

smoothwall[®]

The Web You Want

Smoothwall Connect Filter

Smoothwall Connect Filter for iOS 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: 1 800 959 3760 United Kingdom: 0870 1 999 500 All other countries: +44 870 1 999 500
Fax	USA and Canada: 1 888 899 9164 United Kingdom: 0870 1 991 399 All other countries: +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 the Smoothwall Connect Filter for iOS Client	3
	About Smoothwall Connect Filter for iOS.....	3
Chapter 2	Preparing Your Smoothwall System	5
	Enabling and Configuring MobileProxy	5
	Configuring MobileProxy Servers	6
	Managing MobileProxy Servers	6
	Generating Client Keys.....	7
	Generating Server Keys.....	7
	Installing a Server Key on the MobileProxy Server	7
	Configuring Smoothwall Connect Filter User Credentials.....	8
Chapter 3	Installing Smoothwall Connect Filter	9
	Installing Smoothwall Connect Filter	9
Chapter 4	Troubleshooting Smoothwall Connect Filter	15
	Browser User Agents.....	15
	Index.....	17

About This Guide

Smoothwall Connect Filter for iOS is a web redirector for iOS™ devices.

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

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 the Smoothwall Connect Filter for iOS Client* on page 3
- *Chapter 2, Preparing Your Smoothwall System* on page 5
- *Chapter 3, Installing Smoothwall Connect Filter* on page 9
- *Chapter 4, Troubleshooting Smoothwall Connect Filter* on page 15
- *Index* on page 17

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Smoothwall Connect Filter for iOS
Cross-references and references to other guides	<i>Italics</i>	See <i>Chapter 1, Introduction to the Smoothwall Connect Filter for iOS Client</i> on page 3
Filenames and paths	Courier	The <code>portal.xml</code> file
Variables that users replace	<i>Courier Italics</i>	<code>http://<my_ip>/portal</code>
Smoothwall System	This may be one of: <ul style="list-style-type: none"> 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:

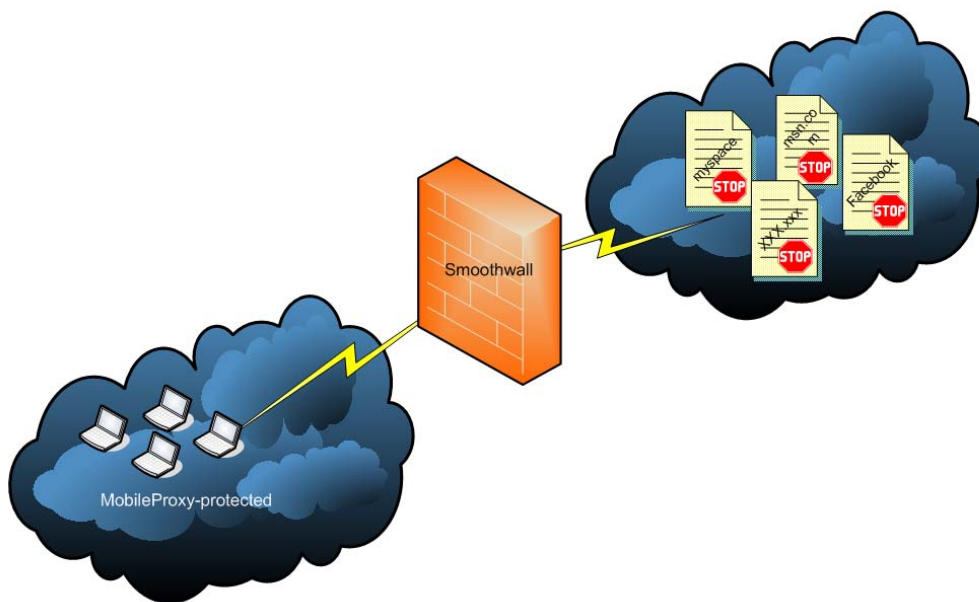
- *Smoothwall Connect Filter for Windows Installation and Administration Guide*, which describes how to install and configure the Smoothwall Connect Filter client for Windows devices
- *Smoothwall Connect Filter for Mac OS Installation and Administration Guide*, which describes how to install and configure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

1 Introduction to the Smoothwall Connect Filter for iOS Client

This chapter provides an overview of Smoothwall Connect Filter.

