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, December 2014

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.

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

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: 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

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:

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 *S4 and S8 Administration Guide*
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`
Links to external websites	Blue text, underlined	Refer to http://www.smoothwall.net/support

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, 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.

The S4 and S8 appliance can be installed to run in either firewall-mode (for Unified Threat Management installations), or, in bridge-mode or basic-mode (for Secure Web Gateway installations).

Reviewing Package Contents

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

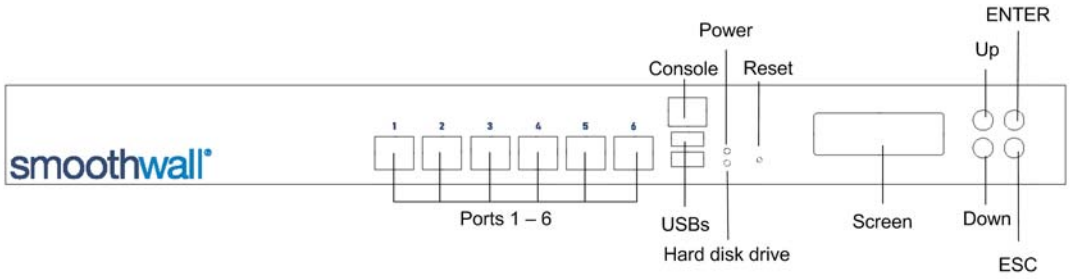
Verify that you have the following components:

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.

Component	Information
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	Port 1 is the default interface. The other ports can be used to provide internal networking zones and external connections. If your S4 and S8 appliance is being installed in bridge mode, use the ports as follows: • Port 3 is the first bridge port • Port 4 is the second bridge port • Ports 2, 5, and 6 are additional network interfaces • Port 1 is the default interface When the S4 and S8 appliance is not powered up, ports 3 and 4 are shorted together, leaving the client network with unfiltered network access without having to re-cable. **Note:** Ports 3 and 4 should not be used for any purpose other than bridging. It is not possible to reuse the ports if bridging mode is not needed.
Console	Can be used to connect a serial console and administer the S4 and S8 appliances.
USBs	Reserved for future use.
Power	Indicates when the power supply to the S4 and S8 appliance is on. The power switch is at the rear. To initiate a clean shutdown when the S4 and S8 appliance is running, press the power switch. To force a power off, press and hold the power switch for five seconds. **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.
Hard disk drive	Indicates hard disk drive activity.
Reset	Can be used to reset the S4 and S8 appliance if it becomes unresponsive.

Object	Description
Screen	By default, the panel screen runs in information mode and displays the following information: • Current bandwidth usage on the external connection • The internal IP address • Current memory usage • The hostname • Time and date This is also where you view and access the panel menu options available.
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.
3. Select the option you require and press **ENTER** to confirm your selection.

2 Installing the S4 and S8 Appliance

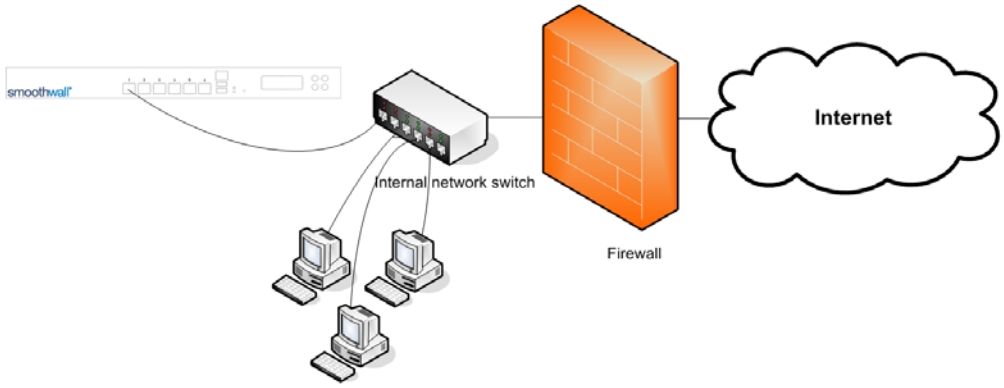
This chapter describes the steps needed to install the S4 and S8 appliance in a number of scenarios, including:

Installing as a Basic Installation

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 S4 or S8 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 S4 or S8 appliance to the power supply.

