smoothwall®

The Web You Want

Smoothwall S12 Appliance

S12 Getting Started Guide

For future reference

S12 serial number:

Date installed:

Smoothwall contact:

Smoothwall® S12, Getting Started Guide, December 2014

Trademark notice

Acknowledgements

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

The Smoothwall S12 Appliance, formally known as the SWG-3600 and the UTM-3000, is the hardware platform required to run either Secure Web Gateway or Unified Threat Management.

This manual will guide you through the initial setup of an S12 Appliance.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying an S12 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	S12 Smoothwall System
Menu flow, and screen objects	**Bold**	**System > Maintenance > Shutdown** Click **Save**
Cross-references	Blue text	See Chapter 1, Introduction to the S12 Appliance on page 3
References to other guides	Italics	Refer to the *S12 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 S12 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 S12 Appliance

The Smoothwall S12 Appliance, formally known as the SWG-3600 appliance and the UTM-3000 appliance, is the hardware platform required to run either Secure Web Gateway or Unified Threat Management.

About the S12 Appliance

The S12 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 S12 package contains the items you will need to set up S12 initially.

Verify that you have the following components:

Component	Information
S12	The S12 appliance.
AC power cord	Provided with S12.
Ethernet crossover cable	Provided with S12.
Rack-mounting kit	Supplied in supplementary box carton.
S12 Getting Started Guide	This guide.
Information sheets	Applicable warranty and certification sheets.

Reviewing the Panel and Ports

The following graphics and section provide an overview of S12 power and ports:

Ports 1-6

Back

Ports 1-6

Back

Object	Description
Power-on indicator, power button	The power-on indicator lights when the system power is on. To force a shutdown, press and hold the power button for five seconds.
Ports	Port 1 is the default interface. The other ports can be used to provide internal networking zones and external connections. If your S12 is being installed in bridge-only mode, use the ports as follows: • Port 4 is the first bridge port • Port 3 is the second bridge port • Ports 2, 5, and 6 are additional network interfaces • Port 1 is the default interface When the S12 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.

Note: At the rear, there is also a serial console port, which can be used to connect a serial console to administer the S12 Appliance.

2 Installing the S12 Appliance

This chapter describes the steps needed to install the S12 Appliance in a number of scenarios, including:

Installing as a Basic Installation

This is the simplest scenario. The S12 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 S12 Appliance in a stable and secure location.

2. Connect an ethernet cable from port 1 to your network; the other ports are not used:
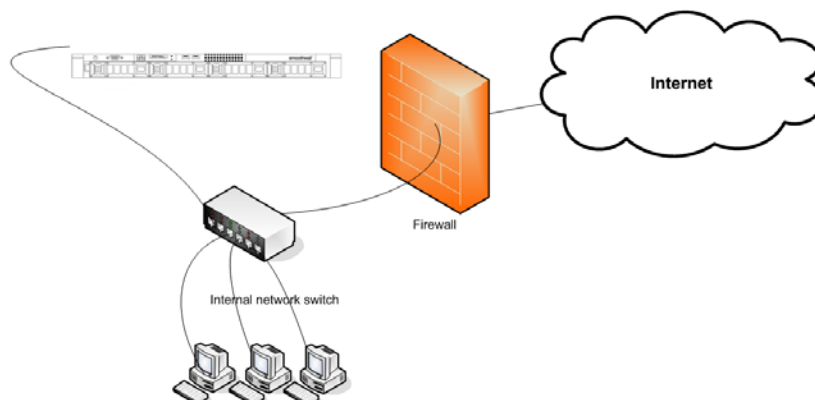
3.   Using the supplied AC power cord, connect the S12 Appliance to the power supply.

     The S12 Appliance boots.

Once installed, you can review the panel menu, and access and register the S12 Appliance.

Installing in Bridge-Only Mode

In this scenario, the bridge is used to both administer the S12 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 S12 Appliance in a stable and secure location.

2.   Connect an ethernet cable from port 4 to your client PC switch.

3.   Connect an ethernet cable from port 3 to your network firewall.

4.   Using the supplied AC power cord, connect the S12 Appliance to the power supply.

     The S12 Appliance boots.

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 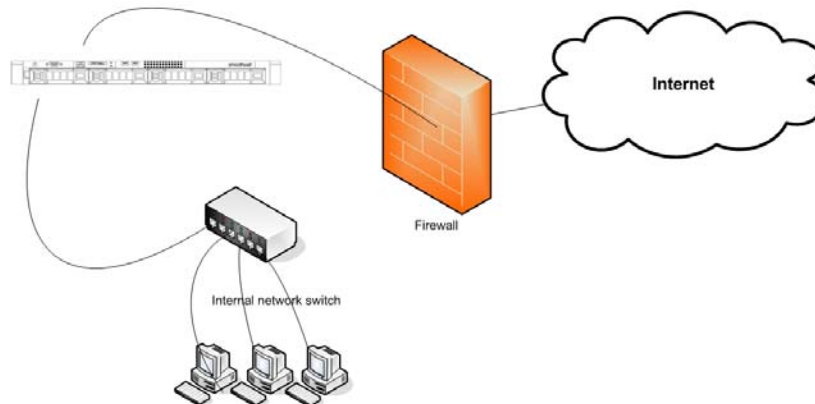be used as additional network interfaces. There is no need to reconfigure clients on the bridge. As far as they are concerned, the bridge does not exist.

