using Smoothwall Connect Filter in a Local Environment 13
Example Configuration in Windows Server 2008 14
Using Smoothwall Connect Filter with HTTPS 14
About Smoothwall Connect Filter Statuses 15
Accessing Smoothwall Connect Filter 15
Configuring the Proxy 16
Changing the Proxy 16

Before Browsing the Internet..... 17
Viewing Log Files 17

Index..... 19

About This Guide

Smoothwall Connect Filter for Windows is a web redirector for Windows devices.

This manual provides guidance for installing Smoothwall Connect Filter for Windows.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Smoothwall Connect Filter.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System application
- An overall understanding of the functionality of the Smoothwall Connect Filter application
- An overall understanding of networking concepts

Organization and Use

This guide is made up of the following chapters and appendices:

- *Chapter 1, Introduction to Smoothwall Connect Filter* on page 3
- *Chapter 2, Preparing Your Smoothwall System* on page 5
- *Chapter 3, Installing Smoothwall Connect Filter* on page 11
- *Chapter 4, Using Smoothwall Connect Filter* on page 13
- *Index* on page 19

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Smoothwall Connect Filter for Windows
Cross-references and references to other guides	*Italics*	See *Chapter 1, Introduction to Smoothwall Connect Filter* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`
Smoothwall System	This may be one of: • Guardian • Advanced Firewall • Network Guardian • Secure Web Gateway • Unified Threat Management • WAM-Edge depending on the license purchased	

This guide is written in such a way as to be printed on both sides of the paper.

Related Documentation

The following guides provide additional information relating to the Smoothwall Connect Filter application:

- *Smoothwall Connect Filter for iOS Installation and Administration Guide*, which describes how to install and configure the Smoothwall Connect Filter client for iOS devices
- *Smoothwall Connect Filter for Mac OS Installation and Administration Guide*, which describes how to install and configure the Smoothwall Connect Filter client for Mac OS devices
- *Guardian Administration Guide*, which describes how to use Guardian3

1 Introduction to Smoothwall Connect Filter

This chapter provides an overview of Smoothwall Connect Filter, including:

- *About Smoothwall Connect Filter* on page 3
- *Supported Operating Systems* on page 6

About Smoothwall Connect Filter

Smoothwall Connect Filter is a web redirector for Windows clients and devices. It enables you to enforce your organization's web content filtering policy on Windows devices owned by your organization, wherever they are located.

By installing Smoothwall Connect Filter on devices, users' browsers are forced to send web content requests to Smoothwall proxies. Smoothwall proxies then enforce your organization's web content filtering policy by blocking undesirable and malicious content.

The following should be considered when using Smoothwall Connect Filter:

- Smoothwall Connect Filter must be installed using administrative privileges. Users should not be given access to the administrator account on the Windows device.
- You must supply users with Smoothwall System usernames and passwords, as Smoothwall Connect Filter prompts users to authenticate themselves when they start to browse.

  For a detailed description of how to set this up, see *Configuring Smoothwall Connect Filter User Credentials* on page 10
- Users cannot remove Smoothwall Connect Filter unless they are using a device account with administrator privileges.

  For more information about removing a Smoothwall Connect Filter installation, see *Removing Smoothwall Connect Filter* on page 12
- It is recommended that you tell users that Smoothwall Connect Filter has been installed on their devices, that web content is being filtered, and their browsing is being logged.

- It is recommended that you provide users with a way of reporting problems with over- or under-blocking of pages, so that you can adjust your policy to suit your organization.

About Smoothwall Connect Filter Locations

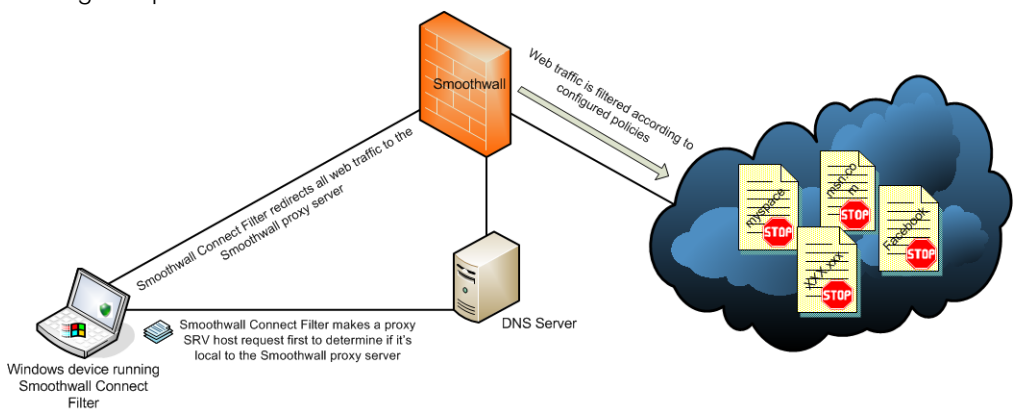
Smoothwall Connect Filter works by determining where the Windows device is on the network, then redirecting web traffic as appropriate.

