



Network Guardian



Quick Start Guide

SmoothWall Network Guardian, 2008 FP2, Quick Start Guide, Version 1, March 2009

SmoothWall Ltd. publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Network Guardian.

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 Ltd.

For more information, contact: docs@smoothwall.net

This document was created and published in the United Kingdom.

© 2001 – 2009 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.

End user notice

During their development, all SmoothWall products are subjected to exhaustive penetration testing. There are no insecurities in a standard SmoothWall system or SmoothWall add-on module.

All files that implement SmoothWall security policies are part of the system configuration and must only be altered using the recommended configuration procedures outlined in this documentation.

SmoothWall Ltd. disclaims all responsibility for any configuration and/or installation changes that may compromise network security.

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.

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

Chapter 1	Network Guardian Quick Start.....	1
	Warning!.....	1
	About this Guide	1
	Installing Network Guardian	1
	Configuring Network Guardian.....	2
	Accessing Network Guardian	3
	Installing Updates	4
	Getting the Latest Blocklists.....	4
	Deploying a Web Security Policy	4
	Trying to Access a Blocked Site.....	5

Network Guardian Quick Start

Welcome to Network Guardian, the intelligent web security solution that dynamically analyses, understands and categorizes all web content requested by your users.

This guide describes the fastest way to install and configure Network Guardian. Full instructions can be found in the *Network Guardian Installation and Setup Guide*.

Warning!

Do not install Network Guardian on your main or only computer.

Network Guardian's installation program **ERASES ALL DATA** on the hard disk or storage device it detects.

Before you start the installation, ensure that all valuable data is safely backed up.

SmoothWall cannot be held responsible for any loss of data.

About this Guide

This guide assumes that:

- Network Guardian will only be installed in a test environment
- You have adequate network and TCP/IP knowledge
- The computer on which you install Network Guardian can be booted from its CD drive
- Your Internet service provider (ISP) does not require you to configure web proxy settings in order to access the Internet.

Installing Network Guardian

Note: Do not install Network Guardian on your main or only computer. Network Guardian's installation program **ERASES ALL DATA** from the computer's hard disk/storage volume. You must ensure that all valuable data is safely backed up. SmoothWall cannot be held responsible for any loss of data.

To install Network Guardian:

- 1 Insert the Network Guardian installation CD into the CD drive and restart the computer. Press Enter to start the installation.
- 2 The screen that opens gives you the option to run Network Guardian's advanced installation program. Wait 5 seconds to access the quick install program.
If you press the space bar and start the advanced installation program, see the *Network Guardian Installation and Setup Guide* for full information.
- 3 On the Welcome screen, press Enter to continue.

- 4 If you have more than one hard disk/storage device, the installation program will ask if you want to enable software RAID 1 support. Select the option you want and press Enter to continue.
- 5 On the Proceed with installation screen, ensure that all valuable data is safely backed up before you continue. SmoothWall cannot be held responsible for any loss of data. Press Enter to continue. Network Guardian files are installed.
- 6 When complete, the Congratulations screen is displayed. Press Enter.
- 7 When asked if you want to restore an earlier configuration, select **No** and press Enter to start configuring Network Guardian.

Note: If you select Yes here, you access migration and restore options for existing Network Guardian systems. For more information, see the *Network Guardian Installation and Setup Guide*.

Configuring Network Guardian

To configure Network Guardian:

- 1 After completing the installation program, the Keyboard mapping screen is displayed. Select your keyboard type, select **Ok** and press Enter to continue.
- 2 On the Hostname screen, specify a hostname for Network Guardian which can be used instead of using its IP address.

We recommend that you only use lowercase characters. A hostname can contain hyphens ('-'). It cannot start with a number, contain spaces or underscores ('_'). Select **Ok** and press Enter to continue.
- 3 Network Guardian automatically detects and lists the network interface cards (NICs) available. You must configure a NIC to connect Network Guardian to your internal network. Press Enter to continue. The Default interface screen is displayed.
- 4 Select a NIC, select **Ok** and press Enter to continue. When prompted, enter the following information:

Field	Enter
Name	A name that identifies the NIC.
Internal IP address	The IP address that this Network Guardian NIC will use on your internal network.
Network mask	The network mask used in conjunction with the internal IP address.
MTU	Accept the default maximum transmission unit (MTU), or enter the value required in your environment.

