

smoothwall®

The Web You Want

Smoothwall S4 and S8 Appliances

S4 and S8 Appliances Getting Started Guide

For future reference

S4 and S8 serial number:

Date installed:

Smoothwall contact:

Smoothwall® S4 and S8, Getting Started Guide, May 2015

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of S4 and S8.

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 – 2015 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.

S4 and S8 contains graphics taken from the Open Icon Library project <http://openiconlibrary.sourceforge.net/>

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

Contents

	About This Guide	1
	Audience and Scope	1
	Organization and Use	1
	Conventions.....	2
	Related Documentation.....	2
Chapter 1	Introduction to the S4 and S8 Appliance	3
	About the S4 and S8 Appliance	3
	Reviewing Package Contents.....	3
	Reviewing the Panel and Ports.....	4
	The Panel Menu	5
Chapter 2	Installing the S4 and S8 Appliance	7
	Installing as a Basic Web Proxy	7
	Installing in Firewall Mode	8
Chapter 3	Getting Started	9
	Registering the S4 and S8 Appliance.....	9
	Configuring the S4 and S8 Appliances for Your Network.....	11
	Changing the IP Address	11
	Creating an External Connection.....	13
	Installing Updates	15
	Deploying a Guardian Web Security Policy	16
	Getting the Latest Guardian Blocklists.....	16
	Index.....	17

About This Guide

The Smoothwall S4 and S8 appliances, formally known as the SWG-700/1200 and the UTM-300/1000 appliances, are the hardware platforms required to run either Secure Web Gateway or Unified Threat Management.

This manual will guide you through the initial setup of an S4 and S8 appliance.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying an S4 and S8 appliance.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of Secure Web Gateway or Unified Threat Management
- 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:

- [Chapter 1, Introduction to the S4 and S8 Appliance on page 3](#)
- [Chapter 2, Installing the S4 and S8 Appliance on page 7](#)
- [Chapter 3, Getting Started on page 9](#)
- [Index on page 17](#)

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	S4 and S8 Smoothwall System
Menu flow, and screen objects	Bold	System > Maintenance > Shutdown Click Save
Cross-references	Blue text	See Chapter 1, Introduction to the S4 and S8 Appliance on page 3
References to other guides	Italics	Refer to the <i>S4 and S8 Administration Guide</i>
Filenames and paths	Courier	The <code>portal.xml</code> file
Variables that users replace	<i>Courier Italics</i>	<code>http://<my_ip>/portal</code>
Links to external websites	Blue text, underlined	Refer to http://www.smoothwall.net/support
Smoothwall System	This may be one of: <ul style="list-style-type: none"> Unified Threat Management Secure Web Gateway 	

This guide is written in such a way as to be printed on both sides of the paper.

Related Documentation

The following guides provide additional information relating to the S4 and S8 application:

- *Secure Web Gateway Administration Guide*, which describes how to configure Secure Web Gateway
- *Secure Web Gateway Operations Guide*, which describes how to use Secure Web Gateway
- *Secure Web Gateway User Portal Guide*, which describes how to use the Secure Web Gateway user portal
- *Unified Threat Management Administration Guide*, which describes how to configure Unified Threat Management
- *Unified Threat Management Operations Guide*, which describes how to use Unified Threat Management
- *Unified Threat Management User Portal Guide*, which describes how to use the Unified Threat Management user portal
- <http://www.smoothwall.net/support> contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introduction to the S4 and S8 Appliance

About the S4 and S8 Appliance

The Smoothwall S4 and S8 appliances are the hardware platforms required to run either Secure Web Gateway or Unified Threat Management.

The S4 and S8 appliance can be installed to run in either firewall-mode, or basic-mode.

For the latest product documentation, refer to <http://www.smoothwall.net/support>.