There are three possible locations that Smoothwall Connect Filter detects in order to connect to the proxy server:

- Behind a local Smoothwall proxy server — In an environment, such as an office, where all web traffic is filtered.

  To determine whether Smoothwall Connect Filter is behind a local Smoothwall proxy server, it makes a proxy Service (SRV) host request. An SRV record is a special type of DNS record that allows you to specify a port number, as well as a hostname, for a given service. This functionality allows Smoothwall Connect Filter to be directed to an internal Guardian proxy port.

  If it determines it is behind a local proxy server, it authenticates the user, and filters according to configured policies.

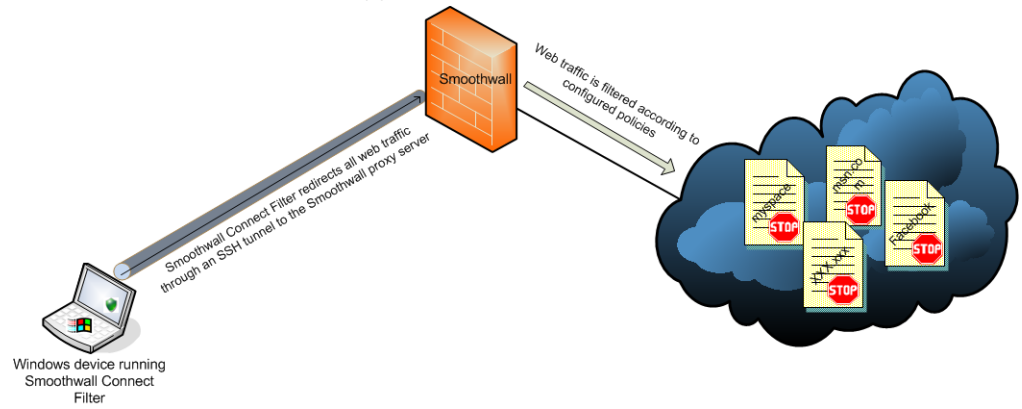


  For more information about how Smoothwall Connect Filter determines if it's behind a local proxy server, see *Using Smoothwall Connect Filter in a Local Environment* on page 13.

- Remote on an open internet connection— Such as a home internet connection.

  Smoothwall Connect Filter opens a secure tunnel (SSH) tunnel between the Windows device and the Smoothwall proxy server configured to support such access. All web requests are

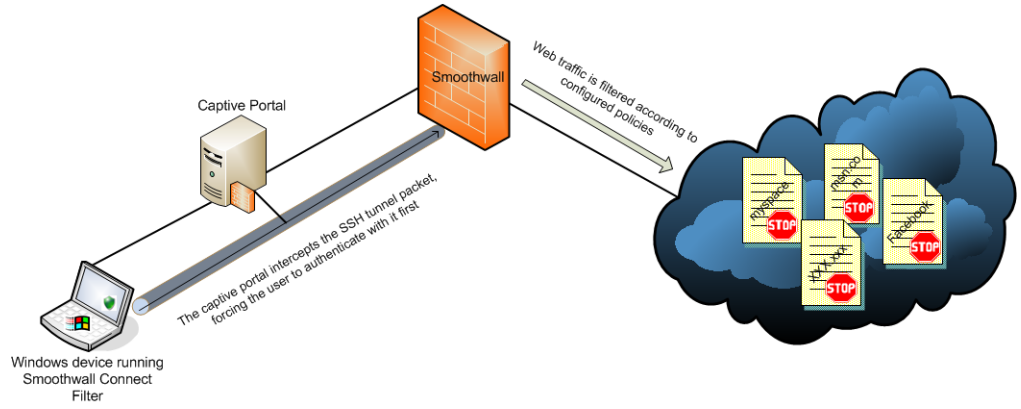
redirected at kernel level through the tunnel to the remote proxy server, and web filtering as if in a local environment, can be applied.