   The S4 or S8 appliance boots.

   If the S4 or S8 appliance does not power on and boot automatically, use the power switch on the back panel.

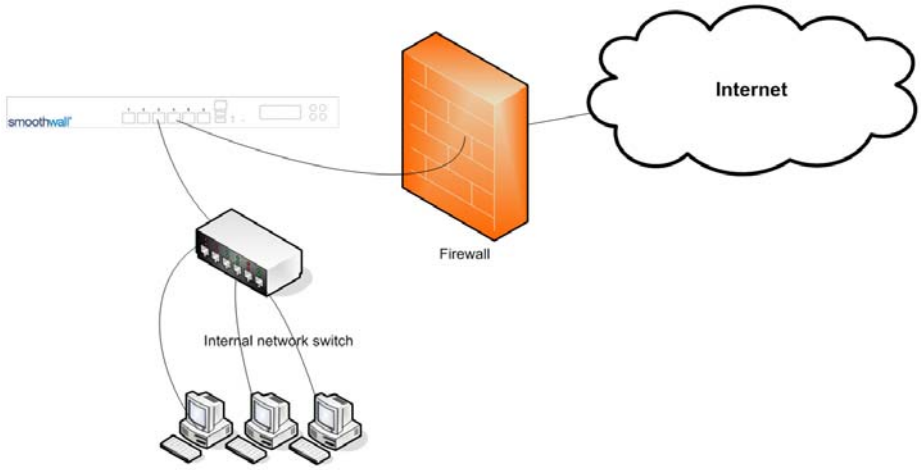
Once installed, you can review the panel menu, and access and register the S4 or S8 appliance.

Installing in Bridge-Only Mode

In this scenario, the bridge is used to both administer the S4 or S8 appliance, and to filter the client network. Administration access can be gained by connecting from either side of the bridge. Typically, this is used in a Secure Web Gateway installation.

To install in bridging-only mode, do the following:

1. Place the S4 or S8 appliance in a stable and secure location.
2. Connect an ethernet cable from port 3 to your client PC switch.
3. Connect an ethernet cable from port 4 to your network firewall.



4. Using the supplied AC power cord, connect the S4 or S8 appliance to the power supply.

   The S4 or S8 appliance boots.

   If the S4 or S8 appliance does not power on and boot automatically, use the power switch on the back panel.

Note: It does not matter which of ports 3 and 4 are connected to the switch or the firewall. Ports 1, 2, 5, and 6 can be used as additional network interfaces. There is no need to reconfigure clients on the bridge. As far as they are concerned, the bridge does not exist.

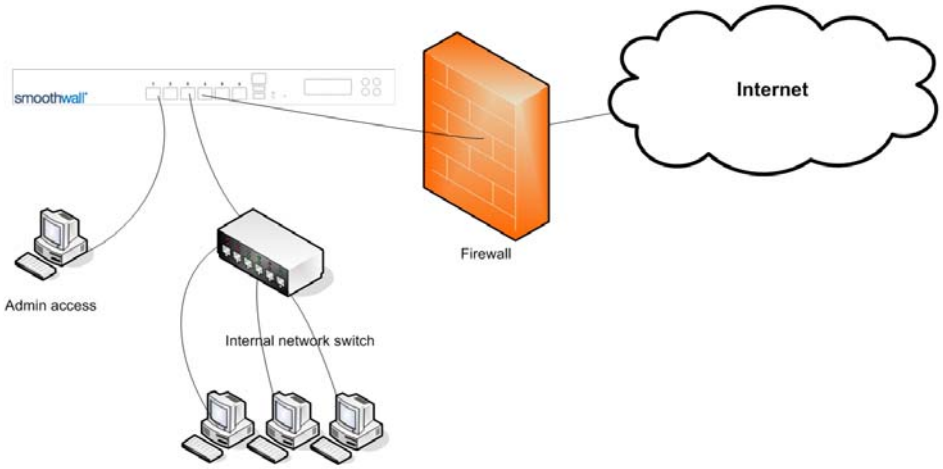
Once installed, you can review the panel menu, and access and register the S4 or S8 appliance.