Reviewing Package Contents

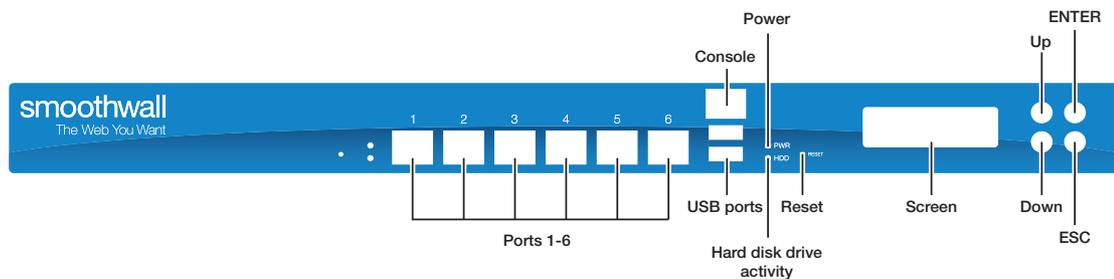
Your S4 and S8 package contains the items you will need to set up an S4 and S8 initially.

Verify that you have the following components:

Component	Information
S4 and S8	The S4 and S8 appliance.
AC power cord	Provided with S4 and S8.
Ethernet crossover cable	Provided with S4 and S8.
S4 and S8 Getting Started Guide	This guide.
Information sheets	Applicable warranty and certification sheets.
An RJ45 to DB9 RS232 cable	Keep this cable safe and to hand with the S4 and S8 appliances. It may be needed in the future in order to gain RS232 console access.

Reviewing the Panel and Ports

The graphic below provides an overview of the S4 and S8 appliance's ports, buttons and screen:



Object	Description
Ports	<p>Port 1 is the default interface.</p> <p>The other ports can be used to provide internal networking zones and external connections.</p> <p>If required, you can configure ports 3 and 4 to be shorted together to provide a bypass port. This leaves the client network with unfiltered network access without having to re-cable.</p> <p>For a detailed description of how to configure bypass ports, refer to your <i>Smoothwall System's Administration Guide</i>.</p>
Console	Can be used to connect a serial console and administer the S4 and S8 appliances.
USBs	For keyboard access, if required.
Power	<p>Indicates when the power supply to the S4 and S8 appliance is on. The power switch is at the rear.</p> <p>To initiate a clean shutdown when the S4 and S8 appliance is running, press the power switch.</p> <p>To force a power off, press and hold the power switch for five seconds.</p> <p>Note: It is not usually necessary to use the power switch to power on the S4 and S8 appliance, as applying mains power should automatically start it.</p>
Hard disk drive activity	Indicates hard disk drive activity.
Reset	Can be used to reset the S4 and S8 appliance if it becomes unresponsive.
Screen	<p>By default, the panel screen runs in information mode and displays the following information:</p> <ul style="list-style-type: none"> • Current bandwidth usage on the external connection • The internal IP address • Current memory usage • The hostname • Time and date <p>This is also where you view and access the panel menu options available.</p>

Object	Description
Up	Used to access and scroll through the panel menu.
Down	Used to access and scroll through the panel menu.
ESC	Used to cancel panel menu options.
ENTER	Used to select and confirm panel menu options. This button can also be used to advance the display of information when the LCD is in idle mode.

The Panel Menu

The panel menu enables you to reset administrator access and settings as well as reboot or shut down the S4 and S8 appliances.

To access the panel menu, do the following:

1. Press either the **Up** or **Down** button to access the menu.
2. Continue to press the **Up** or **Down** button to navigate through the various menu options. The menu options available are:
 - **Reset Admin Access** — Select to reset the default rule which allows administrators to access and configure the S4 and S8 appliances from any source IP that can route to the first network interface.
 - **Restore Default Settings** — Restores the S4 and S8 appliances to the settings it had on first boot.
 - **Reboot** — Reboots the S4 and S8 appliances immediately.
 - **Shutdown** — Prompts the S4 and S8 appliances to perform a system shutdown.
 - Select the option you require and press **ENTER** to confirm your selection.