- Remote behind a captive portal — A captive portal redirects initial web traffic to a special web page for authentication before web browsing can continue. Typically, these are public internet places, such as hotels and coffee shops.

  There is no extra configuration required on Smoothwall Connect Filter to use a captive portal. Smoothwall Connect Filter will try to establish an SSH tunnel to the Smoothwall proxy server. The captive portal will intercept the traffic, and Smoothwall Connect Filter will relax its redirector to allow the user to authenticate with the captive portal before browsing.

  A red shield icon, with a pop-up status message of “Registering with portal” will be displayed to the user until authentication on the captive portal is made. For a detailed description of the different statuses of Smoothwall Connect Filter, see *About Smoothwall Connect Filter Statuses* on page 15.



Note: No matter the location, consistent filtering policies will be used for the user.

Supported Operating Systems

Smoothwall Connect Filter supports the following operating systems on devices:

- Microsoft Windows 7 with the latest updates installed
- Microsoft Windows 8 with the latest updates installed

Note: The following operating systems are not supported by Smoothwall Connect Filter: Windows XP and Windows Vista. Microsoft Surface devices running Windows RT and Windows phones are also not supported.

2 Preparing Your Smoothwall System

Before you can install Smoothwall Connect Filter, the following must be configured on your Smoothwall System:

- *Enabling and Configuring MobileProxy* on page 5
- *Generating Client Keys* on page 7
- *Generating Server Keys* on page 7
- *Configuring Smoothwall Connect Filter User Credentials* on page 8

Note: If running a Network Guardian system, configure a port forward rule from your firewall to Network Guardian.

Enabling and Configuring MobileProxy

You must enable MobileProxy on your Smoothwall System before installing Smoothwall Connect Filter on your iOS devices.This enables proxy authentication for Smoothwall Connect Filter users.

To enable MobileProxy, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Settings**.
2. From the **Global options** panel, select **Enable** and click **Save**.
3. Ensure you click **Restart Proxy** when prompted.
4. Browse to **System > Administration > External access**.
5. From the **Interface** drop-down menu, select **External**.
6. From the **Service** drop-down list, select **MobileProxy server (61001)**.
7. Click **Add**.

   Your Smoothwall System makes MobileProxy available as an external service.

Note: You will need to open port 61001 on your firewall to allow Smoothwall Connect Filter into the proxy from outside the network.

Configuring MobileProxy Servers

You must configure the proxy servers for Smoothwall Connect Filter to proxy through. Typically, this is your Smoothwall System.

To specify the IP address or hostname, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Proxies**.
2. Within the **Manage MobileProxy server** panel, configure the following parameters:
   - **Server name** — The name to identify the proxy server.
   - **Server address** — The IP address or hostname of the proxy server. Typically, this is the external IP address of your Smoothwall System. You can also use the IP address that forwards through to your Smoothwall System instead.
   - **Comment** — You can choose to enter optional text about the proxy server.
3. Click **Save** to save your settings.
4. Repeat steps 2 and 3 to add additional proxy servers.

Note: Any additional proxy servers added here, must have the server key of the original proxy server installed. For a detailed description of how to do this, see *Generating Server Keys* on page 7.

Smoothwall Connect Filter also supports proxy exceptions when running in a remote location. Proxy exceptions are URLs or IP addresses that do not need to be redirected through the tunnel to the remote Smoothwall proxy server.

To specify a proxy exception, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Exceptions**.
2. Enter a valid IP address or hostname for each exception.
3. Click **Save** to save your settings.

For a detailed description of how to configure MobileProxy, refer to your Smoothwall System's Administration Guide.

Managing MobileProxy Servers

All configured proxy servers will appear in the **MobileProxy servers** panel. The order they are listed determines the order of priority, from top to bottom. Smoothwall Connect Filter will try each proxy server until an available proxy responds to requests.

You can change the priority order by dragging and dropping the servers in the **MobileProxy servers** panel into the required order.

You can also edit and delete servers as required.

To edit a MobileProxy server, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Proxies**.
2. Click the **Edit** button for the configured MobileProxy server.

   The configured parameters will appear in the **Manage MobileProxy server** panel.
3. Change the parameters as required, and click **Save**.

