

# smoothwall®

The Web You Want

## Secure Web Gateway

### MobileGuardian Installation and Administration Guide

**For future reference**

MobileGuardian serial number:

Date installed:

Smoothwall contact:

## Smoothwall® MobileGuardian, Installation and 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.

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.

MobileGuardian contains graphics taken from the Open Icon Library project <http://openiconlibrary.sourceforge.net/>

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

# Contents

<b>Chapter 1</b>	<b>Introducing MobileGuardian .....</b>	<b>1</b>
	About MobileGuardian.....	1
	How it Works .....	1
	About MobileGuardian and End-users.....	2
<b>Chapter 2</b>	<b>Installing MobileGuardian .....</b>	<b>3</b>
	Before Installing .....	3
	Installing MobileGuardian .....	3
<b>Chapter 3</b>	<b>Working with MobileGuardian Web Filter Policies. 5</b>	
	Web Security – Overview.....	5
	Overview of MobileGuardian.....	6
	Using the Default Policies .....	6
	About Applying Web Filter Policies – which one first?.....	7
	Applying a Customized Web Filter Policy.....	8
	Defining New Content .....	8
	About Weighted Phrases and Search Terms .....	10
	About Absolute Phrases and Search Terms.....	10
	Configuring Content Filtering Settings .....	11
	Configuring Time Slots.....	12
	Applying a Web Filter Policy .....	12
<b>Chapter 4</b>	<b>Deploying MobileGuardian.....</b>	<b>17</b>
	Configuring Mobile Settings .....	17
	Configuring Mobile Proxy Settings.....	18
	Configuring Proxying Exceptions.....	19
	Disabling Proxying .....	20
	Reviewing Client Status .....	20
	Logging and Reporting .....	21
	About Log Files .....	21
	Reporting .....	21
	Managing Block Pages.....	22

	<b>Configuring a Block Page .....</b>	<b>22</b>
	<b>Using an Intranet Page as a Block Page .....</b>	<b>23</b>
	<b>Managing Locations .....</b>	<b>24</b>
	<b>Adding Content to Locations.....</b>	<b>24</b>
	<b>Adding Location Contents Directly .....</b>	<b>24</b>
	<b>Uploading Content Information .....</b>	<b>25</b>
	<b>Editing Location Contents .....</b>	<b>25</b>
	<b>Deleting Location Contents .....</b>	<b>26</b>
	<b>Deleting Locations.....</b>	<b>26</b>
<b>Chapter 5</b>	<b>Installing MobileGuardian on Devices .....</b>	<b>27</b>
	<b>Installing MobileGuardian on Devices .....</b>	<b>27</b>
	<b>Pre-requirements.....</b>	<b>27</b>
	<b>On Devices.....</b>	<b>27</b>
	<b>On Your Smoothwall System .....</b>	<b>28</b>
	<b>Installing MobileGuardian – Automated .....</b>	<b>28</b>
	<b>Installing Using a Transform .....</b>	<b>28</b>
	<b>Installing Using a Boot-up Script .....</b>	<b>29</b>
	<b>Manually Installing Clients .....</b>	<b>29</b>
	<b>Interactively Installing MobileGuardian .....</b>	<b>29</b>
	<b>Installing MobileGuardian from the Command Line .....</b>	<b>30</b>
	<b>Connecting for the First Time – the Certificate .....</b>	<b>31</b>
	<b>Checking MobileGuardian’s Status.....</b>	<b>31</b>
	<b>Removing MobileGuardian.....</b>	<b>32</b>
	<b>Removing MobileGuardian Using AD .....</b>	<b>32</b>
	<b>Manually Removing MobileGuardian .....</b>	<b>32</b>
	<b>Upgrading MobileGuardian .....</b>	<b>32</b>
	<b>About MobileGuardian and End-users.....</b>	<b>32</b>

# 1 Introducing MobileGuardian

In this chapter:

- An introduction to MobileGuardian, Smoothwall's add-on module for providing web filtering for mobile devices.

## About MobileGuardian

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

## How it Works

At boot up, a MobileGuardian-protected device checks its location by trying to contact your Smoothwall System. If the check is successful, MobileGuardian 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 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, MobileGuardian takes no further action and repeats the location check every 60 seconds.

# About MobileGuardian and End-users

Users cannot remove MobileGuardian from their device unless they are using accounts with administrator privileges.

We recommend that:

- You tell users that MobileGuardian 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.

# 2 Installing MobileGuardian

In this chapter:

- How to install MobileGuardian.

## Before Installing

You install MobileGuardian by adding it to your Smoothwall System. For information on working with Smoothwall products, see the Administrator's Guide delivered with your product.

### Before installing MobileGuardian:

1. Start a web browser, access your Smoothwall System, authenticate yourself and navigate to **System > Maintenance > Updates** page.
2. Click **Refresh updates list** to check that you have all the latest updates installed on your Smoothwall System.
3. If there are any updates available, download and install them. See your *Smoothwall System Administrator's Guide* if you need more information.

## Installing MobileGuardian

After checking that you have the latest updates installed, you are ready to install MobileGuardian.

---

**Note:** Guardian3 must be installed and working before you install MobileGuardian.

---

### To install MobileGuardian:

1. Navigate to the **System > Maintenance > Modules** page.
2. In the **Available modules** list, select **MobileGuardian** and click **Install**. Your Smoothwall System installs MobileGuardian.

3. Navigate to the **System > Maintenance > Shutdown** page.
4. Select **Immediately** and click **Reboot**. The rebooting page opens.
5. When your Smoothwall System has rebooted, authenticate yourself and log in.

You are now ready to begin working with MobileGuardian. For more information, see the chapters that follow.



# 3 Working with MobileGuardian Web Filter Policies

In this chapter:

- An overview of MobileGuardian and its default web filter policies
- How to create and apply a customized policy.

## Web Security – Overview

MobileGuardian provides web security by providing default web filter policies which you deploy on mobile devices. The policies determine how MobileGuardian handles web content and downloads to best protect your users and your organization.

You can also create and apply a custom web filter policy to fit your organization. For more information, see *Applying a Customized Web Filter Policy* on page 8.

# Overview of MobileGuardian

The following table describes the pages used to configure and work with MobileGuardian.

Page	Description
<b>Manage policies</b>	This is where you apply policies by assigning actions to matched content. For more information, see <i>Using the Default Policies</i> on page 6 and <i>Applying a Web Filter Policy</i> on page 12.
<b>Category groups</b>	This is where you configure filters for matching web content. For more information, see <i>Configuring Content Filtering Settings</i> on page 11.
<b>Content categories</b>	This is where you define and edit custom content and security rules for inclusion in filters. For more information, see <i>Defining New Content</i> on page 8.
<b>Time slots</b>	This is where you create and edit time slots to specify when filtering policies are applied. For more information, see <i>Configuring Time Slots</i> on page 12.
<b>Block page</b>	This is where you can customize the page(s) that MobileGuardian displays when it blocks web content. For more information, see <i>Chapter 4, Managing Block Pages</i> on page 22.
<b>Locations</b>	This is where you create locations into which you can place contents such as desktop and laptop computers. For more information, see <i>Chapter 4, Managing Locations</i> on page 24.
<b>Mobile settings</b>	This is where you configure the password used for connections between MobileGuardian-protected devices and your Smoothwall System. For more information, see <i>Chapter 4, Configuring Mobile Settings</i> on page 17.
<b>Mobile proxy</b>	This is where you configure which proxy MobileGuardian clients should use based on their location. For more information, see <i>Chapter 4, Configuring Mobile Proxy Settings</i> on page 18.
<b>Mobile client status</b>	This is where you view MobileGuardian client status. For more information, see <i>Reviewing Client Status</i> on page 20 and <i>Removing MobileGuardian</i> on page 32.

