smoothwall®

The Web You Want

Secure Web Gateway

Network Guardian Installation Guide

For future reference

Network Guardian serial number:

Date installed:

Smoothwall contact:

Smoothwall® Network Guardian, Installation Guide, August 2014

Smoothwall 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.

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.

Network Guardian contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

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

Contents

About This Guide

Network Guardian is a licenced feature of your Smoothwall System.

This manual provides guidance for installing Network Guardian.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Network Guardian.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System
- An overall understanding of networking concepts

Note: We strongly recommend that everyone working with Smoothwall products attend Smoothwall training. For information on our current training courses, contact your Smoothwall representative.

Organization and Use

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

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Network Guardian
Cross-references and references to other guides	Italics	See *Chapter 1, Introduction* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`

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 Network Guardian:

- *Network Guardian Administration Guide*, which describes how to configure Network Guardian
- *Network Guardian Operations Guide*, which describes how to use Network Guardian
- *Network Guardian Upgrade Guide*, which describes how to upgrade versions of Network Guardian
- *Network Guardian User Portal Guide*, which describes how to use the Network Guardian user portal
- http://www.smoothwall.net/ contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introduction

In this chapter:

- An overview of Network Guardian
- System and hardware information
- Support information.

Welcome

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

Network Guardian Overview

Network Guardian provides:

- Protects from pornography and objectionable content
- Controls access to non work-related sites, such as news, sport, travel and auctions.
- Stops web-borne spyware, viruses and browser exploits
- Reports on Internet behavior and resource utilization
- Manages user authentication and applies filtering policies based on group membership.

Minimum Hardware Requirements

The following are the minimum hardware specifications:

Hardware	**Minimum requirement**
Processor	Core 2 Duo or later.

Hardware	Minimum requirement
Memory	Ram: 2 Gbytes or more.

About Registration

After you install Network Guardian, it registers itself online with Smoothwall and checks for the latest updates available. This registration also activates the 30 day email support package that is included as standard with Network Guardian.

The following information is communicated to Smoothwall during the registration process:

- CPU specifications
- System memory (RAM) specifications
- Storage system specifications
- Interface configuration
- Module configuration
- Software version
- Installation date
- Enabled status for optional services
- Number of configured interfaces and whether they are internal or external
- Authentication type and LDAP server type
- Manufacturer name and product name
- Main board manufacturer name and product board name.

Note: All registration data is stored securely, in accordance with BS5750 and the Data Protection Act 1998.
Smoothwall does not, and cannot, capture any information other than that which is stated here, and which is transmitted as part of this one-time registration process.

2 Installing Network Guardian

In this chapter:

- Warning!
- What to consider before installing Network Guardian
- Install program messages and conventions
- How to run Network Guardian's quick and advanced installation programs.

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. This includes any inserted USB storage device. Smoothwall cannot be held responsible for any loss of data.

Before you start the installation, ensure that all valuable data is safely backed up. Smoothwall cannot be held responsible for any loss of data.

Before You Start

Before you start, we strongly recommend that you:

- Consult your organization's acceptable usage policy to determine what is acceptable when users access the Internet
- Consult your organization's security policy to determine the Network Guardian configuration that will suit your organization best

- Determine where your Network Guardian installation will be located physically and how you will control physical access to it
- Install, configure and test Network Guardian in a test environment to ensure that you have the correct level of security before you install it in a production environment
- Ensure everyone who will be working with Network Guardian has good networking and information security skills, has received adequate Network Guardian training and can be trusted to carry out their duties professionally and without malice.

Messages and Conventions

Network Guardian's installation and initial setup programs use a text-based interface that is compatible with all types of graphic card.

The following keyboard controls are used to interact with the programs:

Key	Explanation
Arrows	Move the cursor/focus/highlight between options.
Tab	Advances the focus to the next screen object.
Space	Clicks a button if it has the focus.
Enter or Return	Clicks a button if it has the focus. Click the **Ok** button if the focus is not currently on a button.

The following on-screen buttons are used throughout the installation and setup process:

Button	Explanation
Cancel	Exits the current section of the installation or setup process without saving or activating any changes. If the Setup program is being run as part of the first-time setup process, the Cancel button will exit the setup program and require the installation process to be restarted.
Done	Indicates that configuration of the current feature is complete. Changes will be saved and activated and control will return to the menu or installation procedure.
Finished	Exits once all configuration changes have been completed in the Setup program.
Ok	Confirms the selection of the highlighted option, acknowledges a message or proceeds to the next screen.

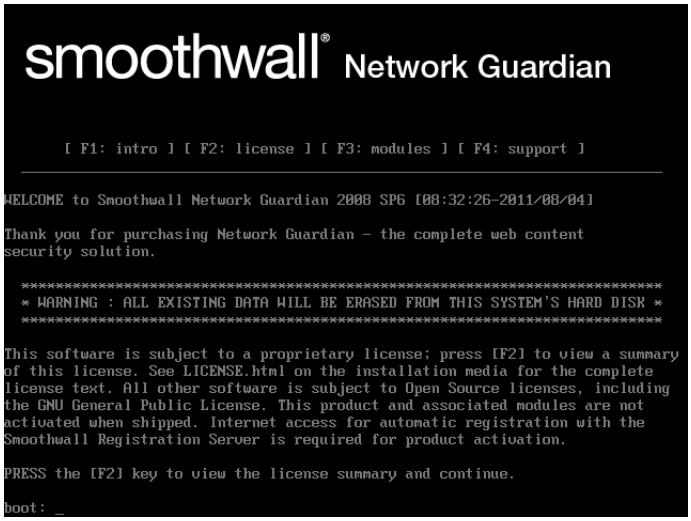
Running Network Guardian's Quick Install

Network Guardian's quick install automatically checks the computer and its hardware components and installs Network Guardian accordingly.

Note: If you are upgrading from a compatible Smoothwall System to Network Guardian, see the *Network Guardian Upgrade Guide* for full information. The following sections explain how to install Network Guardian from scratch.

To install Network Guardian:

1. Insert the Network Guardian installation CD into the CD-ROM drive and reboot the computer. The following screen is displayed:



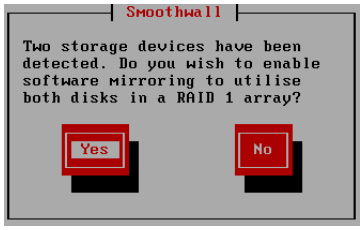
2. Press **Enter**. The following screen is displayed:

3. When the installation program has initialized the drivers, the following screen is displayed:

4. Wait 5 seconds. The following screen is displayed:

5. Press Enter to continue.

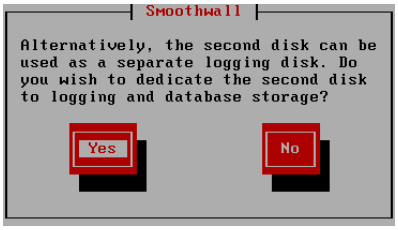
If you have more than one hard disk/storage device, the following screen is displayed:



6. Select **Yes** and press Enter to enable Network Guardian software RAID 1 support. Continue the installation at *step 8.*.

Note: When using a hardware RAID device, the first volume on the first detected RAID card will be used – this is typically set up by RAID BIOS.