To delete a MobileProxy server, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Proxies**.
2. Click the **Delete** button for the configured MobileProxy server.
3. Confirm the correct MobileProxy server, and click **Delete**.

Generating Client Keys

Each iOS device running Smoothwall Connect Filter must have a client key installed. MobileProxy requires the client key to authenticate the iOS device requesting web traffic redirection.

To generate a client key, do the following:

1. On the Smoothwall System, browse to **Web proxy > Mobileproxy > Settings**.
2. From the **Manage MobileProxy keys** pane, click **Download**.
3. Make the client key accessible to the device on a secure server or download it to the iOS device.

Generating Server Keys

All MobileProxy servers listed in the **MobileProxy servers** panel must have the same MobileProxy server key installed. This forces the Smoothwall Connect Filter to only use a limited number of MobileProxy servers. This has the advantage of load-balancing the web traffic from a large number of Smoothwall Connect Filter's across a number of MobileProxy servers.

To generate a server key, do the following:

1. On the Smoothwall System which supplied the client key (see *Generating Client Keys* on page 7), browse to **Web proxy > Mobileproxy > Settings**.
2. From the **Manage MobileProxy keys** pane, click **Advanced >>**.

   Two **Download** button options are available:

   – Download MobileProxy client key

   – Download MobileProxy server key
3. Click the bottom **Download** button to download the server key.
4. Make the server key accessible to other MobileProxy servers or manually upload it. For more information, see *Installing a Server Key on the MobileProxy Server* on page 7.

Installing a Server Key on the MobileProxy Server

You can install the server key using one of two methods:

- By downloading it from the Smoothwall System which supplied the MobileProxy client key, then manually uploading it to each MobileProxy server. For a detailed description of how to do this, see below.
- Replicating it from the Smoothwall System which supplied the MobileProxy client key.

  Your Smoothwall System must be part of a centrally managed solution for the replication to be successful. For a detailed description of how to setup and manage a centrally managed Smoothwall System, refer to your Smoothwall System's Administration Guide.

To manually upload a server key to the MobileProxy server, do the following:

1. Log into the other Smoothwall System, browse to **Web proxy > Mobileproxy > Settings**.
2. From the **Manage MobileProxy keys** pane, click **Advanced >>**.
3. Click **Choose File** and browse to the server key.
4. Click **Upload** and the server key will be made available. Smoothwall Connect Filter will now be able to connect to the proxy server.

Configuring Smoothwall Connect Filter User Credentials

Smoothwall Connect Filter requires user authentication for both local and remote internet access. Usernames and passwords for Smoothwall Connect Filter users must be setup in your Smoothwall System first, via your configured directory services, or as local users.

To configure MobileProxy Local User credentials, do the following:

1. On the Smoothwall System, browse to **Services > Authentication > Directories**.
2. Expand the **Local users** directory tree.
3. Configure your MobileProxy user accounts as required.

   For a detailed description of how to configure local users, and other directory services, refer to your Smoothwall System's Administration Guide.

   For a detailed description of authentication and how to configure it, refer to your Smoothwall System's Administration Guide.

Note: Smoothwall Connect Filter also supports user authentication from account directories, such as Active Directory.

3 Installing Smoothwall Connect Filter

This chapter describes how to install Smoothwall Connect Filter on a Windows device, including:

- *Installing Smoothwall Connect Filter* on page 11
- *Removing Smoothwall Connect Filter* on page 12

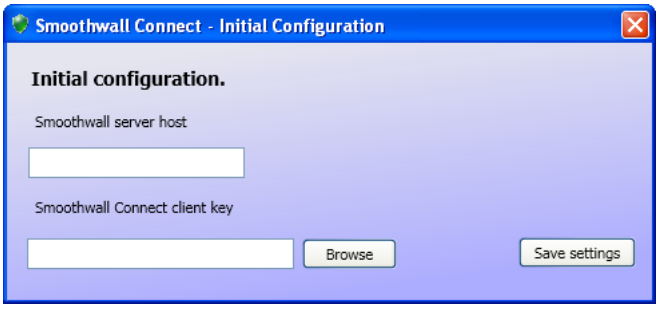
Installing Smoothwall Connect Filter

Note: You must install Smoothwall Connect Filter using an account which has administrative privileges. These privileges should not be provided to the users of the Windows device.

