smoothwall®

The Web You Want

Smoothwall S14-Reporting Appliance

S14-Reporting Getting Started Guide

For future reference

S14-Reporting serial number:

Date installed:

Smoothwall contact:

Contents

About This Guide

The Smoothwall S14-Reporting Appliance, 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 S14-Reporting Appliance.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying an S14-Reporting 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	S14-Reporting 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 *S14-Reporting 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 S14-Reporting 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 S14-Reporting Appliance

About the S14-Reporting Appliance

The Smoothwall S14-Reporting Appliances are the hardware platforms required to run either Secure Web Gateway or Unified Threat Management.

The S14-Reporting 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 S14-Reporting package contains the items you will need to set up an S14-Reporting initially.

Verify that you have the following components:

Component	Information
S14-Reporting	The S14-Reporting appliance.
AC power cord	Provided with S14-Reporting.
Ethernet crossover cable	Provided with S14-Reporting.
S14-Reporting Getting Started Guide	This guide.
Information sheets	Applicable warranty and certification sheets.

Reviewing the Panel and Ports

The graphic below provides an overview of the S14-Reporting Appliance's ports, buttons and screen:
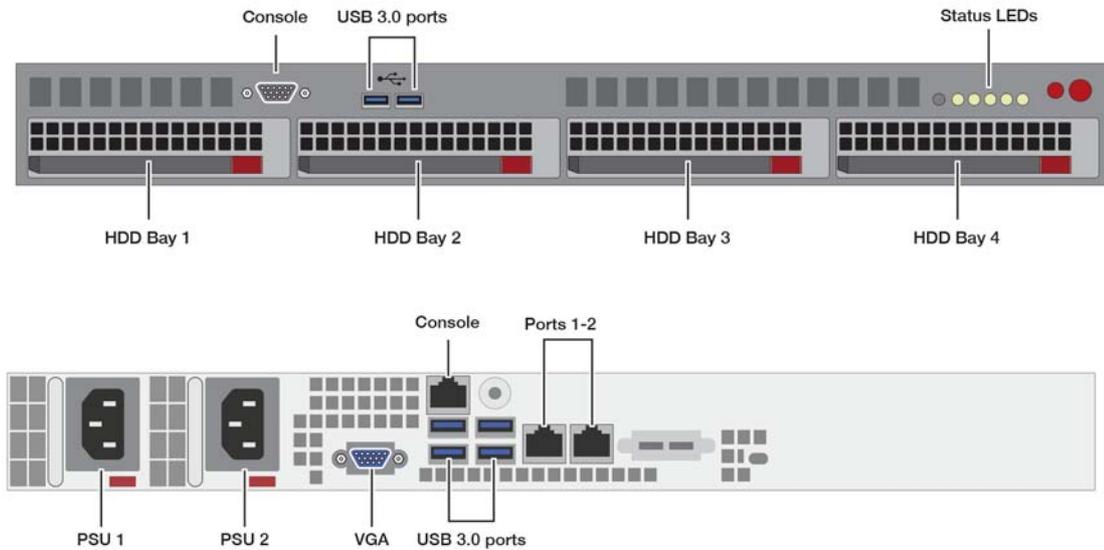
Object	Description
Ports 1 and 2	Port 1 is the default interface. Port 2 can be used to provide an external connection.
Console	Can be used to connect a console and administer the S14-Reporting Appliances.
USB ports	Also for keyboard access, if required.
Power	**Note:** Indicates when the power supply to the S14-Reporting Appliance is on.

2 Installing the S14-Reporting Appliance

This chapter describes the steps needed to install the S14-Reporting Appliance in a number of scenarios, including:

Installing as a Basic Web Proxy

This is the simplest scenario. The S14-Reporting 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:
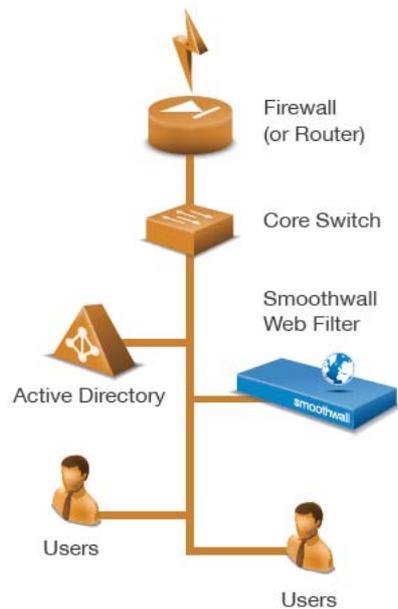
3. Using the supplied AC power cord, connect the appliance to the power supply.

    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 a port on the appliance to an external network, or internet-connected router or firewall.
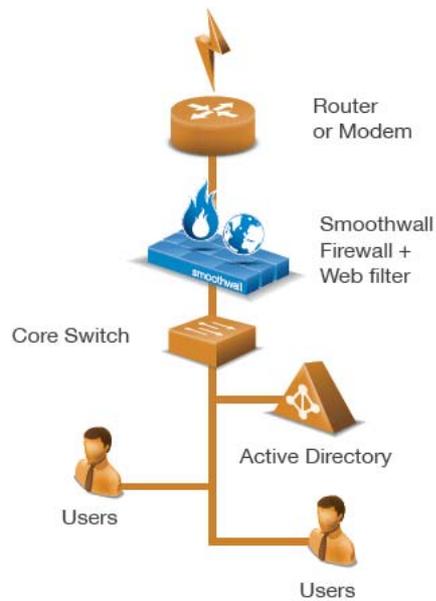
4. Using the AC power cord, connect the appliance to the power supply.

    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 S14-Reporting Appliance, including:

Registering the S14-Reporting Appliance

You must register the S14-Reporting 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 the 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.

Note: The S14-Reporting Appliance displays a warning message stating it is unable to register. This warning remains up to 5 minutes after the appliance has an IP address and correct DNS assigned, and has successfully connected to the Internet.

Configuring the S14-Reporting Appliances for Your Network

To use the S14-Reporting Appliance on your network, you must do the following:

Changing the IP Address

The S14-Reporting 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.

◆ **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 for external gateways, otherwise S14-Reporting 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 for external gateways, otherwise S14-Reporting 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 **System internal DNS server**.

13. Click **Save changes**.

14. From the **DNS forwarders** panel, click **Add new DNS forwarders** to configure the DNS servers for the DNS proxy service to use when resolving requests as follows:

   - **Status** — New DNS forwarders are enabled by default.

   - **Server IP address** — Either enter the server IP addresses, or click the down arrow and select the relevant DNS IP addresses, or ranges.

      For a detailed description about working with address objects, refer to your *Smoothwall System's Administration Guide*.

   - **Link Load Balancing pool or Local IP address** — Leave this option as **Default**.

      For a detailed description about link load balancing, refer to your *Smoothwall System's Administration Guide*.

- ◆ **Comment** — Configure an optional comment for this DNS server.

  An additional button, **Show comments**, appears on the **DNS forwarders** table if any comments are configured. Clicking this displays configured comments under the server IP address.

15. Click **Add**.

16. Browse to the **Web proxy > Web proxy > Settings**.

17. 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.

- **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 for external gateways, otherwise S14-Reporting 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 for external gateways, otherwise S14-Reporting 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 S14-Reporting 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 S14-Reporting appliance downloads the updates and lists them under **Pending updates**.

4. Click **Install**.

    The S14-Reporting 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