2 Installing the S4 and S8 Appliance

This chapter describes the steps needed to install the S4 and S8 appliance in a number of scenarios, including:

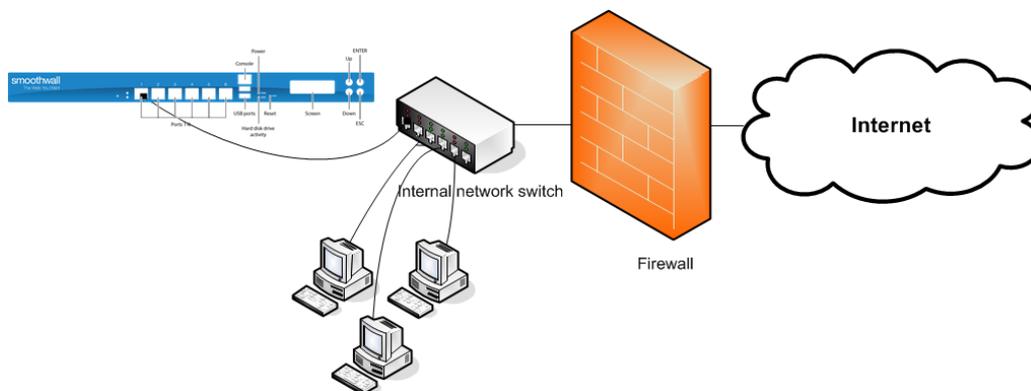
- [Installing as a Basic Web Proxy on page 7](#)
- [Installing in Firewall Mode on page 8](#)

Installing as a Basic Web Proxy

This is the simplest scenario. The S4 and S8 appliance is deployed using only one interface plugged into the network. Typically, this is used in a Secure Web Gateway installation.

To configure a basic installation, do the following:

1. Place the appliance in a stable and secure location.
2. Connect an ethernet cable from port 1 to your network; the other ports are not used:



3. Using the supplied AC power cord, connect the appliance to the power supply.
The appliance boots.

If the appliance does not power on and boot automatically, use the power switch on the back panel.

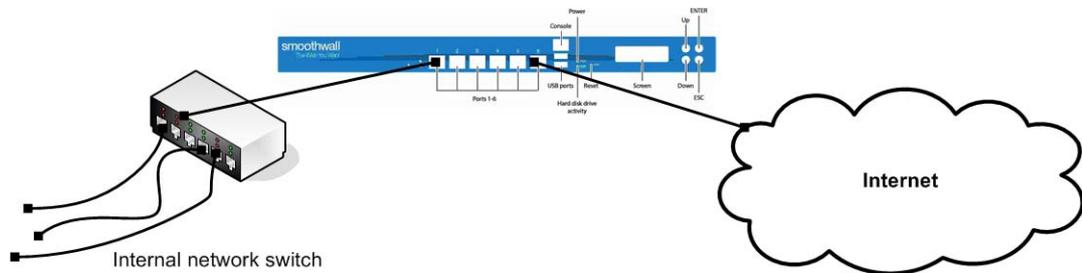
For a detailed description of how to register your appliance, see [Chapter 3, Getting Started on page 9](#).

Installing in Firewall Mode

This section describes how to install the appliance as a firewall. Typically, this is used in a Unified Threat Management installation.

To install the appliance as a firewall, do the following:

1. Place the appliance in a stable and secure location.
2. Connect an ethernet cable from your network switch to port 1 of the appliance.
3. Connect an ethernet cable from port 6 on the appliance to an external network, or internet-connected router or firewall.



4. Using the AC power cord, connect the appliance to the power supply.

The appliance boots.

If the appliance does not power on and boot automatically, use the power switch on the back panel.

For a detailed description of how to register your appliance, see [Chapter 3, Getting Started on page 9](#).

3 Getting Started

This chapter describes the initial setup of the S4 and S8 appliance, including:

- [Registering the S4 and S8 Appliance on page 9](#)
- [Configuring the S4 and S8 Appliances for Your Network on page 11](#)
- [Installing Updates on page 15](#)
- [Deploying a Guardian Web Security Policy on page 16](#)
- [Getting the Latest Guardian Blocklists on page 16](#)

Registering the S4 and S8 Appliance

You must register the S4 and S8 appliance before you can use it.