## Using the Default Policies

MobileGuardian contains a number of preconfigured web security policies which are designed to provide comprehensive web security. The policies are:

Policy	Description
<b>Windows updates</b>	Always allows Microsoft Windows updates to be downloaded.
<b>Reduce overblocking</b>	Always reduces excessive blocking of content.
<b>Custom allowed content</b>	Always allows content specified on the Guardian > Filtering > User defined page.
<b>Lunchtime allowed sites</b>	Allows access to social and web mail sites specified on the MobileGuardian > Policy objects > Category groups page at the time specified as lunchtime on the MobileGuardian > Policy objects > Time slots page. <b>Note:</b> This option is disabled by default. When enabled, it will override some of the content blocked by the default AUP policy.
<b>Default AUP</b>	Blocks pornography, malware, time-wasting and other generally undesirable sites specified on the MobileGuardian > Policy objects > Category groups page.
<b>Custom blocked content</b>	Always blocks access to content specified on the MobileGuardian > Policy objects > Category groups page.
<b>Adverts</b>	Always blocks advertisements.
<b>Recommended security rules</b>	Always applies security rules to cover recent browser exploits.
<b>Force SafeSearch</b>	Enforces the use of SafeSearch on supported search engines.

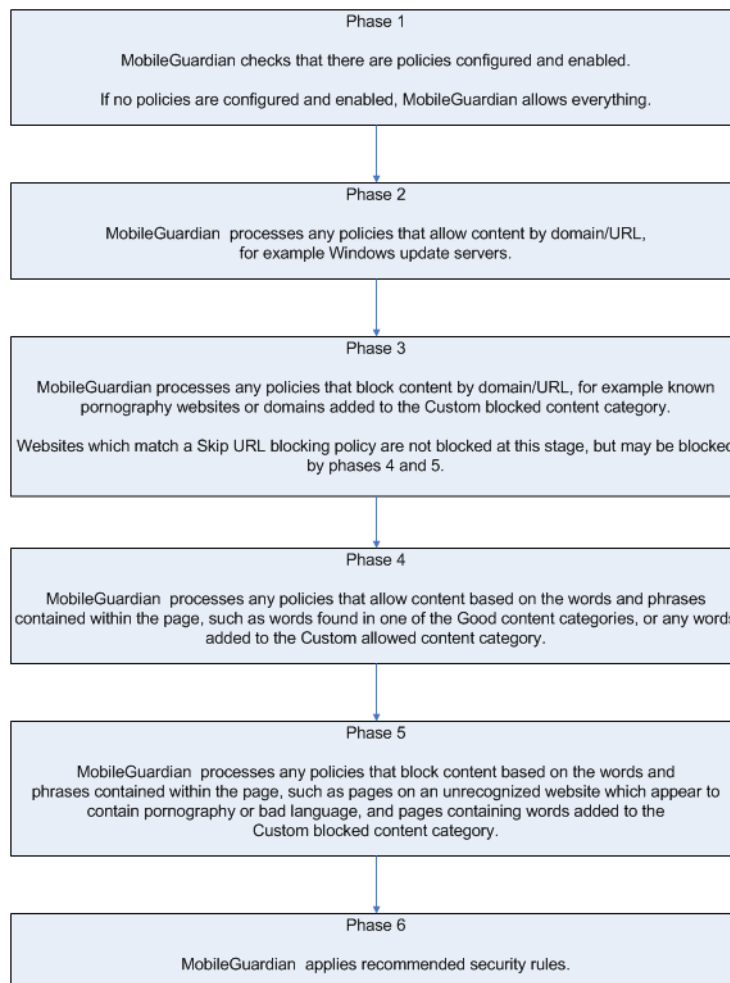
Policy	Description
<b>File security</b>	Always blocks download access to file types classified as not secure.
<b>Everything</b>	Categorizes all non-blocked requests using domain and URL lists.

To use these policies on mobile devices, you only need to configure your Smoothwall System settings, see *Chapter 4, Configuring Mobile Settings* on page 17 and install MobileGuardian on the mobile devices you want to protect, see *Chapter 5, Installing MobileGuardian on Devices* on page 27.

If you require other protection, you can create a custom policy. For more information, see *Applying a Customized Web Filter Policy* on page 8.

## About Applying Web Filter Policies – which one first?

MobileGuardian applies web filter policies based on what the policies have been defined to do. The following graphic lists how the process works:



# Applying a Customized Web Filter Policy

You can configure and apply a custom MobileGuardian web filter policy to specify the content you want to allow or block and time and authentication settings to be applied on mobile devices.

Applying a customized web filter policy entails:

- Consulting your organization's Acceptable Usage Policy (AUP) to draw up a policy to determine what is and is not acceptable usage of the Internet by users
- Optionally, defining new categories, see *Defining New Content* on page 8
- Configuring filtering settings, for more information, see *Configuring Content Filtering Settings* on page 11
- Setting when a policy applies, see *Configuring Time Slots* on page 12
- Applying the policy, see *Applying a Web Filter Policy* on page 12.

## Defining New Content

You can define new content for inclusion in filters to suit the web security requirements of your organization.

### To define new content:

1. Navigate to the **MobileGuardian > Policy objects > User defined** page.

The screenshot shows the Smoothwall MobileGuardian web interface. The top navigation bar includes the Smoothwall logo, the tagline 'The Web You Want', and 'Help' and 'Logout' buttons. The breadcrumb trail reads 'MobileGuardian » Policy objects » User defined'. Below this, there are links for 'Category groups', 'User defined', 'Time slots', 'Block page', and 'Locations'. The main content area is titled 'Filter Type selection' and shows 'Filter Type: Content and URL filtering' with an 'Update' button. Below this is the 'Manage custom content' section, which includes fields for 'Name', 'Comment', and 'Domains and URLs', along with 'Advanced' and 'Add' buttons. At the bottom, there is a 'Custom content categories' table.

Name	Filter Type	Mark
Custom allowed content	Content and URL filtering	<input type="checkbox"/>
Custom blocked content	Content and URL filtering	<input type="checkbox"/>

Remove Edit

2. Select from the following filter type:

Option	Description
<b>Content and URL filtering</b>	Enables you to add domains, URLs, phrases and regular expression URLs to content categories.
<b>File security</b>	Enables you to specify types of files and MIME types that MobileGuardian should block.
<b>Content security</b>	Enables you to remove or substitute content within the URL, the HTTP header, or the page. This can be used to remove malicious or undesirable content as appropriate.

3. Click **Update** and configure the following settings:

Setting	Description
<b>Name</b>	Enter a name for the new content.
<b>Comment</b>	Optionally, enter a comment to make it easier to remember what the category does.