Or, select **No** and press Enter to continue. The following screen is displayed:



7. Select **Yes** and press Enter to use all of the second disk as a separate logging disk. This is mostly useful if the two disks are different sizes, in which case, the bigger disk should be second one and the smaller (OS) disk should be the first one. It also works in Hardware RAID setups. An example would be: volume 1: 2 disks in Mirror (OS) and volume 2: 4 disks in RAID5 (Logging).

   Or, select **No** and press Enter to continue.

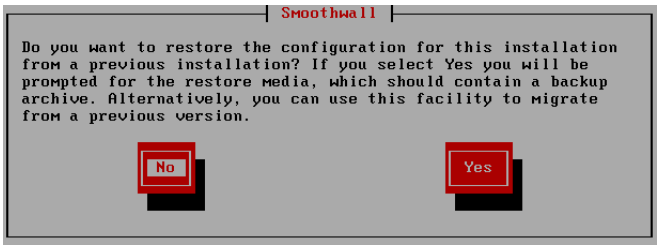
8. The following screen is displayed:

Note: Installing Network Guardian will **ERASE ALL DATA** from the computer's hard disk/storage device. This includes any inserted USB storage device. Ensure that all valuable data is safely backed up before you continue.

This screen is the last opportunity you have to cancel the installation before data is erased. Smoothwall cannot be held responsible for any loss of data.

9. Press Enter to continue. Network Guardian files are installed. When complete, the Congratulations! screen is displayed:

10. Press Enter. The following screen is displayed:

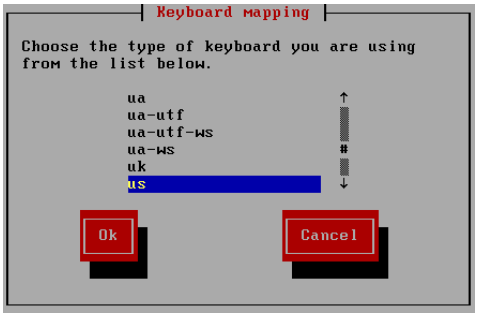


11. Select **No** and press Enter to continue.

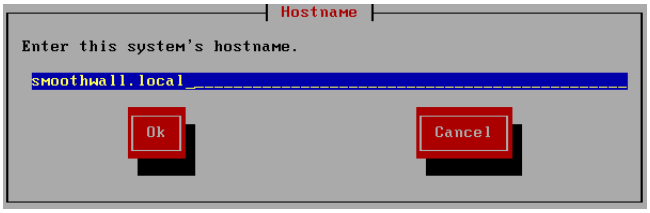
Note: If you select Yes here, you access migration and restore options for existing Network Guardian systems.

For information on migration and restore options, see the *Network Guardian Upgrade Guide*.

The Keyboard mapping screen is displayed:



12. Select your keyboard type and press Enter to continue. The Hostname screen is displayed:



Here you can specify a hostname for Network Guardian which can be used instead of using its IP address.

Note: We recommend that you only use lowercase characters in the hostname.

If the Network Guardian system is going to integrated within an existing network infrastructure that uses domain name structuring, enter a fully qualified hostname that is appropriate to the system's position within the hierarchy.

Note: A hostname can:

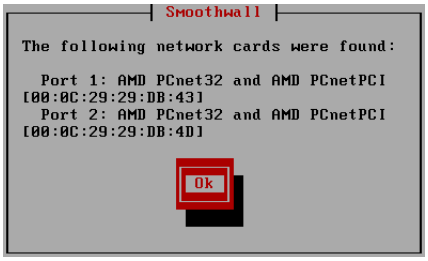
- contain hyphens '-' and dots '.'.

Note: A hostname cannot:

- Start with a number
- Contain spaces
- Contain underscores '_' or any other wildcard or punctuation characters except '.'.

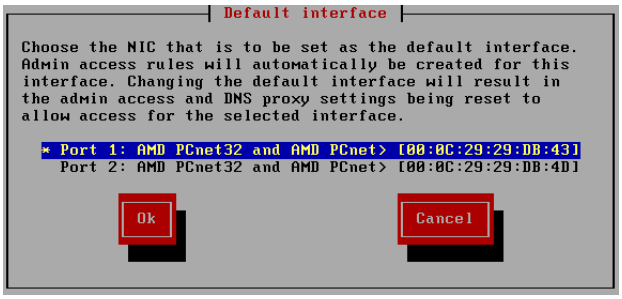
The default hostname is `smoothwall.local`, however, if there are multiple Network Guardian systems, you must identify them using unique hostnames.

13. Accept the default or enter a new hostname for Network Guardian. Select **Ok** and press Enter to continue. A list of available network interface cards (NICs) is displayed, for example:

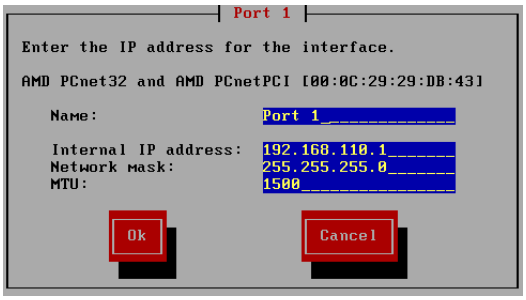


14. Press Enter.

The following screen is displayed:



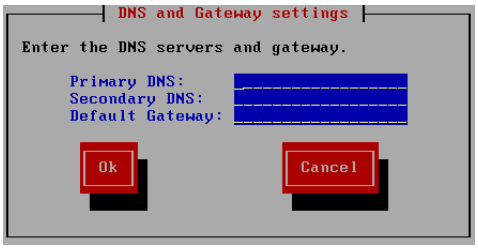
15. Select the Network Iinterface Card (NIC) to use, select **Ok** and press Enter. The following screen is displayed:



16. Enter the following information:

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

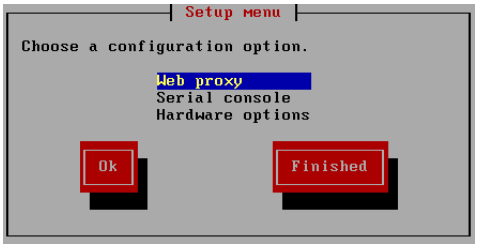
17. Select **Ok** and press Enter to continue. The following screen is displayed:



18. 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. If Network Guardian is going to be integrated into an existing DNS infrastructure, such as when using an Active Directory server, enter the IP address of the appropriate DNS server within the existing infrastructure.
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.

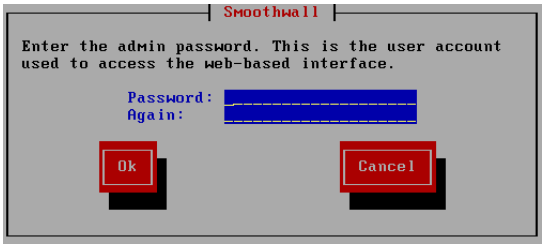
19. Select **Ok** and press Enter to continue. The Setup menu is displayed:



These options are used when running the advanced install program. For more information, see *Chapter 4, Setting up Network Guardian* on page 25.

20. Select **Finished** and press Enter.

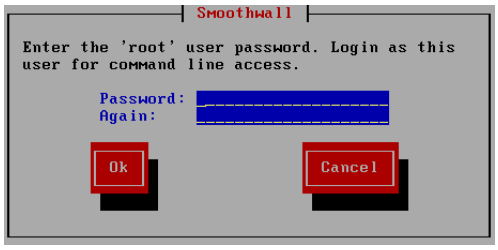
The following screen is displayed:



21. Enter the following information:

Field	Explanation
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.