Note: The appliance comes with pre-assigned internal IP addresses to allow access for the initial configuration, after which you must change them. For more information, see [Changing the IP Address on page 11](#).

To register the appliance, do the following:

1. From a computer on the same subnet as the Smoothwall System, start a web browser and connect to Smoothwall System via HTTPS, using the following URL:

```
https://192.168.110.1:441/
```

If the computer is not in the same subnet, you can add an alias or second IP to your computer's network card, for example: 192.168.110.2 subnet mask 255.255.255.0.

If your appliance is used in a Secure Web Gateway installation, and you need to specify a gateway, use one appropriate to your network.
2. Accept the appliance's security certificate and when the Login page opens, enter the following credentials:
 - **Username** — Enter `admin`. This is the default account used to administer the Smoothwall System.
 - **Password** — Enter `smoothwall`. This is the default password for the `admin` username.

3. Click **Login**.
4. When prompted, enter the following information:
 - **Serial number** — The software license key as received from your Smoothwall representative.
The serial number determines if the appliance is configured as Secure Web Gateway or as Unified Threat Management.
 - **Name** — The name of your organization's contact person for the appliance.
 - **Organization** — The name of your organization.
 - **Department** — The department in which the appliance 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 the appliance.
5. Click **Save**.
Review the information you have supplied.
6. Click **Confirm**.
The appliance reboots and configures its initial settings. This can take up to five minutes to complete.
Once the appliance has rebooted, the browser will refresh back to the login prompt.
7. Re-enter the default username and password.
8. Click **Login**.
9. When prompted, enter the following information:
 - **Timezone** — From the **Timezone** drop-down list, select your timezone.
 - **Initial web filter policy setup** — Select one of the following web filter policies:

Option/field	Description
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.

Option/field	Description
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.

10. Click **Save**.

The appliance applies your selection and displays the Dashboard which is its default home page containing external connectivity controls and a number of reports.

Configuring the S4 and S8 Appliances for Your Network

To use the S4 and S8 appliance on your network, you must do the following:

- [Changing the IP Address on page 11](#)
- [Creating an External Connection on page 13](#)

Changing the IP Address

The S4 and S8 appliances have pre-assigned internal IP addresses. You must change them to make the appliance accessible on your network.

Tip: The safest method is to add an additional IP address to the interface, then delete the pre-assigned address. This way, should the wrong IP address be configured, you can still access the administration user interface to correct it.

To change the IP address, do the following:

1. Browse to **Networking > Configuration > Interfaces**.
2. Click the **IP addresses** link for the relevant interface to display the **Attached addresses** table.
3. Click **Add new IP address**.
4. Configure the following:
 - **Status** — New IP addresses are enabled by default. Clear the check box to create a disabled IP address.
 - **Type** — Choose whether this IP address is assigned a static IP address (**Static IPv4**), or an IP address assigned via DHCP (**DHCP IPv4**).

Depending the type of IP address, additional parameters may require configuration:

Use as	Additional Parameter	Description
Static IPv4	IP address	Enter the additional IP address for this interface.
	Subnet mask	Enter the subnet mask for the IP address
	Gateway	If traffic from this IP address needs to go through a gateway, select User defined , and either enter it into the box provided, or choose it from the drop-down list. Else, leave None selected.
	Bandwidth	This parameter is only displayed if a User defined Gateway is configured. If multiple gateways are configured and used, enter the minimum bandwidth used to load balance traffic between connections. If a single gateway is configured, load balancing is not used so this parameter can be left at 1. Select whether the configured value is in kilobits per second (kbps), or in megabits per second (Mbps).
	Connection monitoring	This parameter is only displayed if a User defined Gateway is configured. Connection monitoring is enabled by default. It is not recommended you disable connection monitoring, otherwise S4 and S8 assumes the gateway always has an internet connection.
DHCP IPv4	Bandwidth	If multiple gateways are configured and used, enter the minimum bandwidth used to load balance traffic between connections. If a single gateway is configured, load balancing is not used so this parameter can be left at 1. Select whether the configured value is in kilobits per second (kbps), or in megabits per second (Mbps).
	Connection monitoring	Connection monitoring is enabled by default. It is not recommended you disable connection monitoring, otherwise S4 and S8 assumes the gateway always has an internet connection.
	DHCP client hostname	Optionally, enter the DHCP client hostname as specified by the DHCP server.