4. Depending on the filter type you have selected, you can configure the following:

Filter type	Description
<b>Custom URLs and content</b>	<p>Enables you to add domains, URLs, phrases and regular expression URLs to content.</p> <p><b>To add custom URLs and content:</b></p> <ol style="list-style-type: none"> <li>In the Domains and URLs area, enter one domain or URL per line. For example: <code>madeup . com</code>. Do not include <code>www .</code> in URLs.</li> <li>Optionally, click <b>Advanced</b> to access more options.</li> <li>In the Absolute and weighted phrases area, enter one phrase per line for example:  <code>( hardcore )</code>  <code>( xxx )</code>            Spaces before and after a phrase are not removed, simplifying searching for whole words.             Parenthesis are required. For more information, see <i>About Weighted Phrases and Search Terms</i> on page 10 and <i>About Absolute Phrases and Search Terms</i> on page 10.</li> <li>In the Regular expression URLs area, enter one regular expression URL per line, for example:  <code>(adultsite sexdream)</code>            The example given above blocks URLs containing either the word <code>adultsite</code> or the word <code>sexdream</code>. Parentheses are a product of regular expression syntax, not a requirement as with absolute and weighted phrases.</li> <li>In the Absolute and weighted search terms area, enter one search term per line for example:  <code>( hardcore )</code>  <code>( xxx )</code>            Spaces before and after a term are not removed, simplifying searching for whole words.             Parenthesis are required. For more information, see <i>About Weighted Phrases and Search Terms</i> on page 10 and <i>About Absolute Phrases and Search Terms</i> on page 10.</li> </ol>

Filter type	Description
<b>Custom file extensions and MIME types</b>	<p>Enables you to specify types of files and MIME types that MobileGuardian should block.</p> <p><b>To add custom file extensions and MIME types:</b></p> <ol style="list-style-type: none"> <li>In the File extensions and MIME types area, enter one file extension, e.g. <code>.doc</code>, or MIME type, e.g. <code>application/octet-stream</code> per line. You must include the dot in file extensions.</li> </ol>
<b>Custom content security rules</b>	<p>Enables you to remove or substitute content within the URL, the HTTP header, or the page. This can be used to remove malicious or undesirable content as appropriate.</p> <p><b>To add custom content:</b></p> <ul style="list-style-type: none"> <li>In the Content security rules area, enter one replacement rule per line. The format is: <code>bad phrase-&gt;*censored*</code></li> <li>In the URL security rules area, enter one replacement rule per line. The format is: <code>http://(www)?example.com-&gt;http://www.example.net</code></li> <li>In the Outgoing HTTP header security rules area, enter one replacement or blocking rule per line. Example of a replacement rule: <code>Cookie: adult=yes-&gt;Cookie: adult=no</code> Example of a blocking rule: <code>User-agent: .*MSIE 5.*</code> Prevents users from using Internet Explorer 5.</li> </ul>

- Click **Add**. The category is added to the list of current categories and made available on the **MobileGuardian > Policy objects > Category groups** page in the User defined group of content.

## About Weighted Phrases and Search Terms

A weighted phrase or search term is a phrase or term which, when present in content or in a search term entered by a user, makes it more or less likely that MobileGuardian will block the content or result of the search.

For example, `(myspace) (10)` adds ten points to the score of any content containing the word `myspace`, if the associated policy action is block. If the action is allow, ten points will be subtracted from the score.

Collections of weighted phrases and search terms loosely define a category. For example, several pornography-related phrases found together would, when their scores are added up, cause the content to be blocked under the pornography category, assuming the total score is above the trip limit.

## About Absolute Phrases and Search Terms

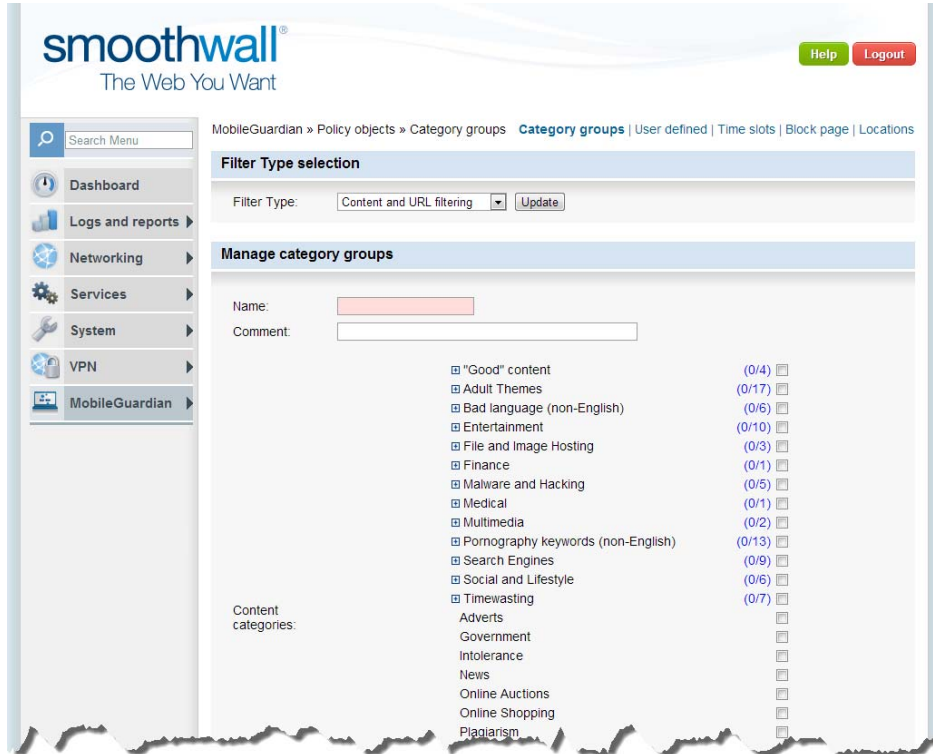
Absolute phrases and search terms define content and search results which you want MobileGuardian to block or allow outright. A single occurrence of an absolute phrase in the content or search term in a search query will cause MobileGuardian to block or allow the content or result of the search, depending on the policy action.

# Configuring Content Filtering Settings

The following section explains how to configure the content filters to be used in a web filter policy.

**To configure filtering settings:**

1. Navigate to the **MobileGuardian > Policy objects > Category groups** page.



2. From the drop-down menu, select the type of filter you want to use. The following options are available:

Setting	Description
<b>Filter type</b>	<p><b>Content and URL filtering</b> – Lists of phrases, domains and URLs used to categorize content.</p> <p><b>File security</b> – Filters which analyze and categorize files and MIME types when downloaded.</p> <p><b>Content security</b> – Filters which identify and stop malicious content embedded in web pages from being downloaded.</p>

3. Click **Update**. Depending on the type of filter you have selected, your Smoothwall System displays the categories available.
4. Configure the following settings:

Setting	Description
<b>Name</b>	Enter a name for the filter.
<b>Comment</b>	Optionally, enter a comment to make it easier to remember what the filter does.

5. Select the content you want to add to the filter to provide web security.
6. Click **Add**. The filter is saved and added to the current list of filters available.

## Configuring Time Slots

You can configure MobileGuardian to allow or stop users accessing the Internet during certain time slots depending on the time and day.

### To configure a time slot:

1. Navigate to the **MobileGuardian > Policy objects > Time slots** page.

2. Configure the following settings:

Setting	Description
<b>Name</b>	Enter a name for the time slot.
<b>Comment</b>	Optionally, enter a comment to help identify when the time slot is used.
<b>Active from</b>	From the drop-down list, select at what hour and minute the time slot starts.
<b>Active to</b>	From the drop-down list, select at what hour and minute the time slot ends.
<b>Days active</b>	Select the days of the week on which this time slot applies.

3. Click **Add**. The time slot is added to the list of current time slots and made available on the MobileGuardian > Web filter policies > Manage policies page on the Time Slot drop-down list.