22. Select **Ok** and press Enter. The following screen is displayed:



23. Enter the following information:

Field	Explanation
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.

24. Select **Ok** and press Enter. The following screen is displayed:

25. Select **Ok** and press Enter to reboot the computer.

    After rebooting, you can access Network Guardian from a network client running a web browser. For more information, see *Chapter 5, Accessing Network Guardian* on page 31.

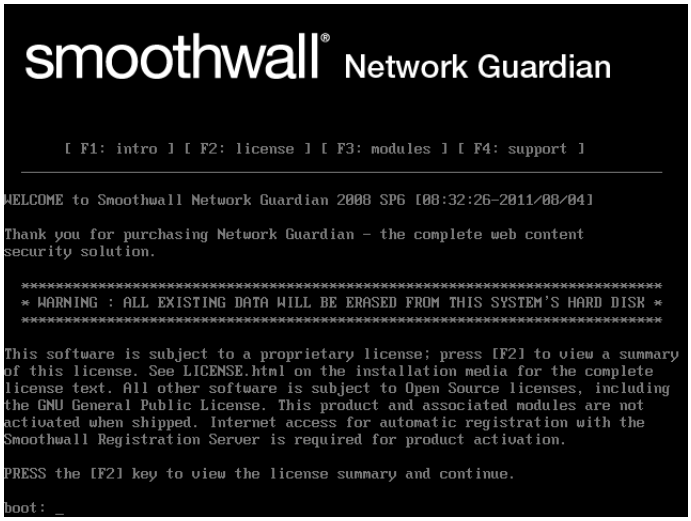
Running Network Guardian's Advanced Install

Network Guardian's advanced install enables you to configure Network Guardian manually to suit your environment.

Note: If you are upgrading from a compatible Smoothwall System to Network Guardian, see the *Network Guardian Upgrade Guide* for full information. The following sections explain how to install Network Guardian from scratch.

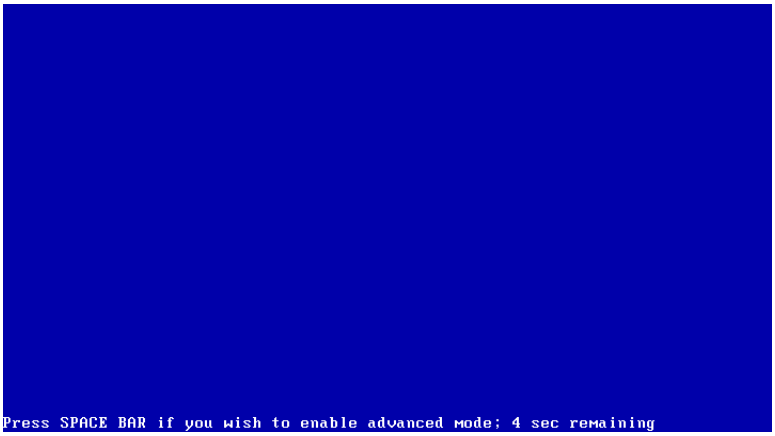
To install Network Guardian:

1. Insert the Network Guardian installation CD into the CD-ROM drive and reboot the computer. The following screen is displayed:



2. Press **Enter**. The following screen is displayed:

When the installation program has initialized the drivers, the following screen is displayed:

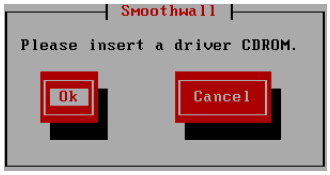


3. Press the space bar to access Network Guardian's advanced install.The following screen is displayed:

4. Press **Enter** to continue. The following screen is displayed:

5. If you are installing Network Guardian on a computer which requires non-standard drivers, this is where you install them. If you are not installing drivers, select **Done**, press Enter and go to *step 10.*.

6. Select the medium on which the drivers are stored, select **Ok** and press Enter. You are prompted to insert the medium, for example:

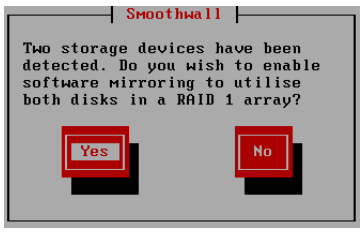


7. Insert the medium into the appropriate drive and press Enter. The installation program loads the drivers and the following screen is displayed:

8. Press Enter. The following screen is displayed:

9. Repeat *step 6.* to *step 8.* above if you need to install more drivers. To continue, select **Done** and press Enter. The following screen is displayed:

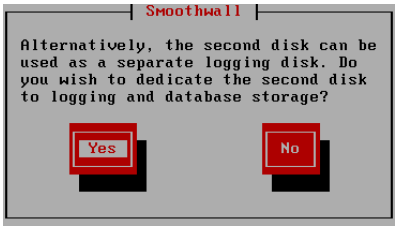
10. When the drivers have been initialized again, if you have more than one hard disk/storage device, the following screen is displayed:



11. Select **Yes** and press Enter to enable Network Guardian software RAID 1 support. Continue the installation at *step 13.*.

Note: When using a hardware RAID device, the first volume on the first detected RAID card will be used – this is typically set up by RAID BIOS.

Or, select **No** and press Enter to continue. The following screen is displayed:



12. Select **Yes** and press Enter to use all of the second disk as a separate logging disk. This is mostly useful if the two disks are different sizes, in which case, the bigger disk should be second one and the smaller (OS) disk should be the first one. It also works in Hardware RAID setups. An example would be: volume 1: 2 disks in Mirror (OS) and volume 2: 4 disks in RAID5 (Logging).

    Or, select **No** and press Enter to continue.

13. The Disk partitioning options screen is displayed, for example:

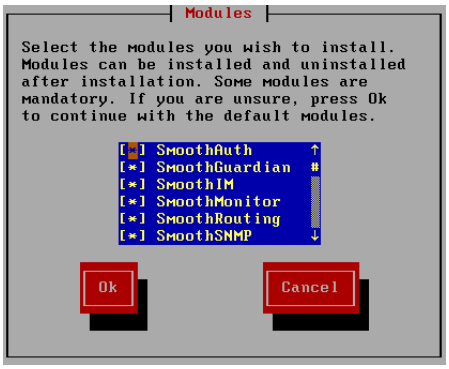
    Here you can configure partition and logging options.

Option	Description
Log to RAM Disk	By default, Network Guardian stores all its logs on the local hard disk. Selecting this option stores the logs in RAM to reduce disk storage requirements. **Note:** Logs are lost at reboot when operating in this mode. RAM disk logging uses a maximum of half of the system's RAM. RAM disk logging is not recommended for systems with less than 128MB of RAM.
Minimal swap partition	Select this option to reduce swap partition requirements.

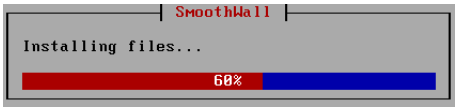
14. Select the options you require and select **Ok** to continue. The following screen is displayed:

Note: The Network Guardian installation process **ERASES ALL DATA** from the computer's hard disk/storage device. This includes any inserted USB storage device. Ensure that all valuable data is safely backed up before you continue. This screen is the last opportunity you have to cancel the installation process before data is deleted. Smoothwall cannot be held responsible for any loss of data.