Installing in Bridge and Administration Mode

In this scenario, port 1 is used only to administer the S4 or S8 appliance. The bridging ports are used to protect the client network. Typically, this is used in a Secure Web Gateway installation.

To configure bridging and separate administration mode, do the following:

1. Place the S4 or S8 appliance in a stable and secure location.
2. Connect an ethernet cable from your administrator computer to port 1.
3. Connect an ethernet cable from port 3 to your client PC switch.
4. Connect an ethernet cable from port 4 to your network firewall.



5. Using the supplied AC power cord, connect the S4 or S8 appliance to the power supply.

   The S4 or S8 appliance boots.

   If the S4 or S8 appliance does not power on and boot automatically, use the power switch on the back panel.

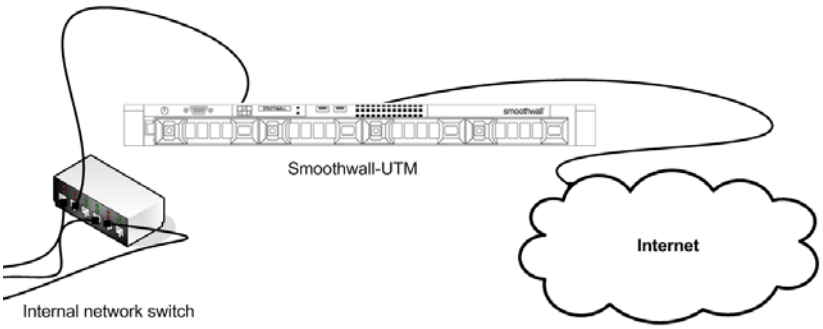
Note: Ports 2, 5, and 6 can be used as additional network interfaces. There is no need to reconfigure clients on the bridge. As far as they are concerned, the bridge does not exist.

Installing in Firewall Mode

This section describes how to install the S4 or S8 appliance as a firewall. Typically, this is used in a Unified Threat Management installation.

To install the S4 or S8 appliance as a firewall, do the following:

1. Place the S4 or S8 appliance in a stable and secure location.



2. Connect an ethernet cable from your network switch, or the supplied crossover cable from your computer, to port 1 of the S4 or S8 appliance.
3. Connect an ethernet cable from a port on the S4 or S8 appliance to an external network, or internet, access point.
4. Using the AC power cord, connect the S4 or S8 appliance to the power supply.

   The S4 or S8 appliance boots.

   If the S4 or S8 appliance does not power on and boot automatically, use the power switch on the back panel.

3 Getting Started

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

Registering the S4 and S8 Appliance

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

Note: The S4 and S8 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 13.

To register the S4 and S8 appliance, do the following:

1. From a computer on the same subnet as the S4 and S8 appliance, start a web browser and connect to the S4 and S8 via HTTPS, using the following URLs:
   - In bridge mode, enter: `https://192.168.111.1:441/`

     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: 192.168.111.2 subnet mask 255.255.255.0. If you need to specify a gateway, use 192.168.111.1.
   - In all other modes, enter: `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 you need to specify a gateway, use 192.168.110.1.

2. Accept the S4 and S8 appliance's security certificate and when the Login page opens, enter the following information:

Field	Explanation
Username	Enter `admin` – the default account used to administer the S4 and S8 appliance.
Password	Enter `smoothwall` – the default password for the administrator's account.

3. Click **Login**, the S4 and S8 appliance about page opens. Enter the following information:

Field	Enter
Serial number	The software license key as received from your Smoothwall sales representative or Smoothwall partner. The serial number determines if the S4 and S8 appliance is configured as Secure Web Gateway or as Unified Threat Management.
Name	The name of your organization's contact person for the S4 and S8 appliance.
Organization	The name of your organization.
Department	The department in which the S4 and S8 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 S4 and S8 appliance.

4. Click **Save**.

   The S4 and S8 appliance prompts you to review the information you have supplied.