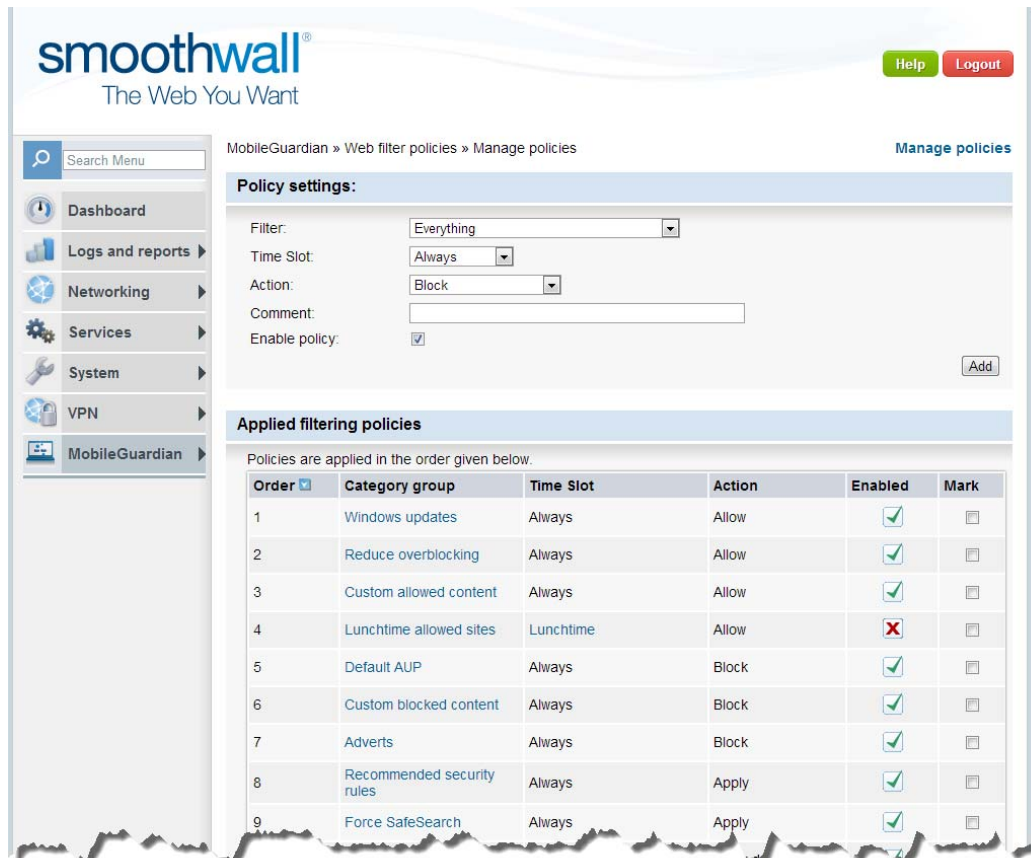
## Applying a Web Filter Policy

The following section explains how to apply a web filter policy.



**To apply a policy:**

1. Navigate to the **MobileGuardian > Web filter policies > Manage policies** page.



smoothwall®  
The Web You Want

Help Logout

MobileGuardian » Web filter policies » Manage policies Manage policies

**Policy settings:**

Filter:

Time Slot:

Action:

Comment:

Enable policy:

**Applied filtering policies**

Policies are applied in the order given below.

Order	Category group	Time Slot	Action	Enabled	Mark
1	Windows updates	Always	Allow	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Reduce overblocking	Always	Allow	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Custom allowed content	Always	Allow	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Lunchtime allowed sites	Lunchtime	Allow	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Default AUP	Always	Block	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	Custom blocked content	Always	Block	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	Adverts	Always	Block	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	Recommended security rules	Always	Apply	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	Force SafeSearch	Always	Apply	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## 2. Configure the following settings:

Settings	Description
<b>Filter</b>	<p>Select the type of filtering, custom or default, required for devices. The following options are available:</p> <p><b>Everything</b> – Applies the policy action selected to all content.</p> <p><b>URLS containing an IP address</b> – Applies the policy action selected to any site whose address is specified using an IP address.</p> <p><b>All HTTPS content</b> – Applies the policy action selected to all content requested using the secure HTTP protocol.</p> <p><b>HTTPS URLs containing an IP address</b> – Applies the policy action selected to to any site whose address is specified using an IP address and the HTTPS protocol.</p> <p><b>Custom blocked content</b> – Applies the policy action selected to content specified on the MobileGuardian &gt; Policy objects &gt; User defined page.</p> <p><b>Reduce overblocking</b> – A filter used in the default web filter policy supplied with MobileGuardian to reduce excessive blocking of content.</p> <p><b>Lunchtime allowed sites</b> – A filter used in the default web filter policy supplied with MobileGuardian, containing social, time wating and and web mail sites that could be allowed at lunchtime.</p> <p><b>Default AUP</b> – A filter used in the default web filter policy supplied with MobileGuardian, applies a comprehensive acceptable usage policy (AUP).</p> <p><b>Windows updates</b> – A filter used in the default web filter policy supplied with MobileGuardian, ensures Windows updates are never blocked.</p> <p><b>Custom allowed content</b> – Applies the policy action selected to content specified on the MobileGuardian &gt; Policy objects &gt; User defined page.</p> <p><b>Adverts</b> – A filter used in the default web filter policy supplied with MobileGuardian which blocks advertising servers and URLs.</p> <p><b>File security</b> – A filter used in the default web filter policy supplied with MobileGuardian, blocks dangerous, time wasting and/or bandwidth wasting files</p> <p><b>Recommended security rules</b> – A filter used in the default web filter policy supplied with MobileGuardian which detects and prevents browser exploits.</p> <p><b>Force SafeSearch</b> – A filter which enforces the use of SafeSearch on supported search engines.</p> <p>For more information on filters, see <i>Configuring Content Filtering Settings</i> on page 11 and <i>Defining New Content</i> on page 8.</p>
<b>Time Slot</b>	<p>Accept <b>Always</b>, the default time period, or, from the drop-down list, select a time slot you have configured. For more information on time periods, see <i>Configuring Time Slots</i> on page 12.</p>

Settings	Description
<b>Action</b>	<p>Select the action you want the policy to perform. Depending on the type of filter you have selected, the following options are available:</p> <p><b>Content and URL filtering:</b></p> <ul style="list-style-type: none"> <li>• <b>Block</b> – If MobileGuardian identifies the content or URL as being listed in the filter, users will be denied access.</li> </ul> <p><b>Note:</b> If soft blocking is enabled, devices will be able to access the content after being warned that it is potentially objectionable. For more information on soft blocking, see the Web filter blocking mode option below.</p> <ul style="list-style-type: none"> <li>• <b>Block (URLs only)</b> – Blocks domains and URLs in the chosen filter, but not phrases.</li> <li>• <b>Allow</b> – Content is allowed to pass unhindered through the filter.</li> <li>• <b>Skip URL blocking</b> – Select when you want to allow a URL listed on a blocklist but still subject the site to phrase filtering.</li> <li>• <b>Categorize</b> – If MobileGuardian identifies the content or URL as being listed in the filter, the user will be allowed access, but the site’s category will be recorded in the access log.</li> </ul> <p><b>File security filtering:</b></p> <ul style="list-style-type: none"> <li>• <b>Allow downloads</b> – File and MIME types specified in the filter are allowed to pass through MobileGuardian subject to any anti-malware protection in place.</li> <li>• <b>Block downloads</b> – File and MIME types specified in the filter are blocked.</li> </ul> <p><b>Content security filtering:</b></p> <ul style="list-style-type: none"> <li>• <b>Apply</b> – Content is filtered according to the content security filter selected. Objectionable content will be sanitized and hazardous content removed.</li> </ul>
<b>Comment</b>	Optionally, enter a comment to make it easier to remember what the policy does.
<b>Enable policy</b>	Select this option to enable the policy.