15. Select **Ok** to continue. The installation program prepares the computer and installs Network Guardian. The Modules screen is displayed:



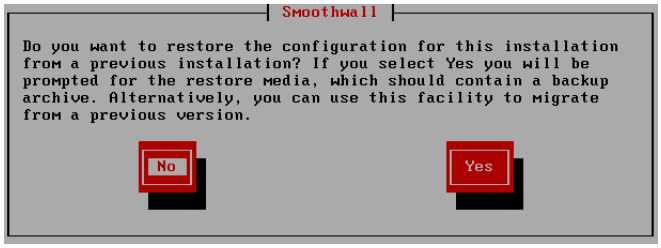
16. Select the modules you want to install, select **Ok** and press Enter to continue. Installation progress is displayed, for example:



Once complete, the Congratulations! screen is displayed:

17. Select **Ok** to continue.

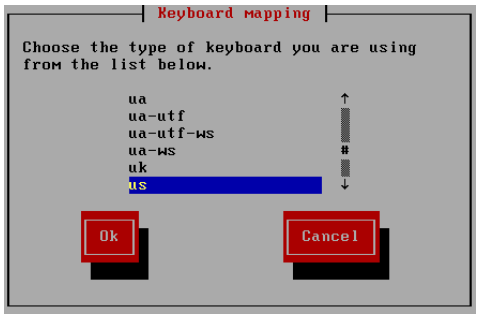
The following screen is displayed:



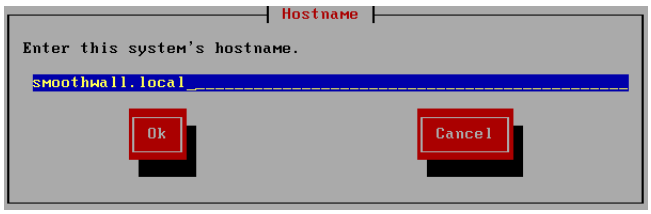
18. Select **No** to start configuring your new installation of Network Guardian.

Note: If you select Yes here, you access migrate and restore options for existing Network Guardian systems. For information, see *Chapter 3, Migrating and Restoring Settings* on page 21.

When the Keyboard screen is displayed:



19. Select your keyboard type, select **Ok** and press Enter to continue. The Hostname screen is displayed:



Here you can specify a hostname for Network Guardian which can be used instead of using its IP address. We recommend that you only use lowercase characters in the hostname.

If the Network Guardian system is going to integrated within an existing network infrastructure that uses domain name structuring, enter a fully qualified hostname that is appropriate to the system's position within the hierarchy.

Note: A hostname can:

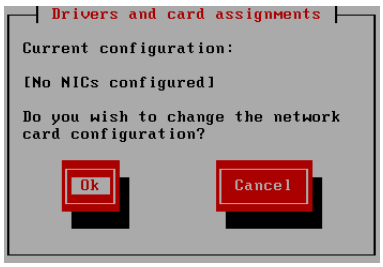
- contain hyphens '-' and dots '.'

A hostname cannot:

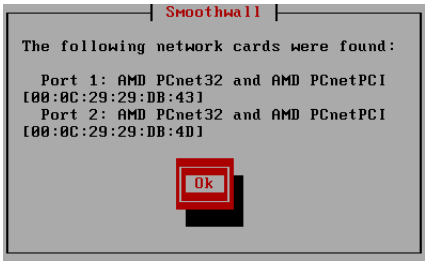
- Start with a number
- Contain spaces
- Contain underscores '_' or any other wildcard or punctuation characters except '.'.

The default hostname is `smoothwall.local`, however, if there are multiple Network Guardian systems, you must identify them using unique hostnames.

20. Accept the default or enter a new hostname for Network Guardian. Select **Ok** and press Enter to continue.
21. The Network configuration screen is displayed:
22. Select **Network Interface Card detection**, select **Ok** and press Enter. The drivers and card assignment screen opens:

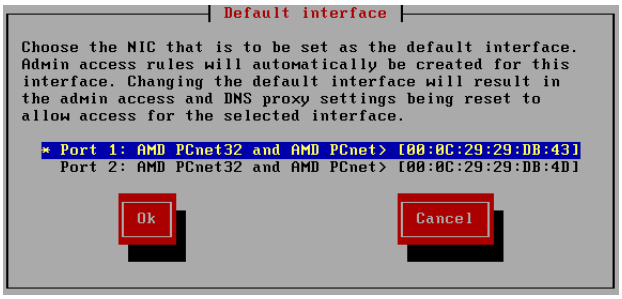


23. Select **Ok** and press Enter to continue. A list of available network cards is displayed, for example:



24. Press Enter.

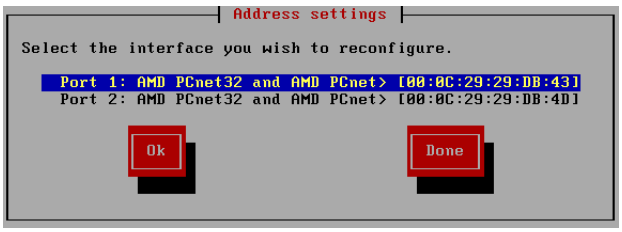
    You return to the Network configuration screen. Select **Default interface** and press Enter. The Default interface screen is displayed:



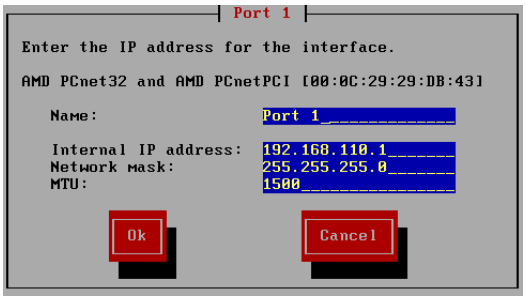
25. Select which NIC to use as the default interface, select **Ok** and press Enter to continue.

26. On the Network configuration screen. Select **Address settings** and press Enter.

    The Address settings screen is displayed:



27. Select the Network Interface Card (NIC) you want to use, select **Ok** and press Enter. The following screen is displayed:



28. Enter the following information:

Field	Enter
Name	A name that identifies Network Guardian's NIC.
Internal IP address	The IP address of the Network Guardian NIC on your internal network, for example.

Field	Enter
Network mask	The network mask used in conjunction with the internal IP address to define the network that this NIC belongs to.
MTU	Accept the default maximum transmission unit (MTU), or enter the value required in your environment.

29. Select **Ok** and press Enter to continue. On the Address settings screen, select **Done** and press Enter.
30. On the Network configuration screen, select **Done** and press Enter.

    The Setup program starts and displays the Setup menu.

The next step is to set up Network Guardian. See *Chapter 4, Setting up Network Guardian* on page 25 for more information.

3 Migrating and Restoring Settings

In this chapter:

- How to migrate or restore settings from a Network Guardian installation or other compatible Smoothwall System.

Prerequisites

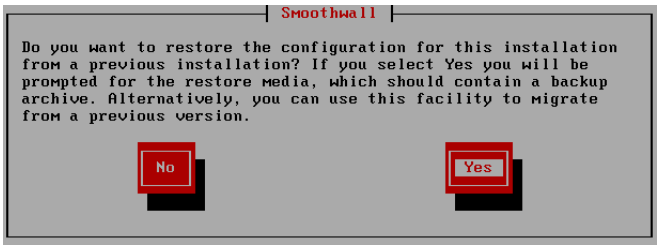
In order to migrate or restore settings, you must have:

- An archive containing the settings you want to migrate, see the *Administration Guide* delivered with your current Smoothwall System for information on how to archive settings
- Carried out the initial Network Guardian installation, see *Chapter 2, Installing Network Guardian* on page 5 for more information.