About Smoothwall Connect Filter for iOS

Smoothwall Connect Filter for iOS is a proxy redirector for iOS clients and devices. It enables you to enforce your organization's web content filtering policy on iOS devices owned by your organization.



By installing a Smoothwall Connect Filter client on devices, users' browsers are forced to send web content requests, both HTTP and HTTPS, 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 a Smoothwall Connect Filter client:

- You must supply users with Smoothwall System usernames and passwords, as the Smoothwall Connect Filter client 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 8

- It is recommended that you tell users that a Smoothwall Connect Filter client 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.

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 a Smoothwall Connect Filter client on an iOS device.

Installing Smoothwall Connect Filter

The following section explains how to install Smoothwall Connect Filter.

To install Smoothwall Connect Filter:

1. In a text editor, enter the following:

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>host</key> <string>Smoothwall_System_IP</string>
    <key>key</key> <string>your .pem filename</string>
    <key>logOutBackground</key> <true_or_false/>
  </dict>
</plist>
```

where:

- *Smoothwall_System_IP* is either:

The Advanced Firewall running Guardian 3, Secure Web Gateway, or Unified Threat Management system's external IP address.

For Network Guardian systems, check you have a port forward rule from your firewall to Network Guardian and then enter the firewall's external IP address.

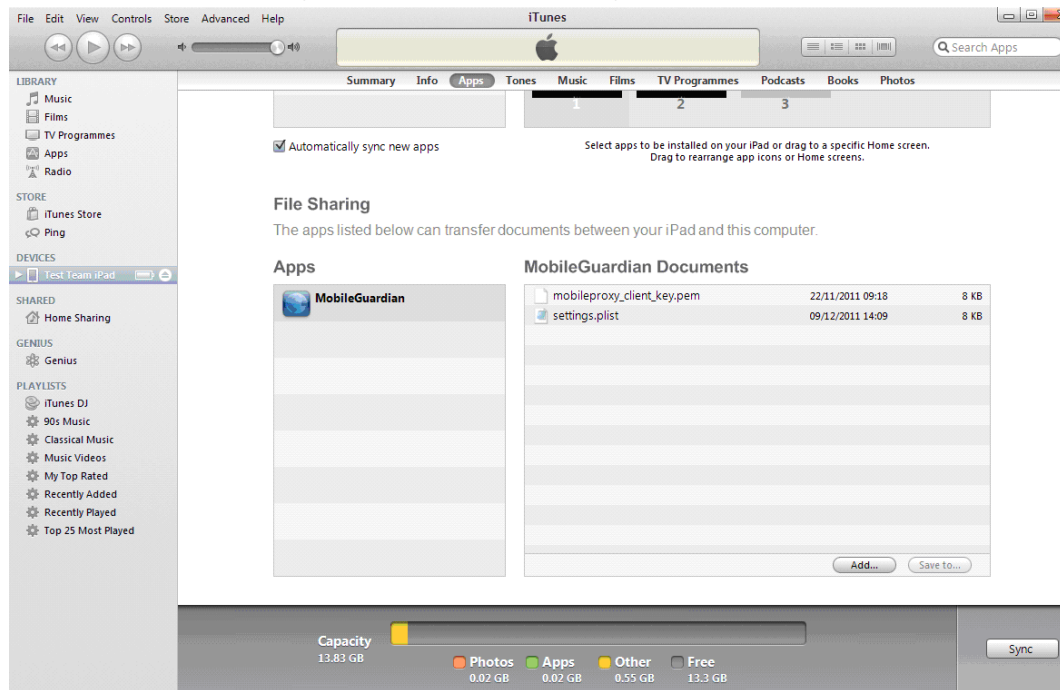
- *<string>.pem filename</string>* is the name of the .pem file downloaded; see *Generating Client Keys* on page 7

- `<key>logOutBackground</key><true_or_false/>` – This setting determines if a persistent authorized tunnel established. This enables users to use the iOS multi-tasking function without being logged out.

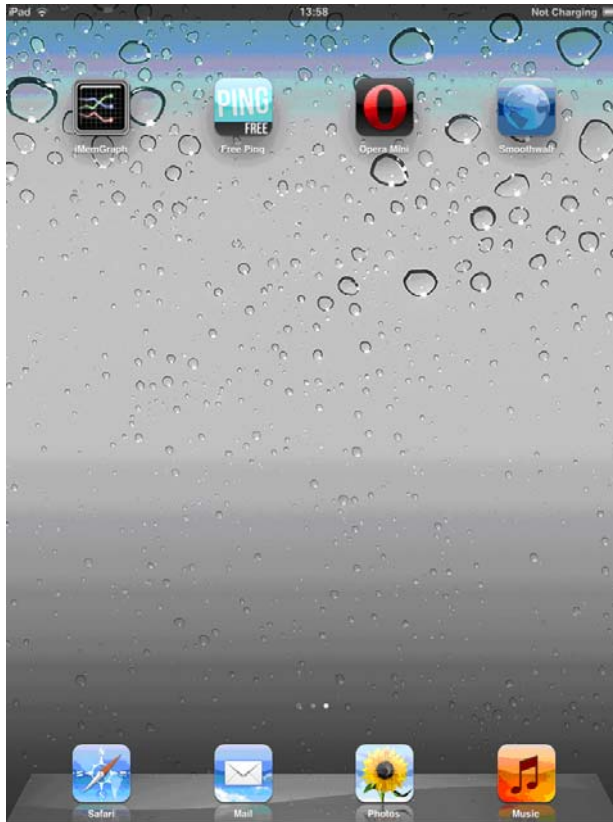
When set to `true`, when a user uses the multi-tasking function, they will be required to re-authenticate when browsing again.

When set to `false`, the connection is left open, allowing the user to return at a later point and continue browsing without re-authenticating.

2. Save the file as `settings.plist` and close the file.
3. On the device, go to the App store and download **Smoothwall MobileGuardian iOS**.
4. Connect the device to your PC and start iTunes®.
5. In iTunes, select the device in the left hand menu and, on the Apps screen, in the File Sharing area, locate and select **MobileGuardian iOS**.
6. Click the **Add...** button, locate the `settings.plist` file and the MobileProxy client key (`.pem`) file you want and click **Choose**. The selected files will be copied to **Smoothwall MobileGuardian iOS** on your iOS device immediately.



7. On the device's Home screen.

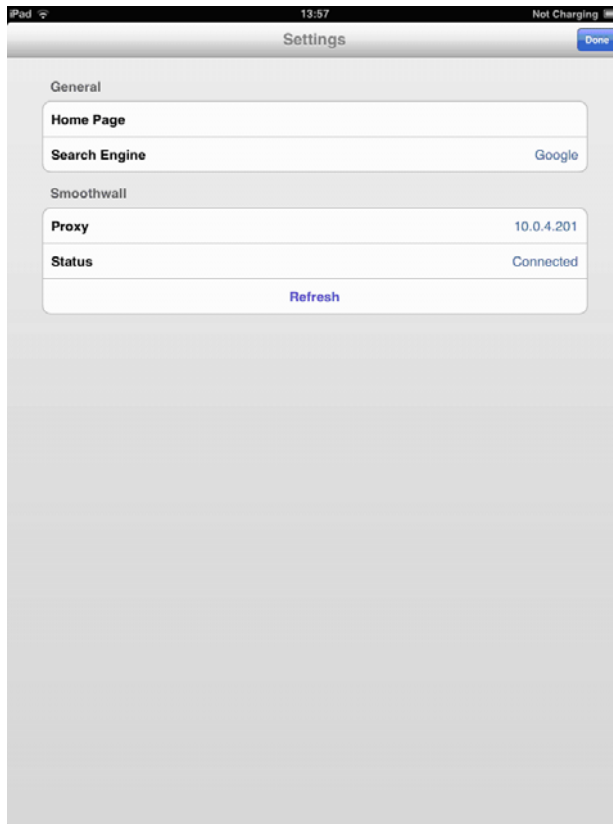


8. Locate and start MobileGuardian iOS.

The MobileGuardian iOS Home screen opens:



9. Click the Settings icon. The Settings screen is displayed:



10. Optionally, configure the following settings:
- Home page — Enter a home page to use on the device
 - Search engine — Select a search engine. Currently, the possible options are Google™, Yahoo™, and Bing™.