3. Click **Add**. The policy is added to the list of current filtering policies.

4. Navigate to the URL filter settings area and configure the following settings:

Setting	Description
<b>URL filter settings</b>	<p>Configure MobileGuardian to identify URLs within URLs and define how links to banned sites affect weighting.</p> <p><b>Perform a deep URL analysis on sites</b> – Checks for banned URLs embedded within larger URLs.</p> <p><b>Apply weight to banned sites and URLs</b> – Whenever a link to something banned by domain or URL, not content, is found, the chosen amount is added to the content's score, making it more likely to reach the limit and be blocked.</p> <p>For example, a page containing images which act as links to known pornography sites is not likely to be blocked by phrases – it may contain very little text – but with this option selected, MobileGuardian can block it for containing those links.</p> <p><b>User-specified additional weight</b> – Enter any additional weight you want to add.</p>

5. Optionally, click **Advanced** to access the following settings:

Setting	Description
<b>Web filter blocking mode</b>	<p>Select <b>Allow users to bypass content block</b> to enable soft blocking and present users with a block page which warns them that the page they are trying to access contains potentially offensive or restricted material.</p> <p>Users can then decide to proceed and bypass the block page or to browse to a different page.</p>
<b>Dynamic Content Analysis settings</b>	<p>Enables you to fine tune MobileGuardian's dynamic analysis of content and set the trip limit appropriately.</p> <p><b>Enable dynamic content analysis</b> – By default, dynamic content analysis is enabled. To disable it, deselect this option.</p> <p><b>Enable search term filtering</b> – When enabled, MobileGuardian filters search terms entered into Google and Yahoo search engines and blocks unsuitable searches. You can add terms to the list of terms, see <i>Defining New Content</i> on page 8 for more information.</p> <p><b>Content weight limit</b> – From the drop-down list, select the threshold for the weighted phrase; anything scoring above this is blocked, or select User specified to enter a custom limit.</p> <p><b>User-specified content weight limit</b> – If you have selected the User-specified weight option for the limit, enter the limit you require.</p>

6. Click **Save**. MobileGuardian will apply the policies to any mobile devices on which it is deployed. For information on deploying MobileGuardian, see *Chapter 4, Deploying MobileGuardian* on page 17.

# 4 Deploying MobileGuardian

In this chapter:

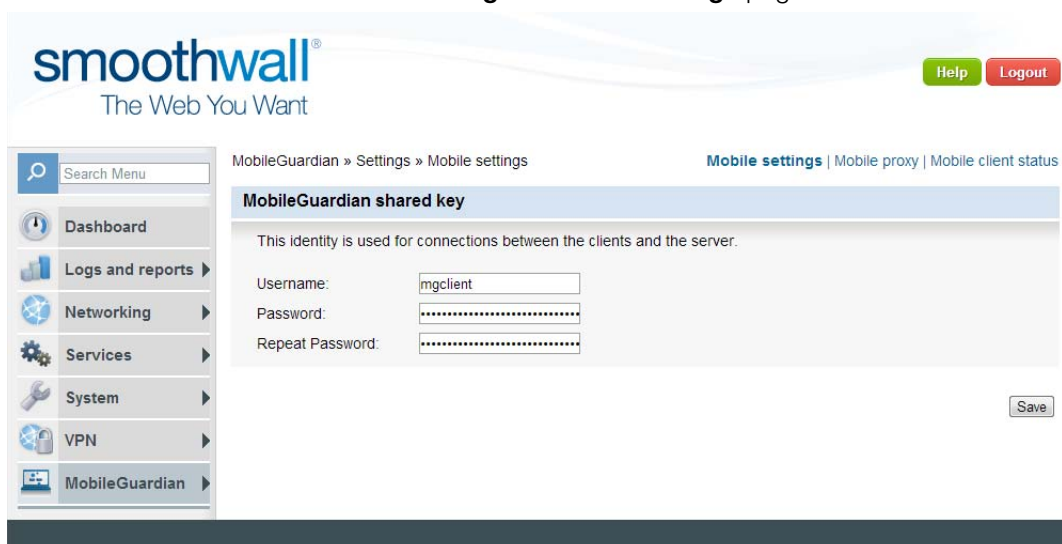
- Configuring your Smoothwall System to deploy and manage MobileGuardian on mobile devices.

## Configuring Mobile Settings

Your Smoothwall System uses mobile settings to authenticate MobileGuardian-protected devices when they attempt to access your Smoothwall System.

### To configure mobile settings:

1. Browse to the **MobileGuardian > Settings > Mobile settings** page.



The screenshot shows the Smoothwall web interface. At the top left is the Smoothwall logo with the tagline "The Web You Want". To the right are "Help" and "Logout" buttons. A navigation sidebar on the left includes "Search Menu", "Dashboard", "Logs and reports", "Networking", "Services", "System", "VPN", and "MobileGuardian". The main content area shows the breadcrumb "MobileGuardian » Settings » Mobile settings" and a sub-header "MobileGuardian shared key". Below this, a text box explains: "This identity is used for connections between the clients and the server." There are three input fields: "Username" (containing "mgclient"), "Password", and "Repeat Password". A "Save" button is located at the bottom right of the form area.

- Configure the following settings:

Setting	Description
<b>Username</b>	Enter a username for the device. This username is used to authenticate the device when it attempts to connect with your Smoothwall System.
<b>Password</b>	Enter a password for the device. This password is used to authenticate the device when it attempts to connect with your Smoothwall System.
<b>Repeat Password</b>	Re-enter the password to confirm it.

- Click **Save**. Your Smoothwall System saves the settings.

## Configuring Mobile Proxy Settings

You configure and apply settings to MobileGuardian-protected devices based on their location. For example, you can configure your Smoothwall System to take over content filtering from MobileGuardian whenever the device joins your branch office LAN and contacts your Smoothwall System.

**Note:** Well known and well defined networks are required in order to configure these settings successfully.

### To configure mobile proxy settings:

- Define the location from which MobileGuardian-protected devices will locate your Smoothwall System. For information on working with locations, see *Managing Locations* on page 24.

**Note:** When configuring a non-LAN location, the MobileGuardian client comms port must be accessible to machines in the defined network locations. You do this on the **System > Administration > External access** page.

When a VPN is used for devices to contact your Smoothwall System, the network location should be based on the IP addresses client devices will use when connected to that VPN, and external access to the MobileGuardian client comms port should be permitted on the required VPN interface.

- After creating the location, browse to the **MobileGuardian > Settings > Mobile proxy** page.

The screenshot shows the Smoothwall MobileGuardian administration interface. The breadcrumb path is "MobileGuardian » Settings » Mobile proxy". The page title is "Mobile settings | Mobile proxy | Mobile client status".