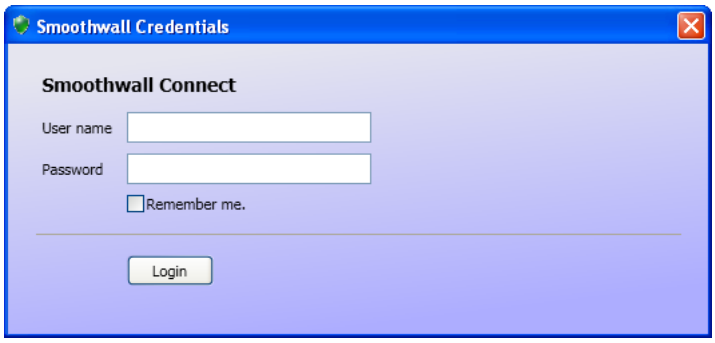
To install Smoothwall Connect Filter:

1. Download the Smoothwall Connect Filter installation program to your Windows device.
2. Double-click on the supplied `.exe` file and select **Install**. The setup wizard starts.
3. You may be prompted to install additional software — Visual C++ and .NET Framework. Confirm both installations.
4. When prompted, either accept the default installation folder or specify a new one.
5. Click **Install** to continue.

   When the Smoothwall Connect Filter files are in place, the Initial Configuration dialog box is displayed:



6. Enter the following information:
   - **Smoothwall server host** — The external IP address of your Smoothwall System
   - **Smoothwall Connect client key** — The full path to the Smoothwall Connect Filter client key. For more information, see *Configuring MobileProxy Servers* on page 8.
7. Click **Save settings**.
8. Click **Next**. The setup wizard applies the settings.
9. Click **Finish** to close the wizard. The Credentials dialog box is displayed:



10. Log in using your Smoothwall System credentials. For more information, see *Accessing Smoothwall Connect Filter* on page 15.

Removing Smoothwall Connect Filter

Note: Only an account with administrative privileges can remove Smoothwall Connect Filter.

To remove Smoothwall Connect Filter from a device, do the following:

1. On the device, open **Control Panel > Add or Remove Programs**.
2. From the list of installed programs, select **Smoothwall Connect Filter** and click **Remove**.
3. Complete the setup wizard to remove Smoothwall Connect Filter.

4 Using Smoothwall Connect Filter

This chapter describes how to use Smoothwall Connect Filter, including:

- *Using Smoothwall Connect Filter in a Local Environment* on page 13
- *Using Smoothwall Connect Filter with HTTPS* on page 14
- *About Smoothwall Connect Filter Statuses* on page 15
- *Accessing Smoothwall Connect Filter* on page 15
- *Configuring the Proxy* on page 16
- *Before Browsing the Internet* on page 17
- *Viewing Log Files* on page 17

Using Smoothwall Connect Filter in a Local Environment

To determine whether Smoothwall Connect Filter is behind the local proxy, it makes a proxy Service (SRV) host request. You must configure your Domain Name System (DNS) server with the SRV record details, including:

- Service name — `_swc`
- Protocol name — `_tcp`
- Port number — Typically, this is `800`.
- Hostname — This is the hostname of your Smoothwall System. The corresponding “A” record for the host should be resolved to an internal IP address.

You can also use this setup to roll out the Smoothwall Connect Filter client across domains with multiple DNS servers, where multiple IP addresses are resolved to a single hostname.

Note: If the SRV record is not configured, Smoothwall Connect Filter assumes the Windows device is in a remote but open location, and will bring up an SSH tunnel to MobileProxy. In this situation, Smoothwall Connect Filter will continue to function normally, but will use additional resources on the Smoothwall proxy server.

Example Configuration in Windows Server 2008

You may not be using Windows Server 2008. You must refer to your own network documentation for a description of how to setup this up according to your network. The following is only relevant for Windows Server 2008.

To configure an SRV record in Windows Server 2008, do the following:

1. Log into your Windows Server 2008 machine, and open the DNS Manager window, ensuring the entry for the Smoothwall System has an “A” record.
2. Right-click in the **DNS** panel, and select **Other New Records**.
3. From the displayed list, highlight **Service Location (SRV)**.
4. Click **Create Record**.
5. Configure the parameters as detailed in *Using Smoothwall Connect Filter in a Local Environment* on page 13.

   If the relevant hostname and port number are not known, you can make a test DNS request to return the required values.