5. Click **Confirm**.

   The S4 and S8 appliance reboots and configures its initial settings. This can take up to five minutes to complete.

   Once the S4 and S8 appliance has rebooted, the browser will refresh back to the login prompt.

6. Re-enter the default username and password.

7. Click **Login** and when prompted, enter the following information:

Option/field	Description
Timezone	From the **Timezone** drop-down list, select your timezone.
Admin password	Enter a new administration password.
Again	Re-enter the administration password to confirm it.
Root password	Enter a new root password.
Again	Re-enter the root password to confirm it.

Option/field	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 S4 and S8 appliance applies your selection and displays the Dashboard which is its default home page. The control page contains external connectivity controls and a number of reports.

Configuring the S4 and S8 Appliance for Your Network

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

- Changing the IP Address on page 13 — For all installation modes
- Connecting to the Internet on page 14 — For firewall mode installations only

Changing the IP Address

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

To change the IP address, do the following:

1. Browse to **Networking > Interfaces > Connectivity**.
2. Within the **Static Ethernet settings** panel, configure the following:
   - **Interface** — From the drop-down menu, select the interface to change the IP address for.
   - **Address** — Specify an internal IP address.

- **Primary DNS** — Specify the primary DNS address.
- **Default gateway** — Specify the default gateway for this appliance.
- **Netmask** — Specify the netmask.
- **Secondary DNS** — If required, specify a secondary DNS address.

3. Click **Save and connect**.

   The S4 and S8 appliance automatically restarts. This can take some time and may interrupt some services.

4. After 15 seconds, browse to the new IP address, using port 81.
5. When prompted, enter your user name and password.
6. Browse to the **Web proxy > Web proxy > Settings**.
7. Click **Save and Restart** to apply the changes to the web proxy.

Additionally, if you have deployed the S4 and S8 appliance in a Secure Web Gateway environment, you must configure the following additional parameters:

1. Browse to **Networking > Interfaces > Interfaces**.
2. Within the **Global settings** panel, configure the following:
   - **Default gateway** — Enter the IP address of your network's default gateway.
   - **Primary DNS** — Enter the IP address of your primary DNS.
   - **Secondary DNS** — Optionally, enter the IP address of your secondary DNS.
3. Click **Save changes**.

Connecting to the Internet

If you have deployed the S4 and S8 appliance in a Unified Threat Management environment, you must configure an internet connectivity profile.

To configure an internet connectivity profile, do the following:

1. Browse to **Networking > Interfaces > Connectivity**.
2. Within the **Profiles** panel, enter a name for the connectivity profile in the **Profile name** box.
3. Within the **Global settings** panel, select the connection method that fits your ISP's specifications from the **Method** drop-down menu.
4. Configure the parameters accordingly.
5. Click **Update**.
6. Click **Save and connect** to save the profile and connect the S4 and S8 appliance to the Internet.

For a detailed description of the internet connectivity profile parameters, refer to the *Unified Threat Management Administration Guide*.

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 the S4 and S8 appliance, refer to the *Unified Threat Management Administration Guide*, or the *Secure Web Gateway Administration Guide*.

Deploying a Guardian Web Security Policy

The S4 and S8 appliance comes with a comprehensive web security policy in place.

Note: The following explains how to deploy the default web security policy on a user's computer, with Internet Explorer 10 installed as the web browser.

To deploy the policy, do the following:

1. 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 S4 and S8 appliance's IP address and the port number of 800.
6. Click **Advanced**.
7. In the **Exceptions** panel, enter the S4 and S8 appliance'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.

If you have deployed the S4 and S8 appliance in a Unified Threat Management environment, you can utilize additional methods to deploy the Guardian web security policy on your network devices. For more information, refer to the *Unified Threat Management 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 S4 and S8 appliance'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 S4 and S8 appliance downloads and installs the latest blocklist.

Note: After this initial blocklist download, the S4 and S8 appliance automatically checks for and downloads updated blocklists daily.

For more information about using Guardian's block lists and customizing web security policies, refer to the *Unified Threat Management Administration Guide*, or the *Secure Web Gateway Administration Guide*.

Index


smoothwall®
The Web You Want