**Location based proxy settings**

Location:

Proxy type:

Address:

Comment:

Enable proxy:

**Location based proxies**

Location	Type	Address	Enabled	Mark

3. Configure the following settings:

Setting	Description
<b>Location</b>	From the drop-down menu, select the location of the protected device as created in <i>step 1.</i>
<b>Proxy type</b>	From the drop-down list, select how the device should get its web content filtering when at this location. The following options are available: <b>MobileGuardian client</b> – select this option if you want MobileGuardian to continue to provide content filtering when the device is at this location. <b>None</b> – select this option if transparent proxying is used at the location or if there is no proxy running. <b>Manually specified</b> – select this option to manually specify the proxy server which will provide content filtering when the device is at this location. <b>From Proxy PAC file</b> – select this option to use the settings in a proxy auto-config (PAC) file to determine the proxy server which will provide content filtering when the device is at this location.
<b>Address</b>	If you have chosen the <b>Manually specified</b> option above, enter the IP address and port or the hostname of the proxy server at this location, e.g. 192.168.72.1:800  If you have chosen the <b>From PAC file</b> option above, enter the location of the file, e.g. http://192.168.72.1/proxy.pac
<b>Comment</b>	Optionally, enter a comment describing the settings.
<b>Enable proxy</b>	Select to apply the settings and enable the proxy.

4. Click **Add**. Your Smoothwall System adds the settings to the list of current proxies.

## Configuring Proxying Exceptions

By default, MobileGuardian proxies all web traffic on the device it is protecting. 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. By default, MobileGuardian stores log files in `C:\Program Files\MobileGuardian\log` and creates a short cut to the log files on the Start > Programs menu.

---

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

### To configure a proxy exception:

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

File	Description
<b>global</b>	Exceptions listed in this file are always applied, except when using automatic configuration with PAC or WPAD. See your <i>Smoothwall System Administrator's Guide</i> for more information.
<b>mobile</b>	Exceptions listed in this file are added to the exceptions listed in the global file when content is filtered by MobileGuardian.

File	Description
<b>proxy</b>	Exceptions listed in this file are added to the exceptions listed in the global file when content is filtered by a manually specified proxy.