- 5 Select **Ok** and press Enter to continue. The DNS and Gateway settings screen is displayed, enter the following information:

Field	Enter
Primary DNS	The IP address of the primary DNS server. This DNS server is used by Network Guardian to resolve hostnames to IP addresses.
Secondary DNS	The IP address of a secondary DNS server, if one is available.
Default Gateway	The IP address of the gateway that Network Guardian should use.

- 6 Select **Ok** and press Enter to continue.

The Setup menu is displayed. Here you can choose to run the setup program to configure advanced Network Guardian settings or select to finish configuring settings. For information on advanced settings, see the *Network Guardian Installation and Setup Guide*.

- 7 Select **Finished** and press Enter to continue.

- 8 When prompted for an admin account password, enter the following information:

Field	Description
Password	Enter a strong password for Network Guardian's admin account. The admin account is used to access Network Guardian via its web interface. Minimum = 6 characters Maximum = 255 characters
Again	Re-enter the password to confirm it.

- 9 Select **Ok** and press Enter to continue. When prompted for a root account password, enter the following information:

Field	Description
Password	Enter a strong password for Network Guardian's root account. The root account is used to access Network Guardian via the console. Minimum = 6 characters Maximum = 255 characters
Again	Re-enter the password to confirm it.

- 10 Setup is complete. Press Enter to reboot the computer. You can now log on to your Network Guardian system, complete the registration process and connect to the Internet.

Accessing Network Guardian

After rebooting, you are ready to log on and register. After that, you can start using Network Guardian to protect your network and users.

To access Network Guardian:

- 1 On a network-connected client, start a web browser and connect to the Network Guardian using HTTP by entering Network Guardian's address, for example: `http://NetworkGuardian_ip_address:81` The login page opens.

- 2 On the login page, enter the following information:

Field	Explanation
Username	Enter <code>admin</code> . This is the default account used to administer Network Guardian.
Password	Enter the password you specified when setting up Network Guardian.

- 3 Click **Login**. The Network Guardian about page opens. Enter the following information:

Field	Explanation
Serial no.	Enter your Network Guardian serial number.

Field	Explanation
Name	The name of your organization's contact person for your Network Guardian.
Organization	The name of your organization.
Department	The department in which your Network Guardian is located.
Locality or town	The town your organization is located in.
State	The state your organization is located in.
Country	The country your organization is located in.
Email	The email address of your organization's contact person for your Network Guardian.

- 4 Click **Save** and, when prompted, review the information you have supplied and click **Confirm**. Network Guardian's control page opens.

The control page is Network Guardian default home page. You can now review Network Guardian functionality. For more information, see the *Network Guardian Administrator's Guide*.

Installing Updates

The next step is to ensure that Network Guardian has the latest updates installed.

To check for and install updates:

- 1 Navigate to the **system > maintenance > updates** page.
- 2 Click **Refresh update list** to list the latest updates available. Click **Download updates**. When they have been downloaded, click **Install updates**. The updates are downloaded and installed.

Getting the Latest Blocklists

Blocklists are groups of settings which are updated on a regular basis by SmoothWall to maintain Network Guardian's list of undesirable, inappropriate or objectionable content.

To update blocklists:

- 1 Navigate to the **system > maintenance > licenses** page.
- 2 In the Blocklist subscriptions area, click **Check for updates**.
- 3 Click **Download update** to download the list.
- 4 When downloaded, click **Install and apply changes** to deploy the latest blocklist.

Deploying a Web Security Policy

By default, Network Guardian comes with a comprehensive web security policy in place. There are several ways of deploying this policy on users' workstations. All of which are documented in your *Network Guardian Administrator's Guide*.

In this section, we explain the quickest way to deploy the policy for review and testing purposes.

Note: The following steps explain how to deploy the default web security policy on a user's workstation with Internet Explorer 7 installed as the web browser.