Once installed, you can review the panel menu, and access and register the S12 Appliance.

Installing in Bridge and Administration Mode

In this scenario, port 1 is used only to administer the S12 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 S12 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.
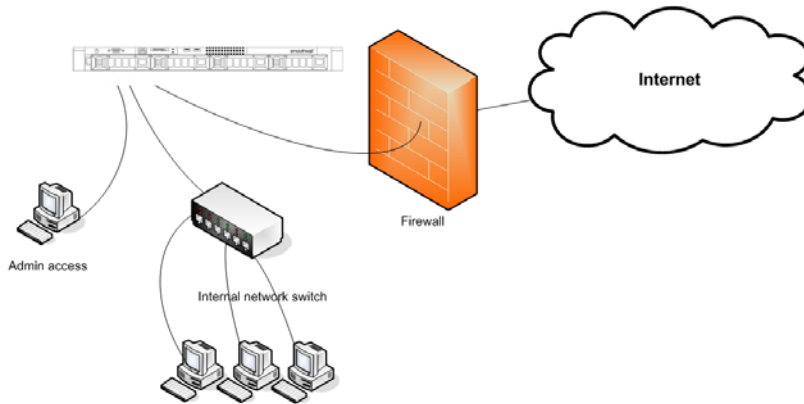
5.   Using the supplied AC power cord, connect the S12 Appliance to the power supply.

      The S12 Appliance boots.

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 S12 Appliance as a firewall. Typically, this is used in a Unified Threat Management installation.

To install the S12 Appliance as a firewall, do the following:

1.   Place the S12 Appliance in a stable and secure location.
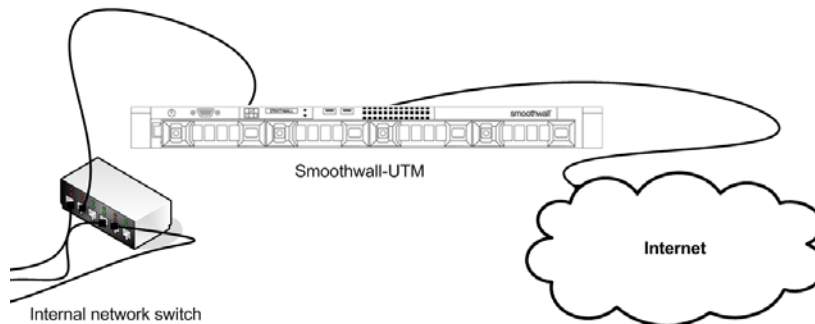
2.   Connect an ethernet cable from your network switch, or the supplied crossover cable from your computer, to port 1 of the S12 Appliance.

3.   Connect an ethernet cable from a port on the S12 Appliance to an external network, or internet, access point.

4.   Using the AC power cord, connect the S12 appliance to the power supply.

      The S12 appliance boots.

Note: If the S12 Appliance does not power on and boot automatically, switch the power switch to on (from the back panel).

3 Getting Started

This chapter describes the initial setup of the S12 Appliance, including:

Registering the S12 Appliance

You must register the S12 Appliance before you can use it.

Note: The S12 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 S12 Appliance, do the following:

1. From a computer on the same subnet as the S12 Appliance, start a web browser and connect to the S12 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 S12 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 S12 appliance.
Password	Enter `smoothwall` – the default password for the administrator's account.

3. Click **Login**, the S12 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 S12 Appliance is configured as Secure Web Gateway or as Unified Threat Management.
Name	The name of your organization's contact person for the S12 Appliance.
Organization	The name of your organization.
Department	The department in which the S12 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 S12 appliance.

4. Click **Save**.

   The S12 appliance prompts you to review the information you have supplied.

5. Click **Confirm**.

   The S12 appliance reboots and configures its initial settings. This can take up to five minutes to complete.

   Once the S12 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 S12 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 S12 Appliance for Your Network

To use the S12 Appliance on your network, you must do the following:

- Changing the IP Address on page 11 — For all installation modes
- Connecting to the Internet on page 12 — For firewall mode installations only

Changing the IP Address

The S12 appliance has pre-assigned internal IP addresses. You must change them to make the S12 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 S12 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 S12 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 S12 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 S12 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 S12 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 S12 appliance downloads the updates and lists them under **Pending updates**.

4. Click **Install**.

    The S12 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 S12 appliance, refer to the *Unified Threat Management Administration Guide*, or the *Secure Web Gateway Administration Guide*.

Deploying a Guardian Web Security Policy

The S12 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 S12 appliance's IP address and the port number of 800.

6. Click **Advanced**.

7. In the **Exceptions** panel, enter the S12 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 S12 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 S12 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 S12 appliance downloads and installs the latest blocklist.

Note: After this initial blocklist download, the S12 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