Migrating/Restoring Settings

To migrate/restore your current settings:

After completing the initial installation, the following screen is displayed:



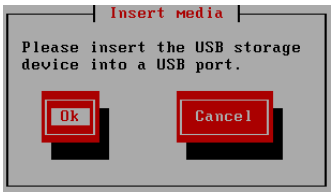
1. Select **Yes** and press Enter.

The following screen is displayed:

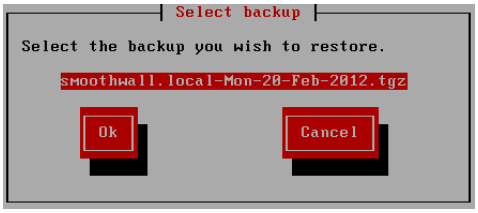
2. Select one of the following:

Option	Select to:
CDROM	Migrate/restore settings using an archive stored on a CD.
Floppy disk	Migrate/restore settings using an archive stored on a floppy disk.
USB storage media	Migrate/restore settings using an archive stored on USB media
Version 3 floppy disk	Migrate/restore Smoothwall Corporate Server settings using an archive stored on a floppy disk.

3. Select **Ok** and press Enter. The Insert media screen is displayed, for example:



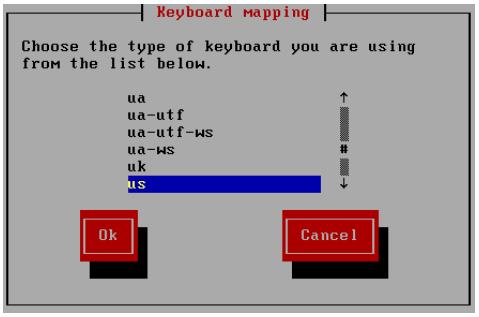
4. Insert the media containing the archive of migration settings, select **Ok** and press Enter. The Select backup screen is displayed, for example:



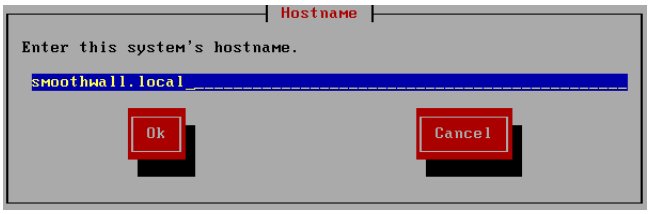
5. Select the archive, select **Ok** and press Enter.

6. Depending on the settings in the archive, you are prompted to select the settings you want to migrate. Select the settings you want to migrate and press Enter.

7. As prompted, continue to select settings you want to migrate. When the settings have been migrated, the installation program displays the Keyboard mapping screen:



8. Select your keyboard type, select **Ok** and press Enter to continue. The Hostname screen is displayed:



Here you can specify a hostname for Network Guardian which can be used instead of using its IP address. We recommend that you only use lowercase characters in the hostname.

If the Network Guardian system is going to integrated within an existing network infrastructure that uses domain name structuring, enter a fully qualified hostname that is appropriate to the system's position within the hierarchy.

Note: A hostname can:

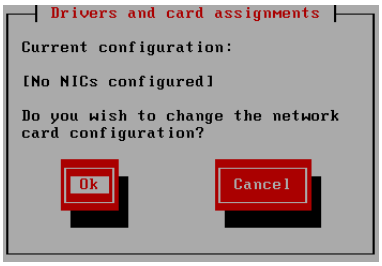
- contain hyphens '-' and dots '.'

A hostname cannot:

- Start with a number
- Contain spaces
- Contain underscores '_' or any other wildcard or punctuation characters except '.'.

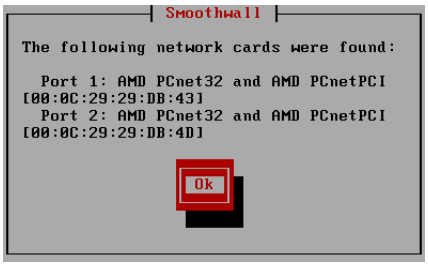
The default hostname is `smoothwall.local`, however, if you have multiple Network Guardian systems, you must identify them using unique hostnames.

9. Accept the default or enter a new hostname for Network Guardian. Select **Ok** and press Enter to continue.
10. The Network configuration screen is displayed:
11. Select **Network Interface Card detection**, select **Ok** and press Enter. The drivers and card assignment screen opens:

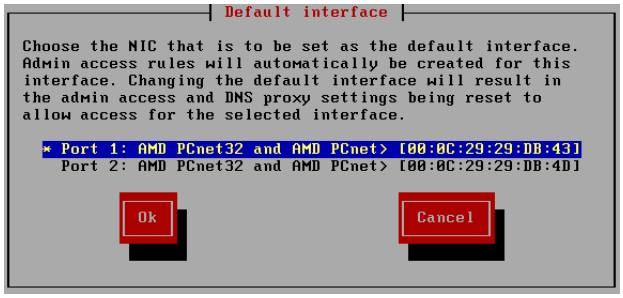


12. Select **Ok** and press Enter to continue.

A list of available network cards is displayed, for example:

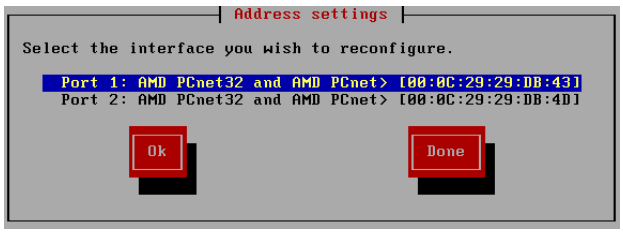


13. Press Enter. You return to the Network configuration screen. Select **Default interface** and press Enter. The Default interface screen is displayed:

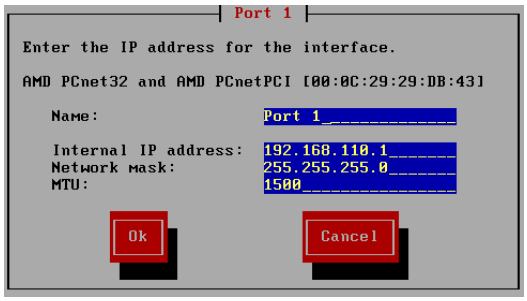


14. Select which NIC to use as the default interface, select **Ok** and press Enter to continue.

15. On the Network configuration screen. Select **Address settings** and press Enter. The Address settings screen is displayed:



16. Select the Network Interface Card (NIC) you want to use, select **Ok** and press Enter. The following screen is displayed:



17. Enter the following information:

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

18. Select **Ok** and press Enter to continue. On the Address settings screen, select **Done** and press Enter.

19. On the Network configuration screen, select **Done** and press Enter. The Setup program starts and displays the Setup menu.

    The next step is to set up Network Guardian. See *Chapter 4, Setting up Network Guardian* on page 25 for more information.

4 Setting up Network Guardian

In this chapter:

- Running the setup program
- How to configure the admin and root accounts required to administer Network Guardian.

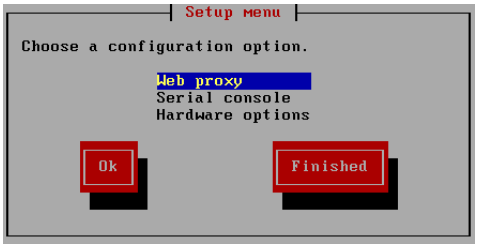
Setting up Network Guardian

Setting up Network Guardian entails configuring network and other connection settings using the Setup program.