To deploy the policy:

- 1 Start Internet Explorer, and from the **Tools** menu, select **Internet Options**.
- 2 On the **Connections** tab, click **LAN settings** and in the Proxy server area, select **Use a proxy server for your LAN ...**
- 3 Enter your Network Guardian's IP address and port number 800.
- 4 Click **Advanced** to access more settings. In the Exceptions area, enter Network Guardian's IP address and any other IP addresses to content that you do not want filtered, for example, your intranet or local wiki.
- 5 Click **OK**, **OK** and **OK** to save the settings.

Trying to Access a Blocked Site

As part of its default acceptable usage policy, Network Guardian blocks access to many popular social networking sites, including <http://www.myspace.com/>

By trying to access this site, you can see Network Guardian's default block page.

To try and access a blocked site:

- 1 Deploy the default web security policy by configuring Internet Explorer to use Network Guardian as its proxy server.
- 2 In Internet Explorer, enter: <http://www.myspace.com/> Network Guardian blocks access to the site and displays the block page.

For full information on working with Network Guardian and how to customize a web security policy to suit your organization, see the *Network Guardian Administrator's Guide*.

Managing Network Guardian Logs Files and Report Data

Network Guardian's web filter log files provide detailed analysis of web proxy and filtering activity.

You can configure Network Guardian to retain log files and prune the reporting database which contains logged information to suit your system.

Retaining Log Files

Network Guardian enables you to set retention periods for the different log files.

To configure the log retention period:

- 1 Browse to the **information > settings > logging options** page. In the Log file retention area, locate the log type you want to configure retention for.
- 2 From the drop-down list, select the retention period. The following periods are available:

Time Period	Description
1 Day	Rotate the log file daily and keep the last day.

Time Period	Description
2 Days	Rotate the log file daily and keep the last 2 days.
A week	Rotate the log file weekly and keep the last week.
A fortnight	Rotate the log file weekly and keep the last 2 weeks.
A month	Rotate the log file monthly and keep the last month.
Two months	Rotate the log file monthly and keep the last 2 months.
Three months	Rotate the log file monthly and keep the last 3 months.
Four months	Rotate the log file monthly and keep the last 4 months.
Five months	Rotate the log file monthly and keep the last 5 months.
Six months	Rotate the log file monthly and keep the last 6 months.
Seven months	Rotate the log file monthly and keep the last 7 months.
Eight months	Rotate the log file monthly and keep the last 8 months.
Nine months	Rotate the log file monthly and keep the last 9 months.
Ten months	Rotate the log file monthly and keep the last 10 months.
Eleven months	Rotate the log file monthly and keep the last 11 months.
A year	Rotate the log file monthly and keep the last 12 months.
A week (large)	Rotate the log file daily and keep the last 7 days.
A month (Large)	Rotate the log file daily and keep the last 31 days.
A year (large)	Rotate the log file daily and keep the last 365 days.

- 3 Click **Save** to save the settings.

Automatically Deleting Log Files

Network Guardian can be set to automatically delete log files if there is a limited amount of free disk space available.

To configure automatic log deletion:

- 1 Browse to the **information > settings > logging options** page. In the Automatic log deletion area, select **Delete old logs when free space is low**.
- 2 Choose a level at which log deletion will be activated using the **Amount of disk space to use for logging** drop-down list.
- 3 Click **Save** to save the settings.

Pruning Report Data

Network Guardian stores report data in its own database. You can configure Network Guardian to prune the contents of the database in order to save storage space.

To prune the database:

- 1 On the **information > settings > database settings** page, configure the following setting:

Setting	Description
Mode	Accept the default setting Local .

Setting	Description
Pruning	Select if you want to prune entries in the database at specified intervals to save storage space and potentially speed up information processing. Don't prune – Select to not remove any enties from the database. Over a month – Select to remove entries that are more than one month old and repeat pruning every month. Over three months – Select to remove entries that are more than three months old and repeat pruning every month. Over six months – Select to remove entries that are more than six months old and repeat pruning every month.

Note: We strongly recommend that you configure Network Guardian to prune the database regularly. If you do not, the database will grow continuously.

- 2 Click **Save** to save the settings.

Copyright 2001-2009 – SmoothWall
All rights reserved.