Note: Using the Group Policy in Windows Server to configure proxy settings will interfere with the operation of Smoothwall Connect Filter. You must ensure Smoothwall Connect Filter clients do not have proxies configured in this way.

Using Smoothwall Connect Filter with HTTPS

Smoothwall Connect Filter filters HTTPS traffic and applies decrypt and implement policies. Typically, your Smoothwall System displays a warning page to users who try to access HTTPS websites that their traffic is being decrypted and inspected. However, to ensure correct operations, the warning page needs to be disabled.

Note: When you enable a HTTP inspection policy, which decrypts and inspects content, you must install the Guardian3 CA certificate uploaded in order for the policy to work. For a detailed description of how to download the Guardian3 CA certificate, refer to the *Guardian Administration Guide*.

To disable the warning page, do the following:

1. On the Smoothwall System, browse to **Guardian > HTTPS inspection > Settings**.
2. From the Manage **HTTPS interception warning** panel, change **Warning frequency** to **Never**.
3. Click **Save**.

About Smoothwall Connect Filter Statuses

Once installed on a Windows device, Smoothwall Connect Filter runs as a system tray user interface. The following tray icons are available:

Icon	Popup Status Message	Description
	Connected	Smoothwall Connect Filter has authenticated with the proxy server and the user is now being filtered.
	Waiting for network	The Windows device does not have an IP address; or The network state has changed and the Windows device is waiting for a new connection prior to re-establishing the connection to the proxy; or Smoothwall Connect Filter is unable to locate a remote proxy server.
	Connecting to proxy	Smoothwall Connect Filter is trying to bring up a secure tunnel with the proxy server using new or saved credentials.
	Logging on	Smoothwall Connect Filter is attempting to authenticate with the proxy server using new or saved credentials.
	Connection failed	Smoothwall Connect Filter is unable to create a secure tunnel to the proxy server.
	Registering with portal	Smoothwall Connect Filter has determined it is behind a captive portal, and has relaxed the redirector to allow the user to register with the portal. For more information, see *About Smoothwall Connect Filter Locations* on page 4.

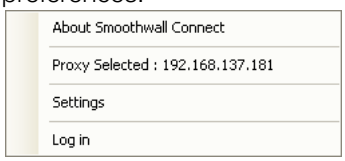
Accessing Smoothwall Connect Filter

Once installed, Smoothwall Connect Filter is accessible from the system tray. For a detailed description of the various Smoothwall Connect Filter icons, and their meanings, see *About Smoothwall Connect Filter Statuses* on page 15.

To access Smoothwall Connect Filter, do the following:

- Right-click on the Smoothwall Connect Filter icon.

  Smoothwall Connect Filter status, and proxy information are displayed. You can also change preferences:



Configuring the Proxy

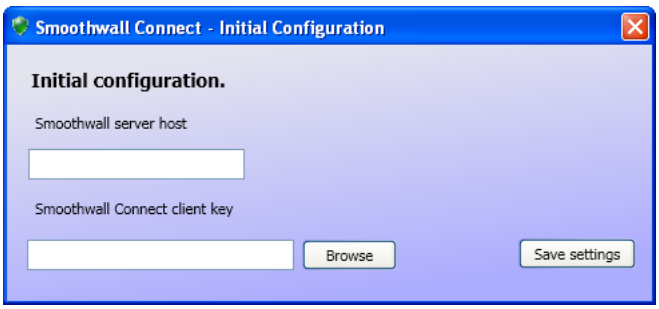
You must configure Smoothwall Connect Filter to use the correct proxy server before web traffic can be redirected. The initial Smoothwall Connect Filter configuration is done during installation. However, you can edit this configuration after installation.

Note: You must have administrator privileges to configure Smoothwall Connect Filter.

To edit the Smoothwall Connect Filter configuration, do the following:

1. In `C:\Program Files\Smoothwall\Smoothwall Connect`, double-click on **MGConfig.exe**.

   The Initial Configuration dialog box is displayed:



2. Enter the following information:
   - **Smoothwall server host** — The external IP address of your Smoothwall System
   - **Smoothwall Connect client key** — The full path to the Smoothwall Connect Filter client key. For more information, see *Configuring MobileProxy Servers* on page 8.
3. Click **Save settings** to confirm your changes.