11. Click **Done** to save the settings.

12. In a browser on the device, go to `www.google.com`, the following screen is displayed:



13. Enter a valid Smoothwall System username and password and click **Login**.

4 Troubleshooting Smoothwall Connect Filter

This chapter describes typical issues with Smoothwall Connect Filter, and provides guidance for resolving them.

Browser User Agents

If a browser on the device displays strange page behavior, for example Google Docs not loading or web sites not being able to determine what browser is being used, you can hard code the browser user agent key.

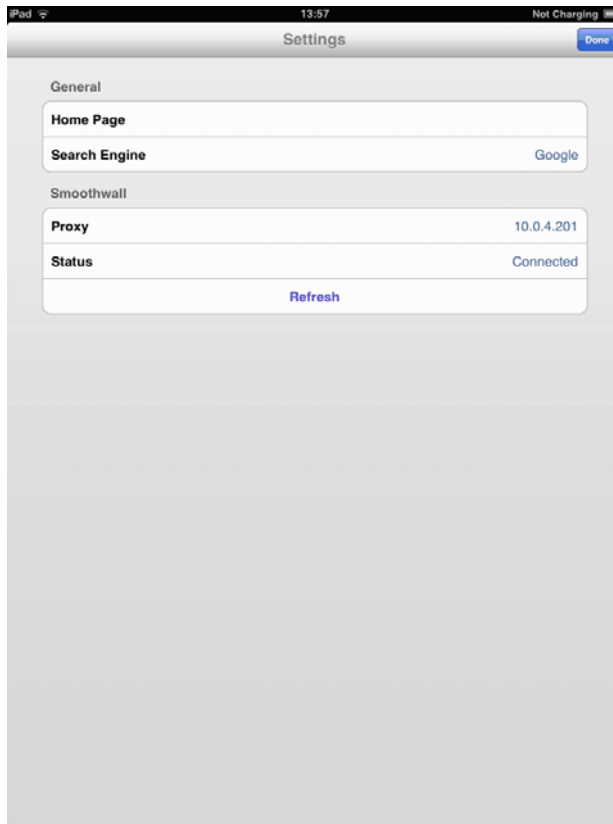
This setting is not visible by default in the plist file and is only required to work around web site incompatibility with non industry standard browsers.

To hard code a browser user agent:

1. In the plist file, enter the following:

```
<key>userAgent</key> <string>Mozilla/5.0 (iPhone; CPU OS 5_0_1 like Mac X) MobileGuardian/1.0</string> </dict> </plist>
```
2. Save and close the file. Transfer the file to the device.
3. Locate and start Smoothwall iOS on the device.
4. On the Smoothwall iOS Home screen, click the Settings icon.

5. The Smoothwall iOS Settings screen is displayed:



6. Click **Refresh** to apply the change to the plist file and restart Smoothwall iOS.
7. Click **Done**.

Index

B

browser user agents 15

C

client key 7

I

installing 9

M

MobileProxy 5
 configuring 5
 enable 5

P

prerequisites 5

S

Smoothwall Connect Filter 3

T

troubleshooting
 browser user agents 15

U

user credentials 8
username 8

smoothwall[®]

The Web You Want