Note: You can configure settings after Network Guardian has been installed and configured. See the *Network Guardian Administration Guide* for more information.

To setup Network Guardian:

1. Complete installing Network Guardian and configuring keyboard, hostname and network settings. The Setup menu is displayed:



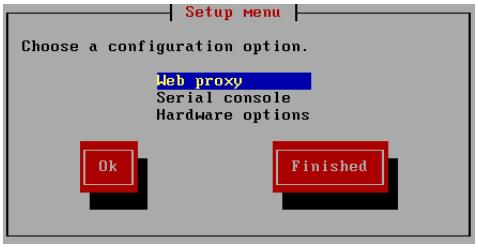
2. Here you can choose to run the setup program to configure advanced Network Guardian settings or select to finish configuring settings.

- Select **OK** and press Enter to start the Setup program and see *Running the Setup Program* on page 26 for more information

- Or, select **Finished** to complete Network Guardian basic configuration. Your next step will be to configure administration accounts for Network Guardian. See *Setting Account Passwords* on page 29 for more information.

Running the Setup Program

After completing the basic installation of Network Guardian, the Setup menu is displayed:



The Setup program contains the following optional settings that you may need to configure depending on your ISP, hardware and network:

Option	Description
Web proxy	Select to set web proxy settings that your Internet Service Provider (ISP) requires you to use to access the Internet. Select and press Enter to continue. See *Configuring Web Proxy Settings* on page 26 for more information.
Serial console	Used to enable terminal or console access via the computer's serial port. Select and press Enter to continue. See *Enabling Access via the Serial Console* on page 27 for more information.
Hardware options	Used to configure motherboard and processor settings, including SMP support. Select and press Enter to continue. See *Configuring Hardware Options* on page 28 for more information.

The sections that follow explain how to configure the setup options.

Configuring Web Proxy Settings

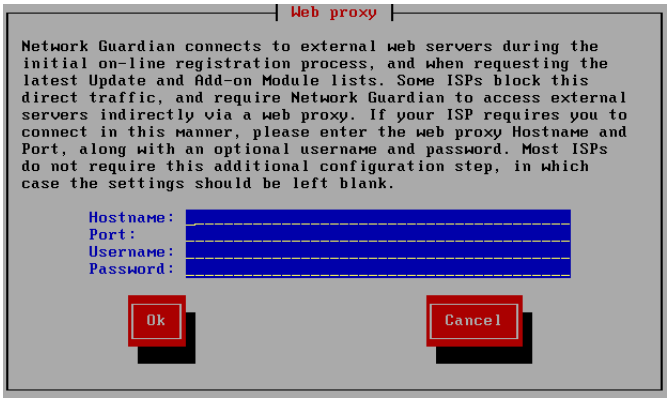
Note: As the majority of Internet Service Providers (ISPs) do not use web proxy servers, it is unlikely that you will need to make changes on this screen. If your ISP does use a proxy server, you should already know the configuration details. If you do not, consult your ISP.

Some ISPs require you to connect to the Internet via a web proxy server. The Setup program's Web proxy option enables you to configure Network Guardian to use such a proxy server. This ensures that Network Guardian will be able to connect to the Internet, register itself and download any updates available from Smoothwall.

To configure web proxy settings required by your ISP:

Note: These settings do not apply to your Network Guardian proxy service.

1. From the Setup menu, select **Web proxy**. The following screen is displayed:



2. Enter the following information:

Field	Enter
Hostname	The hostname of the web proxy your ISP requires you to use to access the Internet. Contact your ISP if you are unsure of the address.
Port	The port number of the port used by the web proxy. 80 and 8080 are the most commonly used ports for web proxies. Contact your ISP if you are unsure of the number.
Username	A username for the proxy, if one has been allocated by your ISP.
Password	A password for the proxy, if one has been allocated by your ISP.

Note: The settings here have nothing to do with Network Guardian's own web proxy service, which is configured separately using the web-based interface. See the *Network Guardian Administration Guide* for more information.

3. Select **Ok** to return to the Setup menu. To continue with the Setup program, select another Setup menu option and press Enter. To end the Setup program, select **Finished** and press Enter.

   If you have finished with the Setup program, the next step is to set administration account passwords. For more information, see *Setting Account Passwords* on page 29.

Enabling Access via the Serial Console

The Setup menu's Serial console option enables you to access Network Guardian via the computer's serial port. This option is primarily intended for use when operating Network Guardian in headless mode, that is, without a screen and keyboard, as would normally be the case in a communication/server cabinet.

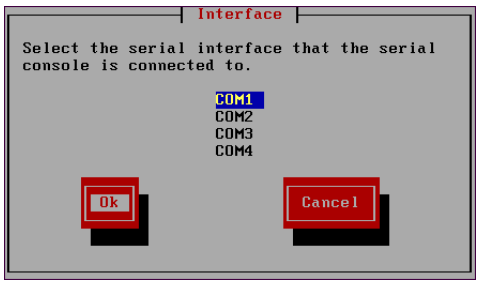
Typically, you can connect a notebook PC running a VT100 terminal program to one of Network Guardian's RS232 serial communications ports using an RS232 null modem cable.

To enable serial console access:

1. From the Setup menu, select **Serial console**. The following screen is displayed:

2. Select **Enabled**.

   The following screen is displayed:



3. Select the serial interface that the console is connected to. Select **Ok** to return to the Setup menu.

   To access the serial console once this configuration has been completed, use the following comms parameters: 9600 baud, 8 databits, No parity, 1 start/stop bit – also referred to as: 96008n1.

4. To continue with the Setup program, select another Setup menu option and press Enter. Or, to end the Setup program, select **Finished** and press Enter.

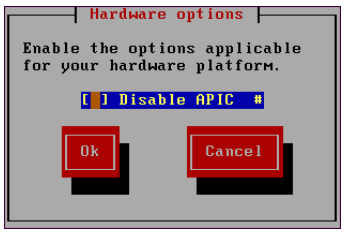
   If you have finished with the Setup program, the next step is to set administration account passwords. For more information, see *Setting Account Passwords* on page 29.

Configuring Hardware Options

The Setup menu's Hardware option enables you to configure advanced hard disk and motherboard settings.

To configure hardware options:

1. From the Setup menu, select **Hardware options**. The Hardware options screen is displayed, for example:



2. You can configure the following setting:

Setting	Description
Disable APIC	Select this setting if you are experiencing hardware problems. Disabling Advanced Programmable Interrupt Controller (APIC) improves compatibility with older hardware drivers that are not fully APIC-compliant.

3. Select **Ok** and press Enter to return to the Setup menu. To continue with the Setup program, select another Setup menu option and press Enter. To end the Setup program, select **Finished** and press Enter.

   If you have finished with the Setup program, the next step is to set administration account passwords. For more information, see *Setting Account Passwords* on page 29.

Setting Account Passwords

As part of setting up Network Guardian, you must specify passwords for the default admin and root accounts used to administer Network Guardian.

The passwords entered here will be required by administrators when accessing Network Guardian via the web-based interface and root account users when accessing Network Guardian using a console.