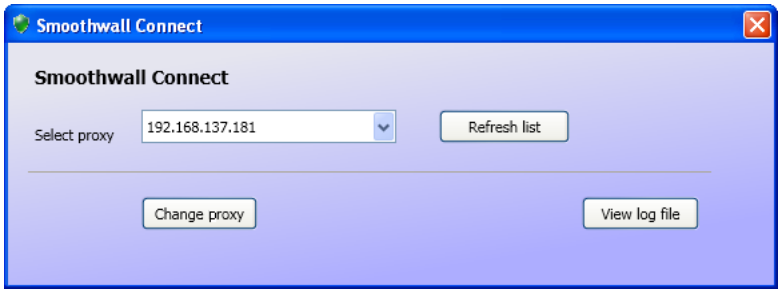
Changing the Proxy

From time to time, you may need to change the proxy server your Smoothwall Connect Filter client uses, but need to keep the same client key.

To configure which proxy to use, do the following:

1. Ensure the new proxy server is configured in MobileProxy — see *Configuring MobileProxy Servers* on page 8
2. From your Windows device, right-click on the Smoothwall Connect Filter icon in the system tray, and select **Settings**.

   The following dialog box is displayed:



3. From the **Select proxy** drop-down list, choose the proxy server to user for this Windows device.

   You may need to click **Refresh list** if the required proxy server has been added recently.

4. Click **Change proxy** to confirm your selection.

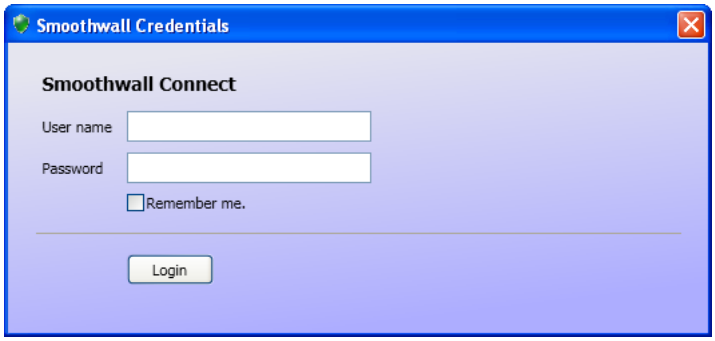
The user will be prompted to re-enter their Smoothwall System credentials.

Before Browsing the Internet

Before users can start browsing the internet from their Windows device, they must log into Smoothwall Connect Filter using their Smoothwall System user credentials.

To log into Smoothwall Connect Filter, do the following:

1. In the system tray, right-click on the Smoothwall Connect Filter icon and select **Login**. The following dialog box is displayed:



2. Enter the following information:
   - **User name** — The Smoothwall username
   - **Password** — The Smoothwall password
   - **Remember me.** — Select this to save user credentials for future authentication. This is an optional setting.
3. Click **Login**.

The user's username and password are stored in the Current User registry and the values are encrypted to prevent plain text view.

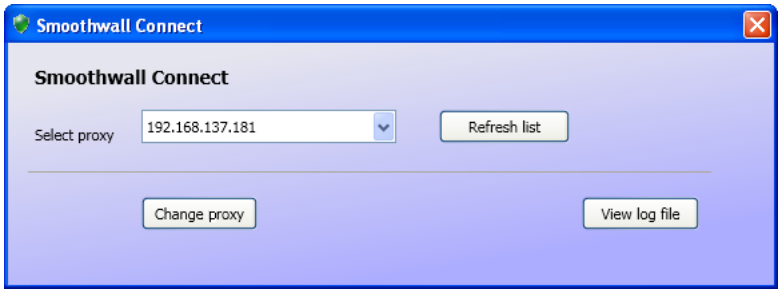
Viewing Log Files

Smoothwall Connect Filter maintains a separate log file for support and diagnostic purposes only.

To view the log file for a particular proxy server, do the following:

1. In the system tray, right-click on the Smoothwall Connect Filter icon and select **Settings**.

The following dialog box is displayed:



2. Click **View log**.

   Smoothwall Connect Filter opens the log file in a separate window.

Index

A
about 3
accessing 15

C
changing MobileProxy 16
client key 9
configuring 16

H
HTTPS 14

I
installation 11

L
locations 4
log files 17
logging in 17

M
MobileProxy 7
  configuring 7
  enable 7

P
prerequisites 7

R
removing 12

S
Smoothwall Connect 3
SRV record 13
status 15
supported operating systems 6
system tray icon 15

U
user credentials 10
username 10

smoothwall®

The Web You Want