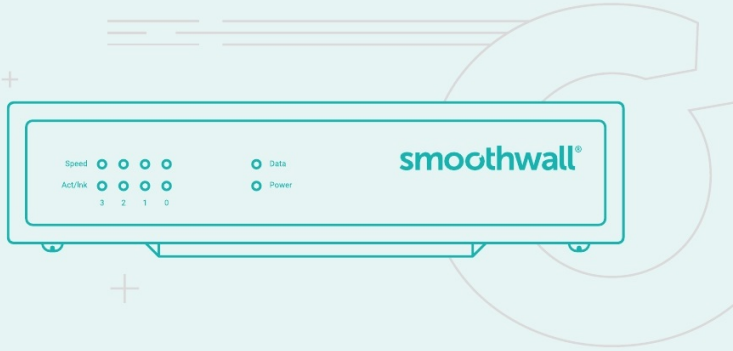
Smoothwall Hardware

# S2 Appliance




## Getting Started Guide

**For future reference:**

Serial number:

Date installed:

Smoothwall contact:

## Disclaimer



The information contained herein has been obtained from sources believed to be reliable. Smoothwall Ltd disclaims all warranties as to the accuracy, completeness or adequacy of such information. Smoothwall Ltd shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The content herein is subject to change without notice.

All brands or product names used in this document are acknowledged.

# Contents

# About this guide

This guide provides you with a walk through of the initial setup of your Smoothwall appliance.

## Audience and scope

This guide is aimed at system administrators maintaining and deploying the appliance.

It 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.

## Related information

For additional information relating to your appliance see:

- https://help.smoothwall.net/product_documentation contains the latest user assistance.
- https://kb.smoothwall.com contains helpful articles to help you troubleshoot problems.

# Introduction to the appliance

## About the appliance

The Smoothwall S2 appliance has been designed specifically for smaller installations such as Primary Schools or small business firewalls. Although small it is still mighty, with an Intel® Processor with 8GB memory, four 1GB Ethernet ports, and 500GB solid state hard disk.

The Smoothwall appliances come preinstalled with Smoothwall and provides you with the hardware platform required to run either:

**Secure Web Gateway** delivering the features you need to provide a security online experience for all types of users. Smoothwall's web content filtering analyzes actual page content to make an intelligent filtering decision.

**OR**

**Unified Threat Management** delivering all the features of the Secure Web Gateway paired with a next generation firewall to give you total protection.

For the latest Smoothwall product documentation, refer to http://help.smoothwall.net/product_documentation.

## Reviewing package contents

Your package contains the items needed to initially set up an Appliance.

For a detailed hardware specification, refer to your Smoothwall representative.

| Component | Information |
|---|---|
| **S2** | The S2 appliance. |
| **AC power cord (US and UK)** | Provided with the appliance. |
| **Ethernet crossover cable** | Provided with the appliance. |
| **Getting started Guide** | This guide. |
| **Information sheets** | Applicable warranty and certification sheets. |

# Reviewing the panel and ports

## Front


| Label | Indicator Light-Emitting Diode (LED) Lamps |
|---|---|
| **Speed** | Indicates the speed of the connection when lit. |
| **Act/Link** | Indicates the activity of the LAN port respectively when lit. |
| **4 3 2 1** | Indicates which port is in use when lit. |
| **Data** | Indicates that data is being sent and received when lit. |
| **Power** | Indicates that there is power being supplied to the appliance when lit. |

## Back


| Label | Description |
|---|---|
| **LAN 4 3 2 1** | The Ethernet ports available to connect the appliance to other devices. Port 1 is the default interface port. The other ports can be used to provide internal networking zones and external connections. Bypass ports are not available on the S2 appliance. |
| **USB** | You can used these to connect to external storage devices or a keyboard. |
| **Console** | You can use this to connect an Ethernet RJ45 console cable with either a DB9 or other connector so that you can connect to your computer and configure your appliance. |
| **F/D** | This reboots the appliance. This does not factory reset the appliance. |
| **Power** | Switches the appliance on or off. When you plug in the power cable, the appliance switches on automatically. To initiate a clean shutdown when the Appliance is running, press the power button. To force a power off, press and hold the power button for five seconds. |
| **DC 12V** | The power cable port. The appliance switches on automatically when you plug the power cable in. |