- 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
```

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

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

## Disabling Proxying

By default, MobileGuardian 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 must be stopped from enforcing proxy settings by using the `disable_setproxy` configuration.

### To stop MobileGuardian from enforcing proxy settings:

- On the MobileGuardian-protected device, start Windows Explorer, browse to where MobileGuardian is installed and open the `setproxy` directory.
- Using a text editor, open the `global` file and, on the first line, enter:  
`disable_setproxy`
- Save the file. You can now edit the device's browser's proxy settings as required, without intervention from MobileGuardian.

---

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

---

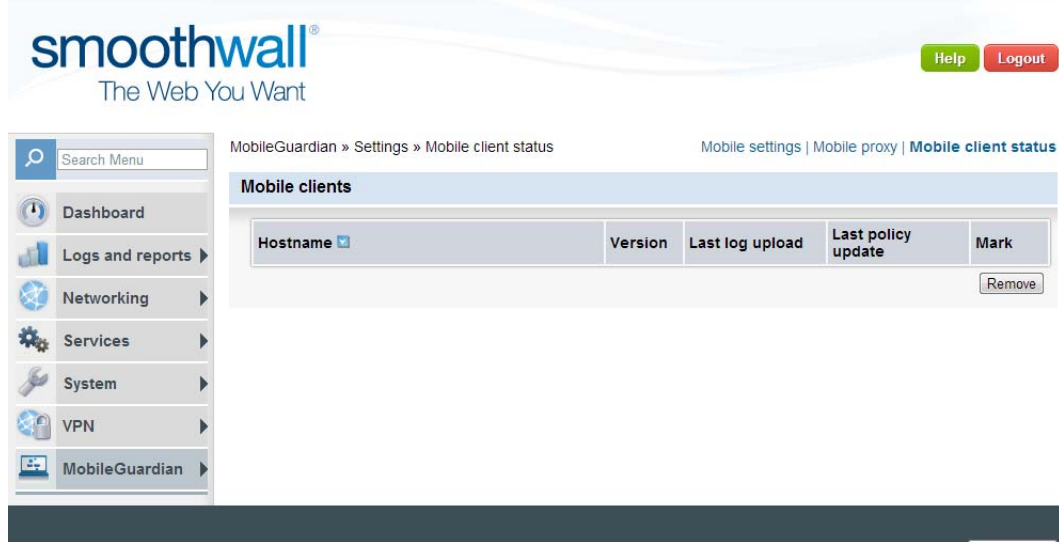
## Reviewing Client Status

You can review information on the devices which have MobileGuardian installed on them.



### To review MobileGuardian clients' status:

1. Browse to the **MobileGuardian > Settings > Mobile client status** page.



Your Smoothwall System displays hostname and version information on the MobileGuardian clients currently installed on devices. It also displays when the latest log files were uploaded to your Smoothwall System and when the latest content filtering policy was applied.

## Logging and Reporting

The following sections discuss logging and reporting in MobileGuardian.

### About Log Files

By default, MobileGuardian stores log files on the device 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 retains the log files until they are successfully uploaded to your Smoothwall System.

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

# Managing Block Pages

When an end-user's web request is blocked, MobileGuardian displays its default block page. You can configure MobileGuardian to display different types of block pages:

- A default block page which you can customize, for more information, see *Configuring a Block Page* on page 22
- An intranet page, for more information, see *Using an Intranet Page as a Block Page* on page 23.

## Configuring a Block Page

To configure the block page:

1. Navigate to the **MobileGuardian > Policy objects > Block page** page.

The screenshot shows the Smoothwall MobileGuardian administration interface. The breadcrumb path is MobileGuardian » Policy objects » Block page. The page is titled 'Block page type' and has two radio buttons: 'Built-in HTML Template' (selected) and 'Use Intranet Page'. There is an 'Update' button. Below this is the 'Upload built-in block page images' section, which includes fields for 'Custom title image (JPEG)', 'Custom title image size', 'Custom background image (JPEG)', and 'Custom background image size'. Each image field has a 'Choose File' button, a 'No file chosen' status, and 'Upload' and 'Remove' buttons. The 'Built-in block page settings' section includes text input fields for 'Message line 1', 'Message line 2', and 'E-mail address'. Below these are several checkboxes: 'Show email address', 'Show URL of blocked page', 'Show reason for block', 'Enable custom background image', 'Show client username', 'Show category matched', and 'Enable custom title image'. A 'Save' button is at the bottom right.

2. Configure the following settings:

Setting	Description
<b>Block page type</b>	<p>The options here determine what kind of block page to use. The following options are available:</p> <p><b>Built-in HTML Template</b> – Select to use MobileGuardian’s default block page.</p> <p><b>Use intranet page</b> – For more information on this option, see <i>Using an Intranet Page as a Block Page</i> on page 23.</p>
<b>Custom title image</b>	<p>This option determines the image displayed at the top of the block page.</p> <p><b>Note:</b> To use a custom title image, the image must be in 551 x 79 pixels in jpeg format.</p> <p><b>To specify a custom title image:</b></p> <ol style="list-style-type: none"> <li>1. Click <b>Browse</b>.</li> <li>2. In the dialog box that opens, browse to and select the image. Click <b>OK</b>.</li> <li>3. Click <b>Upload custom jpeg</b>.</li> </ol>

Setting	Description
<b>Custom background image</b>	This option determines the image displayed as a background to the block page. <b>Note:</b> To use a custom title image, the image must be in 551 x 552 pixels in jpeg format. <b>To specify a custom background image:</b> 1. Click <b>Browse</b> . 2. In the dialog box that opens, browse to and select the image. Click <b>OK</b> . 3. Click <b>Upload custom jpeg</b> .
<b>Message line 1</b>	Accept the default message, or enter a custom message explaining to the user what has happened.
<b>Message line 2</b>	Accept the default message, or enter a custom, secondary message.
<b>E-mail address</b>	Optionally, enter your Smoothwall System administrator's email address, for contact purposes.
<b>Show email address</b>	Optionally, select to display the administrator's email address.
<b>Show client username</b>	Optionally, select to display the users username, if applicable.
<b>Show URL of blocked page</b>	Optionally, select to display the URL of the blocked web request.
<b>Show category matched</b>	Optionally, select to display the filter category that caused the page to be blocked, if applicable.
<b>Show reason for block</b>	Optionally, select to display the reason why the web request was blocked.
<b>Enable custom title image</b>	Select this option if you have specified a custom title image, see above for more information.
<b>Enable custom background image</b>	Select this option if you have specified a custom background image, see above for more information.

- Click **Save** to implement your changes to the block page.

## Using an Intranet Page as a Block Page

MobileGuardian enables you to use an intranet page hosted elsewhere on your network as a block page.

### To configure an intranet page as the block page:

- Navigate to the **MobileGuardian > MobileGuardian > Block page** page and configure the following settings:

Setting	Description
<b>Block page type</b>	<b>Use intranet page</b> – Select to use an intranet page hosted elsewhere on your network.

- Click **Update**, your Smoothwall System updates the settings displayed.
- In the **Enter URL for block page field**, enter the URL for the intranet page.
- Click **Save** to use the block page you have specified.

# Managing Locations

Proxy settings are applied to MobileGuardian-protected devices based on the devices' location.

## To create a location:

1. Browse to the **MobileGuardian > Policy objects > Locations** page.
2. In the Manage locations area, click **New**. Your Smoothwall System creates the location and gives it a default name.
3. In the New name field, enter a custom name for the location and click **Rename**. Click **Save**. Your Smoothwall System renames the location.

## Adding Content to Locations

It is possible to add contents to a location by entering information directly or by uploading a csv file containing the content source information.

### Adding Location Contents Directly

#### To add contents to a location:

1. Browse to the **MobileGuardian > Policy objects > Locations** page.

2. In the Manage location contents area, configure the following settings:

Setting	Description
<b>Address</b>	Enter the individual IP, hostname, IP range or a subnet of the content, for example: For a computer, enter: 192.168.0.58 For a range of computers, enter: 192.168.0.61-192.168.0.71 For content identified by a hostname, enter: roaming_laptop
<b>Name</b>	Enter a name for the content you are adding.
<b>Comment</b>	Optionally, enter a comment describing the content.

Setting	Description
<b>Enable location</b>	Select to enable the content.

- Click **Add**, your Smoothwall System adds the contents to the location and lists it in the Contents at selected location list.
- Repeat *step 1.* and *step 3.* to add more contents.

## Uploading Content Information

It is possible to upload a comma separated values (csv) file containing contents information for the location to your Smoothwall System.

### To upload a csv file:

- Create and save the csv file. The values in the file will be interpreted by your Smoothwall System as follows:

Column	Description
<b>1</b>	The value of the first column will be read as the source. This is the very least information the file can contain and specifies the IP, IP-range, subnet or hostname. For example: For a computer, enter: 192.168.0.58 For a range of computers, enter: 192.168.0.61-192.168.0.71 For content identified by a hostname, enter: roaming_laptop
<b>2</b>	The value of optional second column will be read as the name of the content. If the name is not specified, this will default to the value specified as the source
<b>3</b>	The value of the optional third column should be: on or off, i.e. enabled or not enabled. If this value is not specified, it will default to on.
<b>4</b>	The value of the optional fourth column is read as a comment.

- On the **MobileGuardian > Policy objects > Locations** page, in the Automatically upload contents for selected location area, click **Browse** and locate and select the file.
- Click **Upload**. Your Smoothwall System uploads the file and lists it in Contents at selected location area.

## Editing Location Contents

You can edit a location's contents.

### To edit contents:

- On the **MobileGuardian > Policy objects > Locations** page, from the **Selected location** drop-down list, select the location and click **Select**. The contents are listed in the Contents at selected location area.
- Select the contents and click **Edit**.
- Make the changes you require and click **Add** to save and apply them.

## Deleting Location Contents

You can delete contents at a location.

### To delete contents:

1. On the **MobileGuardian > Policy objects > Locations** page, from the **Selected locations** drop-down list, select the location and click **Select**. The contents are listed in the Contents at selected location area.
2. Select the contents and click **Remove**.

## Deleting Locations

### To delete a location:

1. On the **MobileGuardian > Policy objects > Locations** page, from the **Selected locations** drop-down list, select the location.
2. Click **Select** and then click **Delete**. Your Smoothwall System deletes the location.

# 5 Installing MobileGuardian on Devices

In this chapter:

- What is required to install MobileGuardian on devices
- How to install, upgrade and remove MobileGuardian.

## Installing MobileGuardian on Devices

You can deploy MobileGuardian on devices in the following ways:

- **Automated deployment** – using Active Directory (AD) and group policy distribution
- **Interactively** – by running the installation wizard on individual devices
- **On the command line** – on individual devices.

---

**Note:** To ensure a high level of security, any installation of MobileGuardian should be done in a controlled environment, e.g. on your organization's LAN, by trusted administrators.

---

## Pre-requirements

The following sections describe what is required to install MobileGuardian and get it up and running.

### On Devices

On mobile devices, MobileGuardian requires:

- Microsoft Windows XP, Vista or Windows 7

- Internet Explorer. – other browsers may be used, however, to ensure that Active Directory integration is supported and your Group Policy is applied, we recommend Internet Explorer version 8
- A security policy deployed which stops users from removing or tampering with MobileGuardian. This includes ensuring that the registry is not writable, service control is not allowed, process control is not allowed and web proxy settings are not editable.

## On Your Smoothwall System

Before you start installing MobileGuardian, the following must be configured on your Smoothwall System:

- Mobile settings specifying the MobileGuardian username and password, for more information, see *Chapter 4, Configuring Mobile Settings* on page 17
- Mobile proxy settings specifying how and where devices will get their web content filtering, for more information, see *Chapter 4, Configuring Mobile Proxy Settings* on page 18.

## Installing MobileGuardian – Automated

For an automated installation, MobileGuardian can be installed:

- As an unattended silent install using a transform (.mst file)
- Using a boot-up script and the MobileGuardian .msi file.

## Installing Using a Transform

In order to generate a transform file, you use the Microsoft MSI SDK. At the time of writing, this was available to download at: <http://www.microsoft.com/downloads/>.

For detailed information, we recommend that you refer to the accompanying Microsoft documentation.

### To create a transform:

1. Start **Orca**, a component of the MSI SDK, and open `MobileGuardian.msi`.
2. From the **Transform** menu, select **New Transform**.
3. In the list of tables, click **Property**. Orca displays the file's properties.
4. From the **Tables** menu, select **Add Row**. The Add Row dialog box opens.
5. Configure the following settings:

Setting	Description
<b>Property</b>	In the <b>Value</b> column, enter in capital letters: <code>USER</code> .
<b>Value</b>	In the <b>Value</b> column, enter the MobileGuardian username as specified on the MobileGuardian > Settings > Mobile settings page of your Smoothwall System. For more information, see <i>Chapter 4, Configuring Mobile Settings</i> on page 17.

6. Click **OK** to save the settings and close the dialog box.



- From the **Tables** menu, select **Add Row** and, in the Add Row dialog box, configure the following settings:

Setting	Description
<b>Property</b>	In the <b>Value</b> column, enter in capital letters: PASSWORD.
<b>Value</b>	In the <b>Value</b> column, enter the MobileGuardian password as specified on the Guardian > Mobile > Mobile settings page of your Smoothwall System. For more information, see <i>Chapter 4, Configuring Mobile Settings</i> on page 17.

- Click **OK** to save the settings and close the dialog box.
- From the **Tables** menu, select **Add Row** and, in the Add Row dialog box, configure the following settings:

Setting	Description
<b>Property</b>	In the <b>Value</b> column, enter in capital letters: SERVER.
<b>Value</b>	In the <b>Value</b> column, enter your Smoothwall System's hostname. <b>Note:</b> You can enter your Smoothwall System IP address. However, if the IP address changes, you will have to re-install MobileGuardian using the new address. We recommend that you enter your Smoothwall System's hostname.

- Click **OK** to save the settings and close the dialog box.
- From the **Transform** menu, select **Generate Transform** and, in the Save Transform As dialog box, enter a name for the transform, browse to a secure location and click **Save**.
- In Group Policy Object Editor, in the Computer Settings node, create a new software installation package.
- Select the **MobileGuardian.msi** file, click **Advanced** and on the **Modifications** tab, click **Add** and select the .mst file you created.
- Deploy the installation package as you usually do in your environment.

## Installing Using a Boot-up Script

When using a boot-up script, make `MobileGuardian.msi` available to all the clients through a network location and use the silent install command. See *Installing MobileGuardian from the Command Line* on page 30, for more information.

## Manually Installing Clients

---

**Note:** You must use an account with administrator permissions to install MobileGuardian.

---

### Interactively Installing MobileGuardian

#### To manually install MobileGuardian on a device:

- Connect the mobile device to your Smoothwall System-protected network and download **MobileGuardian.msi** to the device.
- Right-click on **MobileGuardian.msi** and select **Install**. The Welcome screen opens.
- Click **Next** to continue. The License Agreement screen opens.

4. Read the agreement and select **I accept the terms of the License Agreement**. Click **Next** to continue.

The Setup screen opens.

5. Configure the following settings:

Setting	Description
<b>Username</b>	Enter the MobileGuardian username as specified on the MobileGuardian > Settings > Mobile settings page. For more information, see <i>Chapter 4, Configuring Mobile Settings</i> on page 17.
<b>Password</b>	Enter the MobileGuardian password as specified on the MobileGuardian > Settings > Mobile settings page. For more information, see <i>Chapter 4, Configuring Mobile Settings</i> on page 17.
<b>Server</b>	Enter the Smoothwall System hostname. <b>Note:</b> You can enter the Smoothwall System IP address. However, if the IP address changes, you will have to re-install MobileGuardian using the new address. We recommend that you enter Smoothwall System's hostname.
<b>Port</b>	Accept the default port number.

6. Click **Next** to continue. The next Setup screen opens.
7. Click on one of the following options:

Option	Description
<b>Custom</b>	Click to access the option to install MobileGuardian in a custom location. On the screen that opens, click <b>Browse</b> , specify a location and click <b>Next</b> to continue.
<b>Install</b>	Click to install Mobile Guardian in the default location.

The Ready to Install screen opens.

8. Click **Install**. The wizard installs MobileGuardian. The final screen opens.
9. Click **Finish** and restart the device.

Once restarted, MobileGuardian downloads the latest blocklists and settings from your Smoothwall System and implements your organization's web filter policy on the device.

---

**Note:** Downloading the latest blocklists and settings can take a few minutes.

---

## Installing MobileGuardian from the Command Line

You can run the MobileGuardian installer from the command line.

### To install MobileGuardian from the command line:

1. On the device, click **Start** and select **Run**. On the command line, enter the following:  

