smoothwall®

The Web You Want

Secure Web Gateway

MobileGuardian Client Administration Guide

For future reference

MobileGuardian Client serial number:

Date installed:

Smoothwall contact:

Smoothwall® MobileGuardian Client, Administration Guide, June 2014

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

For more information, contact: docs@smoothwall.net

Trademark notice

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.

MobileGuardian Client 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

1 Working with MobileGuardian Client

In this chapter:

- Who should read this guide
- What documentation and help is available
- An overview of MobileGuardian Client when installed on users' devices.

Who should read this guide?

System administrators maintaining and deploying MobileGuardian Client should read this guide.

Note: We strongly recommend that everyone working with Smoothwall products attend Smoothwall training. For information on our current training courses, see http://www.smoothwall.net/support/training/

Documentation

Apart from this guide, the following documentation is available:

- the *MobileGuardian Client Installation Guide*
- your *Smoothwall System Administrator's Guide*

About MobileGuardian Client

MobileGuardian Client provides web security by enforcing your organization's web security policy on mobile devices. A web security policy, containing filters and, optionally, time settings, determines how MobileGuardian Client handles web content and downloads to best protect your users and your organization.

Before You Start

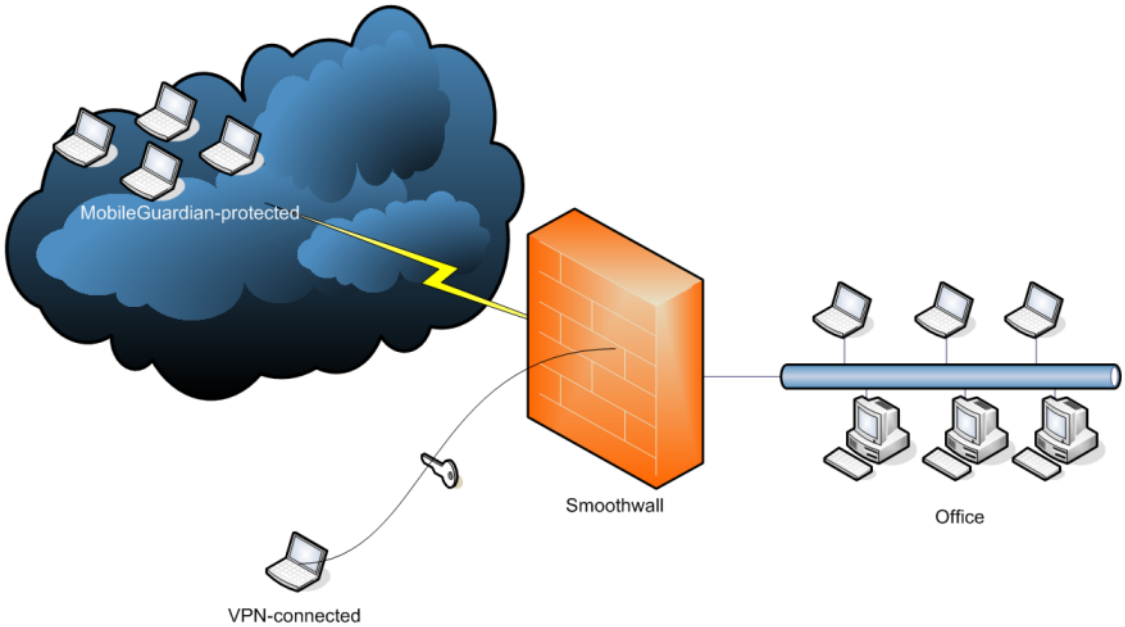
As documented in the *MobileGuardian Client Installation Guide*, before MobileGuardian Client can start protecting the device it is installed on, the following must be configured on your Smoothwall System:

- A group containing the users who will be using MobileGuardian Client on their devices
- Mobile settings specifying the group's username and password
- Mobile proxy settings specifying how and where devices will get their web content filtering.

For more information, see your *Smoothwall System Administrator's Guide*.

How it Works

The following graphic and section give an overview of what happens when MobileGuardian Client is installed on a mobile device and your Smoothwall System is configured to supply blocklists and a web content security policy for mobile devices.



At boot up, a MobileGuardian Client-protected device checks its location by trying to contact your Smoothwall System. If the check is successful, MobileGuardian Client knows that the device is either on-site or has external access, e.g. via VPN, and it downloads the latest blocklists and filtering policy and uploads access logs. This cycle is repeated every time the device is booted.