# Installing the appliance

This section describes the steps needed to install the appliance in a number of scenarios, including:

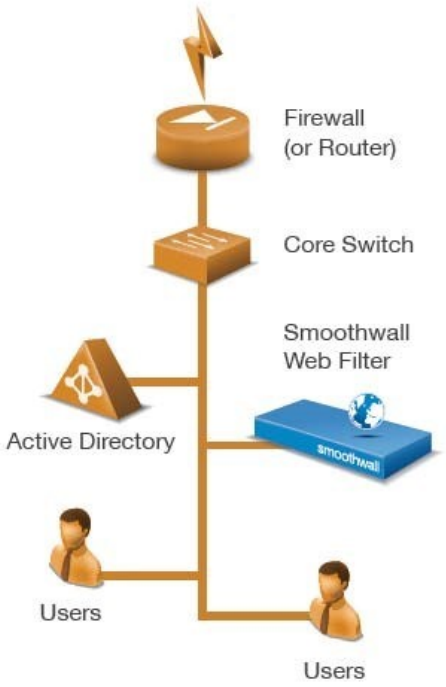
- **Installing as a basic web proxy**
- **Installing in firewall mode**

## Installing as a basic web proxy

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

**To do a basic installation:**

1. Place the appliance in a stable and secure location.
2. Connect an Ethernet cable from port 1 on the appliance 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.

**Note:** On initial start-up your appliance will perform a series of system configuration tasks. Please be patient while your appliance completes this initial start-up procedure.

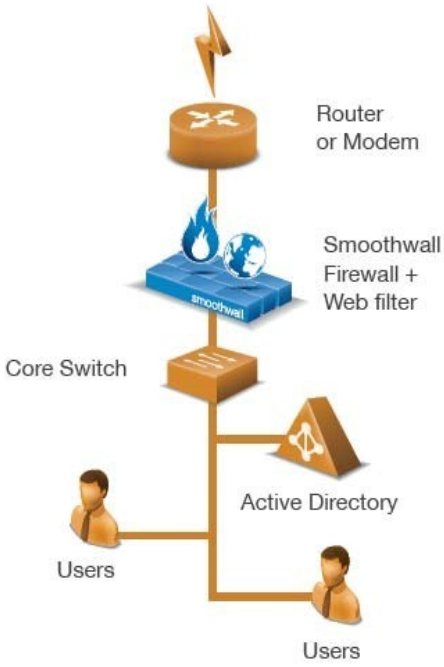
If the appliance does not power on and boot automatically, hold down the ✔ key on the keypad for one second.

# 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:**

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.

> Note: On initial start-up your appliance will perform a series of system configuration tasks. Please be patient while your appliance completes this initial start-up procedure.

If the appliance does not power on and boot automatically, hold down the ✔ key on the keypad for one second.

# Getting started

This section describes the initial setup of the appliance, including:

- Registering the appliance
- Configuring the appliance for your network
- Updating the Smoothwall
- Getting the latest guardian blocklists

## Registering the appliance

You must register the 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.

To register the appliance:

1. From a device on the same subnet as the Smoothwall System, start a web browser and connect to Smoothwall System via HTTPS, using the URL: **https://192.168.110.1:441/**
   or via HTTP, using the following URL: **http://192.168.110.1:81/**
   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 provided by your Smoothwall representative. The serial number determines whether the appliance is configured as Secure Web Gateway or as Unified Threat Management.
   - **Name** - Your organization's contact person in matters relating to the appliance.
   - **Organization** - The name of your organization.
   - **Department** - The department within your organization that has ownership of the appliance.
   - **Locality or town** - The town, or location, in which your organization is located.
   - **State** - The state in which your organization is located.
   - **Country** - The country in which your organization is located.
   - **Email** - Email address of your organizations appliance contact.
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.
   - **Admin password** - Enter your new system administrator password, re-entering the new admin password in the Again field to confirm consistent password entry.

- **Root password** - Enter your new system root password, re-entering the new root password in the Again field to confirm consistent password entry.
- **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).<br>**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. |

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. The browser will refresh back to the login prompt.
11. Enter your new login credentials and click **Login**.