- ♦ **Comment** — Configure an optional comment for this IP address.

An additional button, **Show comments**, is displayed on the **Attached addresses** table if any comments are configured. Clicking this displays configured comments under the IP address.

5. Click **Add**.

The appliance applies the new IP address to the interface.

6. Log out of the administration user interface, and browse to the new IP address, using port 81.
7. Browse to **Networking > Configuration > Interfaces**.
8. Click the **IP addresses** link for the relevant interface to display the **Attached addresses** table.
9. Locate and highlight the pre-assigned IP address.
10. Click **Delete**.
11. Browse to **Networking > Configuration > DNS**.
12. From the **Global** panel, select **User defined**.
13. Configure the primary DNS server, and secondary DNS server if required, in the relevant boxes.
14. Click **Save changes**.

You can choose to use the Smoothwall System's internal DNS server instead, but you must ensure you add the DNS server details that the internal DNS proxy uses. For a detailed description of how to configure your Smoothwall System to use this, refer to your *Smoothwall System's Administration Guide*.

15. Browse to the **Web proxy > Web proxy > Settings**.
16. Click **Save and Restart** to apply the changes to the web proxy.

Creating an External Connection

If your Smoothwall System is to provide access to the Internet, you must configure the connection details as follows:

Note: The following instructions are for external connections made through a NIC (Network Interface Card) interface. You can also configure an external connection to use a PPPoE connection. For a detailed description of how to configure a PPPoE connection, refer to your *Smoothwall System's Administration Guide*.

1. Browse to **Networking > Configuration > Interfaces**.
2. Highlight the relevant interface, and click **Edit**.
3. Configure the following:
 - **Name** — Configure a meaningful name for this connection.
 - **Use as** — Select **External**.
 - **Spoof MAC** — If MAC address spoofing is required, enter the new MAC address here.
 - **MTU** — If required, you can set the Maximum Transmission Unit (MTU) size, in bytes, this connection.
 - **Comment** — Configure an optional comment for this external interface.

An additional button, **Show comments**, is displayed on the **Ethernet interfaces** table if any comments are configured. Clicking this displays configured comments under the interface name.

4. Click **Add**.

You must assign the IP address, and gateway if provided, as advised by your ISP. This can either be a static IP address or one assigned dynamically.

5. Click the **IP addresses** link for the external interface to display the **Attached addresses** table.6. Click **Add new IP address**.

7. Configure the following:

- **Status** — New IP addresses are enabled by default. Clear the check box to create a disabled IP address.
- **Type** — Choose whether this IP address is assigned a static IP address (**Static IPv4**), or an IP address assigned via DHCP (**DHCP IPv4**).

Depending the type of IP address, additional parameters may require configuration:

Use as	Additional Parameter	Description
Static IPv4	IP address	Enter the additional IP address for this interface.
	Subnet mask	Enter the subnet mask for the IP address
	Gateway	If traffic from this IP address needs to go through a gateway, select User defined , and either enter it into the box provided, or choose it from the drop-down list. Else, leave None selected.
	Bandwidth	This parameter is only displayed if a User defined Gateway is configured. If multiple gateways are configured and used, enter the minimum bandwidth used to load balance traffic between connections. If a single gateway is configured, load balancing is not used so this parameter can be left at 1. Select whether the configured value is in kilobits per second (kbps), or in megabits per second (Mbps).
	Connection monitoring	This parameter is only displayed if a User defined Gateway is configured. Connection monitoring is enabled by default. It is not recommended you disable connection monitoring, otherwise S4 and S8 assumes the gateway always has an internet connection.