```
msiexec.exe /i MobileGuardian.msi /qn USER=USERNAME  
PASSWORD=PASSWORD SERVER=SERVERNAME
```
2. Where:

Parameter	Description
USERNAME	Enter the username as entered when configuring mobile settings on the MobileGuardian > Settings > Mobile settings page.

Parameter	Description
PASSWORD	Enter the password as entered when configuring mobile settings on the MobileGuardian > Settings > Mobile settings page.
SERVERNAME	Enter the Smoothwall System hostname. <b>Note:</b> You can enter the Smoothwall System IP address. However, if the IP address changes, you will have to re-install MobileGuardian using the new address. We recommend that you enter Smoothwall System's hostname.

- Click **OK** to start the installation. When the installation has finished, restart the device.  
Once restarted, MobileGuardian downloads the latest blocklists and settings from your Smoothwall System and implements your organization's web filter policy on the device.

---

**Note:** Downloading the latest blocklists and settings can take a few minutes.

---

## Connecting for the First Time – the Certificate

MobileGuardian uses HTTPS to communicate with your Smoothwall System.

When a MobileGuardian-protected device contacts your Smoothwall System for the first time, it expects to receive an SSL certificate. MobileGuardian stores this certificate, called `mg.crt`, in its installation directory and uses it to verify your Smoothwall System in all future communication. No further tasks and communication are done without this certificate.

As this certificate is not part of the installation, when MobileGuardian is removed, reinstalled or upgraded, this certificate is retained, and there should be no impact on authentication and no involvement or extra work needed for continuity of filtering.

However, if your Smoothwall System changes certificate, the MobileGuardian certificate must also be changed, i.e. removed from the device so that a new one is requested on next contact. You can automate this in your AD environment using a startup script or group policy. Or, manage it manually by removing it from the MobileGuardian installation directory.

## Checking MobileGuardian's Status

**To access status information:**

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

# Removing MobileGuardian

The following sections explain how to remove MobileGuardian from devices.

## Removing MobileGuardian Using AD

**To manually remove MobileGuardian:**

1. In your AD environment, remove the old package assigned to the group of MobileGuardian clients.

## Manually Removing MobileGuardian

---

**Note:** You must use an account with administrator permissions to remove MobileGuardian.

---

**To manually remove MobileGuardian:**

1. On the device, open **Windows Control Panel** and select **Add or Remove Programs**.
2. In the list of currently installed programs and updates, locate **MobileGuardian** and click **Remove**.
3. When prompted to confirm that you want to remove MobileGuardian, click **Yes**.
4. Restart the device, MobileGuardian is removed from the device.
5. On your Smoothwall System, browse to the **MobileGuardian > Settings > Mobile client status** page.
6. In the Current clients list, select the device and click **Remove**. Your Smoothwall System removes MobileGuardian from the list.

## Upgrading MobileGuardian

**To upgrade MobileGuardian:**

1. Remove the currently deployed MobileGuardian package. For more information, see *Removing MobileGuardian* on page 32.
2. Install the new package. For more information, see *Installing MobileGuardian on Devices* on page 27.

## About MobileGuardian and End-users

Users do not see MobileGuardian on their devices.

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

We recommend that:

- You tell users that MobileGuardian 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 to you so that you can adjust your policy to suit your organization better.

---

**Note:** If you want MobileGuardian content filtering to be mandatory, without users being able to intervene, you must apply an administration policy which locks down the appropriate system settings.

---

- Once installed, download the latest Smoothwall blocklists on MobileGuardian, see your *Smoothwall System Administrator's Guide* for more information.





**smoothwall**<sup>®</sup>

The Web You Want