**Note:** The S2 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 appliance for your network

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

- Change the IP address
- Create an external connection

## Change the IP address

The 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 preassigned 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 **Network** > **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. Complete 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.<br>Else, leave None selected. |
| | **Bandwidth** | This parameter is only displayed if a User defined Gateway is configured.<br>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.<br>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.<br>Connection monitoring is enabled by default.<br>It is not recommended you disable connection monitoring for external gateways, otherwise the S2 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.<br>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.<br>It is not recommended you disable connection monitoring for external gateways, otherwise S2 assumes the gateway always has an internet connection. |

| Use as | Additional Parameter | Description |
|---|---|---|
| | **DHCP client hostname** | Optionally, enter the DHCP client hostname as specified by the DHCP server. |

- **Comment** — If require, enter any information relating to this IP address.
  If comments have been added, the Show comments button is displayed on the Attached addresses table. Clicking this displays comments added for 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, via HTTPS using port 441 or HTTP using port 81.
7. Browse to **Network** > **Configuration** > **Interfaces**.
8. Click the **IP addresses** link for the relevant interface to display the **Attached addresses** table.
9. Locate and select the pre-assigned IP address.
10. Click **Delete**.
11. Browse to **Network** > **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 select the relevant DNS IP addresses, or range from the drop-down list.
      For a detailed description about working with address objects, refer to the Smoothwall product help https://help.smoothwall.com
    - **Link Load Balancing pool or Local IP address** - Leave this option as Default.
      For a detailed description about link load balancing, refer to the Smoothwall product help https://help.smoothwall.com
    - **Comment** - Enter an optional comment for this DNS server.
    - **Show comments** - Displayed on the DNS forwarders table if any comments have been added. Clicking this displays the comments added for 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.

## Create 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 the Smoothwall product help https://help.smoothwall.net.

1. Browse to **Network** > **Configuration** > **Interfaces**.
2. Select the relevant interface, and click **Edit**.
3. Complete the following:
   - **Name** — Enter 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, for this connection.
   - **Comment** — Enter an optional comment for this external interface.
     If any comments are added, a Show comments button is displayed allowing interface comments to be reviewed.
4. Click **Save changes**.
   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. Complete 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.<br>Else, leave None selected. |
| | **Bandwidth** | This parameter is only displayed if a User defined Gateway is configured.<br>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.<br>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.<br>Connection monitoring is enabled by default.<br>It is not recommended you disable connection monitoring for external gateways, otherwise the S2 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.<br>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.<br>It is not recommended you disable connection monitoring for external gateways, otherwise S2 assumes the gateway always has an internet connection. |
| | **DHCP client hostname** | Optionally, enter the DHCP client hostname as specified by the DHCP server. |

- **Comment** — Enter an optional comment for this IP address.
  If comments have been added, the Show comments button is displayed on the Attached addresses table. Clicking this displays comments added for the IP address.

8. Click **Add**. The appliance applies the new IP address to the interface.

# Updating the Smoothwall

You must ensure the S2 Appliance has the latest Smoothwall software release and update:

- Releases provide new features and product improvements.
- Updates provide bug fixes and enhancements to address potential security threats.

The Smoothwall must be connected to the Internet in order to discover, download and install system updates. Smoothwall's support systems are directly integrated with the Smoothwall's update procedure.

**To check for and install releases and updates:**

1. Browse to System > Maintenance > Updates and releases.
2. In the Update: fix and patch your installed release section, click Check for updates.
    - If an update exists it will be listed under Available updates.
    - If a new release exists it will be listed under the Available releases, in the Releases: new functionality and major upgrades section.
3. If you want to:
    - Review Update/Release details:
        a. Click **Details**. Review details of the current update including any previous release updates.
        b. Click **OK** to close the Update information dialog.
    - Install the Smoothwall Update/ Release:
        a. Click **Install**. Details of the update, including details of any previous release updates are displayed.
        b. Click **Install and reboot**.
    - Schedule the Smoothwall Update/ Release install at a later time:
        a. Click **Schedule**.
        b. Select the preferred update implementation time.
        c. Click **Apply**.

**Note:** The scheduled update process will automatically reboot the system following the scheduled install.

For a detailed description of further configuration needed for your Smoothwall system, refer to the Smoothwall product help https://help.smoothwall.net.

# 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 initiate Guardian blocklists download:**

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 will check for updated blocklists hourly. When a new blocklist becomes available, the Smoothwall automatically downloads and installs the updated blocklist.