Use as	Additional Parameter	Description
DHCP IPv4	Bandwidth	If multiple gateways are configured and used, enter the minimum bandwidth used to load balance traffic between connections. If a single gateway is configured, load balancing is not used so this parameter can be left at 1. Select whether the configured value is in kilobits per second (kbps), or in megabits per second (Mbps).
	Connection monitoring	Connection monitoring is enabled by default. It is not recommended you disable connection monitoring, otherwise S4 and S8 assumes the gateway always has an internet connection.
	DHCP client hostname	Optionally, enter the DHCP client hostname as specified by the DHCP server.

- **Comment** — Configure an optional comment for this IP address.

An additional button, **Show comments**, is displayed on the **Attached addresses** table if any comments are configured. Clicking this displays configured comments under the IP address.

8. Click **Add**.

The appliance applies the new IP address to the interface.

Note: IPv6 is not yet supported. For more information, refer to your Smoothwall representative.

Installing Updates

You must ensure the S4 and S8 appliance has the latest Smoothwall updates installed.

To check for and install updates, do the following:

1. Browse to **System > Maintenance > Updates**.

2. Click **Refresh update list**.

If there are updates available these will be listed under **Available updates**.

3. Click **Download Updates**.

The S4 and S8 appliance downloads the updates and lists them under **Pending updates**.

4. Click **Install**.

The S4 and S8 appliance installs the updates and prompts you to reboot if necessary.

5. Click **rebooted** in the prompt text.

6. Select **Immediately** and click **Reboot**.

The Smoothwall logo is displayed whilst the system is rebooting. This screen will refresh to the login prompt once the reboot has completed.

For a detailed description of further configuration needed for your Smoothwall System, refer to your *Smoothwall System's Administration Guide*.

Deploying a Guardian Web Security Policy

Note: The following instructions are for a Microsoft Windows™ environment, using Internet Explorer as the browser. For more information about other supported platforms, refer to your Smoothwall representative.

The Smoothwall System comes with a comprehensive web security policy in place.

To deploy the policy, do the following:

1. From a network client, start Internet Explorer.
2. From the **Tools** menu, select **Internet Options**.
3. On the **Connections** tab, click **LAN settings**.
4. Within the **Proxy server** panel, select **Use a proxy server for your LAN ...**
5. Enter the Smoothwall System's IP address and the port number of 800.
6. Click **Advanced**.
7. In the **Exceptions** panel, enter the Smoothwall System's IP address, and any other IP addresses to content that you do not want filtered, for example, your intranet or local wiki.
8. Click **OK**, **OK** and **OK** to save the settings.

You can utilize additional methods to deploy the Guardian web security policy on your network devices. For more information, refer to your *Smoothwall System's Administration Guide*.

Getting the Latest Guardian Blocklists

Guardian blocklists are groups of settings, which are updated on a regular basis by Smoothwall, to maintain the Smoothwall System's list of undesirable, inappropriate or objectionable content.

To update Guardian blocklists, do the following:

1. Browse to **System > Maintenance > Licenses**.
2. Within the **Blocklist subscriptions** panel, click **Update**.

The Smoothwall System downloads and installs the latest blocklist.

Note: After this initial blocklist download, the Smoothwall System automatically checks for and downloads updated blocklists daily.

For more information about using Guardian's block lists and customizing web security policies, refer to your *Smoothwall System's Administration Guide*.

Index

B

basic installation 7
blocklists 16

C

configuring 11
 IP address 11

F

firewall installation 8

I

installing 7
 basic 7
 firewall 8
 web proxy 7
IP address 11

P

panel
 menu 5
policies 16

R

registering 9

T

training 1

U

updates 15

W

web proxy installation 7

smoothwall[®]

The Web You Want