After the boot up cycle, MobileGuardian Client checks its location every 60 seconds, then applies the client proxy settings determined by both the client-side proxy exceptions settings and the server-side location-based proxy settings. If it finds your Smoothwall System, it downloads any new settings and blocklist updates available once every hour and it sends its logs to your Smoothwall System once every 24 hours at midnight.

If the location check is unsuccessful, i.e. the device has no connectivity with your Smoothwall System then MobileGuardian Client takes no further action and repeats the location check every 60 seconds.

By default, MobileGuardian Client provides content filtering for the device. You can of course, configure this. For more information, see your *Smoothwall System Administrator's Guide*.

Checking MobileGuardian Client's Status

To access status information:

1. In the device's system tray, right-click on the MobileGuardian Client icon and select **Status**. MobileGuardian Client displays the current status, for example:

Configuring Proxying

By default, MobileGuardian Client proxies all web traffic on the device. It is, however, possible to configure proxy exceptions for specific hostnames or IP addresses depending on where the device is located. It is also possible to disable proxying completely.

Tip: Check the `setproxy` log file to see current information on how proxying is configured. See *About Log Files* on page 4 for more information on logging in MobileGuardian Client.

Configuring Proxy Exceptions

Configuring proxy exceptions entails editing global, mobile or proxy settings.

To configure a proxy exception:

1. On the MobileGuardian Client-protected device, start Windows Explorer, browse to where MobileGuardian Client is installed and open the `setproxy` directory. The following files are available:

File	Description
global	Exceptions listed in this file are always applied, except when using automatic configuration with PAC or WPAD. See your *Smoothwall System Administrator's Guide* for more information.
mobile	Exceptions listed in this file are added to the exceptions listed in the global file when content is filtered by MobileGuardian Client.
proxy	Exceptions listed in this file are added to the exceptions listed in the global file when content is filtered by a manually specified proxy.

2. Using a text editor, open the file that matches your proxy exception requirements and enter each proxy exception on a separate line with no spaces. There is no need to delimit them with a semi colon. For example:

   ```
   192.168.*.*
   ```

   ```
   *.example.com
   ```

3. Save the file and repeat the step above with the other files to configure any other exceptions you require.

The next time MobileGuardian Client checks its location, the exceptions will be implemented.

Disabling Proxying

By default, MobileGuardian Client does not allow normal users to change their browsers' proxy settings. If a user with administrative privileges wants to manually configure proxy settings for rollout, trouble shooting and diagnostics purposes, MobileGuardian Client must be stopped from enforcing proxy settings by using the `disable_setproxy` configuration.

To stop MobileGuardian Client from enforcing proxy settings:

1. On the MobileGuardian Client-protected device, start Windows Explorer, browse to where MobileGuardian Client is installed and open the `setproxy` directory.
2. Using a text editor, open the `global` file and, on the first line, enter:

   ```
   disable_setproxy
   ```

3. Save the file. You can now edit the browser's proxy settings of the browser as required, without intervention from MobileGuardian Client.

Note: To re-enable proxy setting enforcement, in the `global` file, remove the `disable_setproxy` and save the file.

Logging and Reporting

The following sections discuss logging and reporting in MobileGuardian Client.

About Log Files

By default, on the device, MobileGuardian Client stores log files in `C:\Program Files\MobileGuardian\log` and creates a short cut to the log files on the Start > Programs menu.

Log files are rotated daily and MobileGuardian Client retains the log files until they are successfully uploaded to your Smoothwall System.

MobileGuardian Client uploads the log files at each reboot and every 24 hours if it can connect to your Smoothwall System. The log files are uploaded in chunks of 1Mb so that large log files, caused by an extended period of no access to the Smoothwall System, are uploaded a chunk at a time, minimizing the risk of failure.

For complete information on working with log files, see your *Smoothwall System Administrator's Guide*.

Reporting

On your Smoothwall System, all reports which apply to web filtering contain origin options. These enable you to create reports which show only logs which are applicable to devices running MobileGuardian Client. For more information, see your *Smoothwall System Administrator's Guide*.

Limitations when Deploying Web Security

Currently, MobileGuardian Client does not support the following when creating and applying a web content filtering policy to devices.

- SSL interception
- Anti-virus scanning
- Upstream proxies
- Uploaded HTML templates and custom intranet block pages.

About MobileGuardian Client and End-users

Users cannot remove MobileGuardian Client unless they are using accounts with administrator privileges.

We recommend that:

- You tell users that MobileGuardian Client has been installed on their devices and that web content is being filtered and their browsing is being logged
- You provide users with a way of reporting problems with over and/or under-blocking of pages so that you can adjust your policy to suit your organization better.

smoothwall®

The Web You Want