About Passwords

The passwords used by these accounts should be strong passwords that fulfil the following recommended conditions:

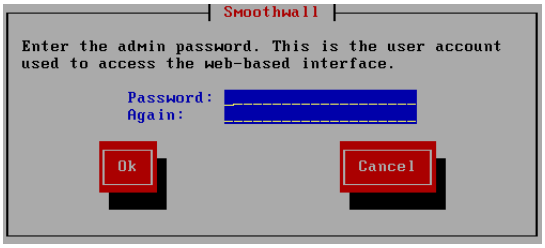
- Contain both upper and lower case characters: a-z, A-Z
- Contain numbers: 0-9
- Contain special characters, such as: `!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)`
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, or jargon
- Are not based on personal information, such as family or pet names
- Are never written down or stored on-line.

Setting Passwords

After completing the basic installation and either running or skipping the Setup program, you must set passwords for Network Guardian's admin and root accounts.

To set passwords:

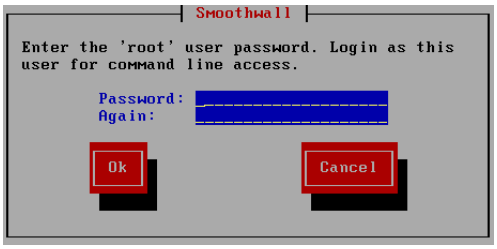
When the following screen is displayed:



1. Enter the following information:

Field	Explanation
Password	Enter a strong password for Network Guardian 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.

2. Select **Ok** and press Enter. The following screen is displayed:



3. Enter the following information:

Field	Explanation
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.

4. Select **Ok** and press Enter. The following screen is displayed:

5. Select **Ok** and press Enter to reboot the computer.

   After rebooting, you can access Network Guardian from a network client running a web browser. For more information, see *Chapter 5, Accessing Network Guardian* on page 31.

5 Accessing Network Guardian

In this chapter:

- How to access Network Guardian for the first time
- Registering Network Guardian
- Checking for updates

Accessing Network Guardian for the First Time

Note: The examples in the following sections are illustrated using Mozilla Firefox. You can access and administer Network Guardian using a browser of your choice.

To access Network Guardian for the first time:

1. In the browser of your choice, enter the address of your Network Guardian, for example: `https://10.0.0.3:441`

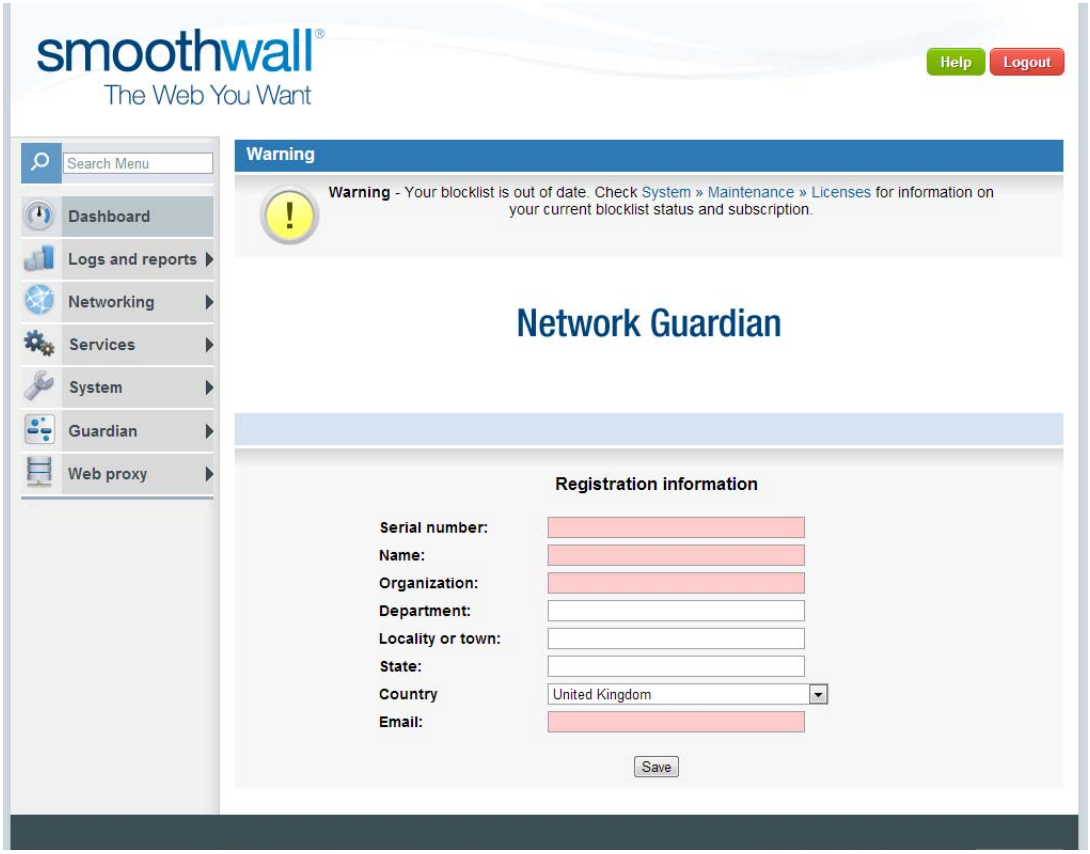
Note: The example address above uses HTTPS to ensure secure communication with your Network Guardian. It is possible to use HTTP on port 81 if you are satisfied with less security.

2. Accept Network Guardian's certificate. The login screen is displayed.
3. Enter the following information:

Field	Information
Username	Enter `admin`. This is the name of the default Network Guardian administrator account.
Password	Enter the password you specified for the admin account when installing Network Guardian. See *Chapter 2, Installing Network Guardian* on page 5 for more information.

4. Click **Login**.

The following page opens:

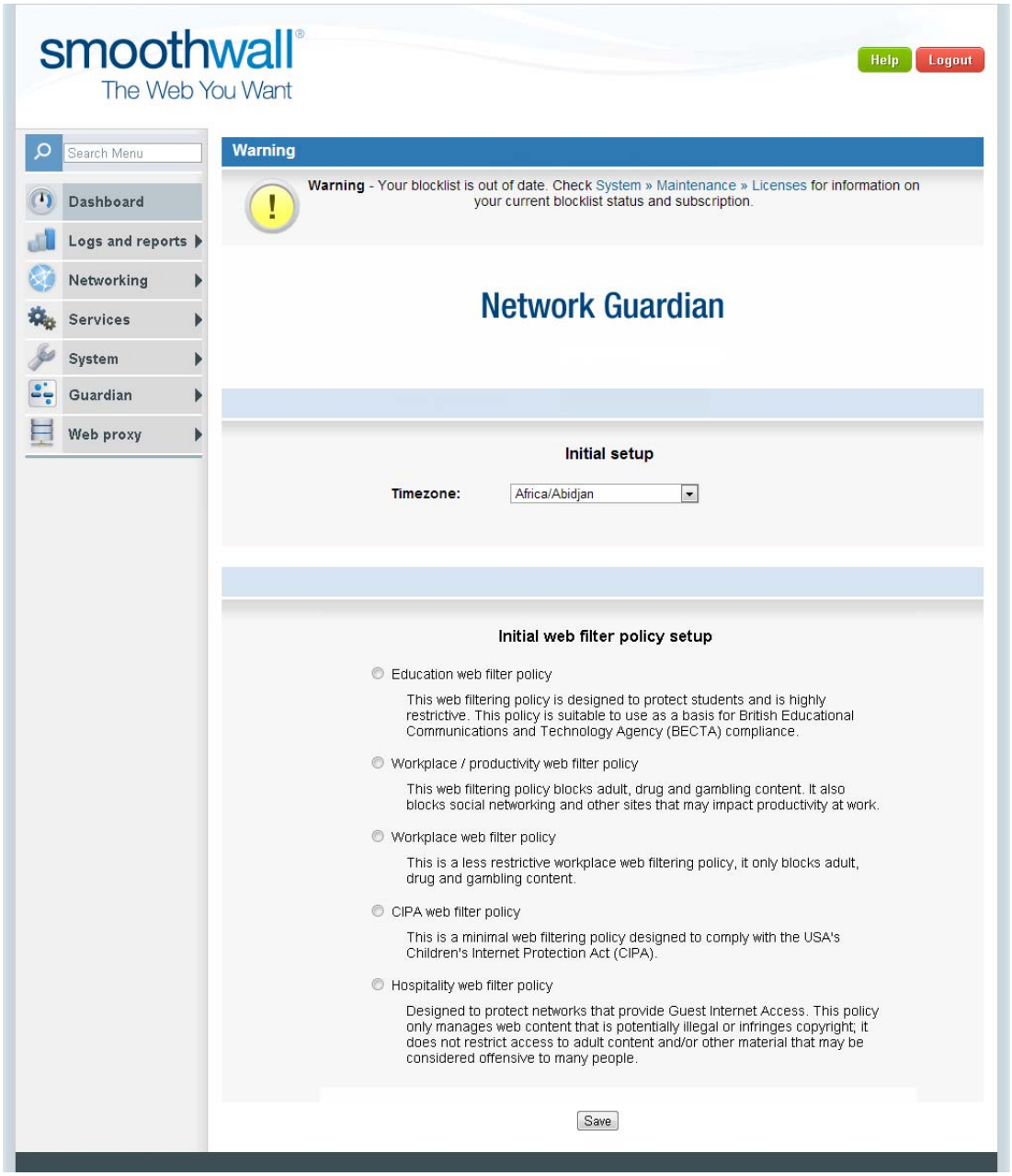


5. Enter the following information:

Information	Enter:
Serial number	The serial number you received with your copy of Network Guardian. Serial numbers are not case sensitive and can be entered with or without spaces. If you do not have a serial number, contact your Smoothwall representative or, visit http://www.smoothwall.net/ for more information.
Name	The name of the administrative contact person for Network Guardian.
Organization	The name of the organization in which Network Guardian will reside.
Department	The name of the department in which Network Guardian will reside.
Locality or town	Location information for Network Guardian.
State	Regional location information for Network Guardian.
Country	The country in which Network Guardian will reside
Email	The email address of the administrative contact for Network Guardian. This should be a valid and actively used email account.

6. Click **Save**. When prompted, review the information you have supplied and then click **Confirm**.

The following page opens:



7. Configure the following setting:

Setting	Description
Timezone	From the **Timezone** drop-down list, select your timezone.

Setting	Description
Initial web filter policy setup	Select one of the following web filter policies: **Education web filter policy** – This is designed to protect students and is highly restrictive. It is suitable to use as a basis for British Educational Communications and Technology Agency (BECTA) compliance. **Workplace/productivity web filter policy** – This policy blocks adult, drug and gambling content. It also blocks social networking and other sites that may impact productivity at work. **Workplace web filter policy** – This policy is a less restrictive workplace web filtering policy. It only blocks adult, drug and gambling content. **CIPA web filter policy** – This is a minimal web filtering policy designed to comply with the USA's Children's Internet Protection Act (CIPA). **Note:** The CIPA web filter policy does not include an intolerance category as the American Civil Liberties Union (ACLU) considers such a category to be a violation of the USA constitution's First Amendment. **Hospitality web filter policy** – this policy is designed to protect networks that provide guest internet access. It only manages web content that is potentially illegal or infringes copyright. It does not restrict access to adult content and/or other material that may be considered offensive to many people.

8. Click **Save**. The Dashboard opens:

The Dashboard is Network Guardian's default home page.

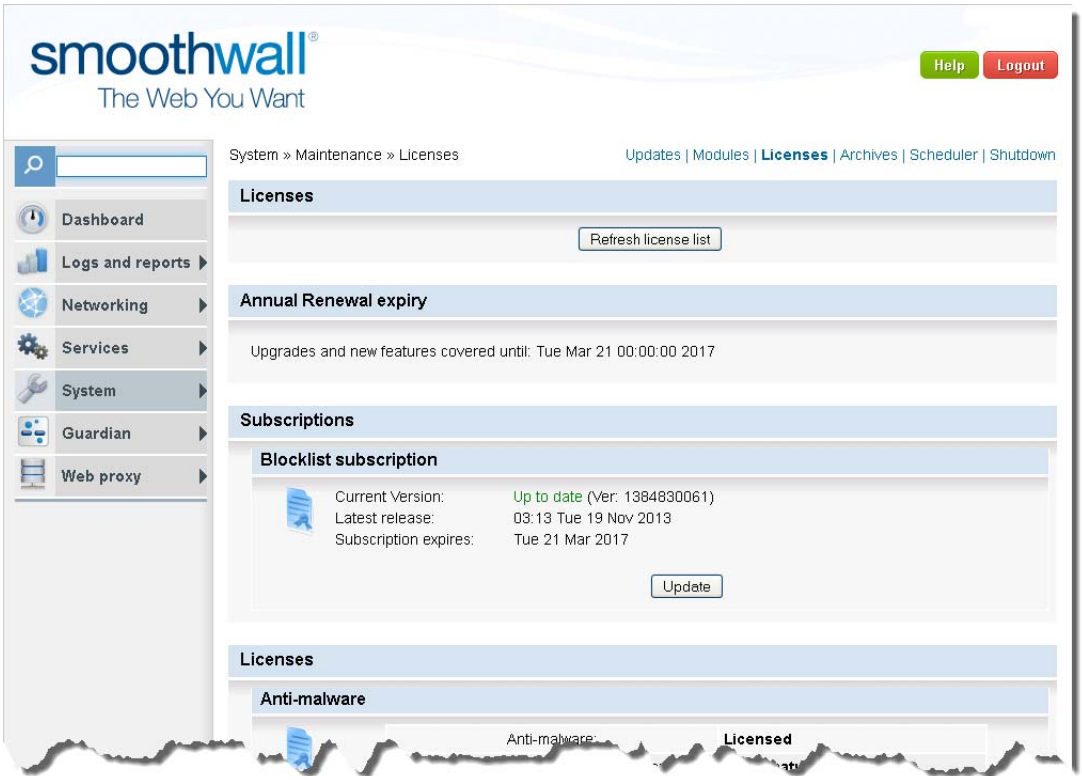
You can now review Network Guardian functionality. For more information, see the *Network Guardian Administrator's Guide*.

Getting the Latest Blocklists

A blocklist is a group of settings which is updated on a regular basis by Smoothwall to maintain Network Guardian's list of undesirable, inappropriate or objectionable content.

To get the latest blocklist:

1. Browse to the **System > Maintenance > Licenses** page:



2. Click **Update**. Network Guardian downloads and installs the latest blocklists.

Installing Updates

You should 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**. The Available updates area displays any updates available.
3. Click **Download updates** to get the updates and then click **Install updates**. The updates are installed.

   For full information on working with Network Guardian, see the *Network Guardian Administration Guide*.

Index


smoothwall®
The Web You Want