

SOPHOS

 **web security and control**

Reviewer's guide
WS1000 Appliance



WELCOME

Welcome to the Sophos Web Appliance reviewer's guide. This document provides a review of the core functionalities of the appliance, highlighting its effectiveness and ease of use. After reading the guide, you will have a deeper understanding of how the Sophos WS1000 Appliance delivers the security you need and the performance you expect for safe, productive web browsing.

This appliance is part of Sophos's award-winning security and control solution and is purpose-built for business, education, and government. Sophos appliances are backed up by 20 years' experience and combined in-house anti-virus and anti-spam expertise delivered by SophosLabs™ – our global network of threat analysis centers. Early detection and protection from ever-more complex and fast-spreading security threats is one of the reasons that Sophos is acclaimed for delivering the highest level of customer satisfaction and protection in the industry.

As with all our products, the WS1000 includes comprehensive 24-hour support from our worldwide network of support engineers, available at no additional cost, every day of the year.

For information on pricing and availability of this appliance in your area, please contact your local Sophos representative. To find out who serves your area, please visit:

www.sophos.com/products/howtobuy

If you would like to request an evaluation, please fill out our online request form at:

www.sophos.com/products/wsa/eval

“ *The Sophos WS1000 is exactly what companies have been looking for – it thwarts virtually all malware without hindering or slowing clients' web access.* ”

Barry Nance,
Network Testing Labs

CONTENTS

1	INTRODUCTION	6
	Management highlights	7
	Core features and benefits	7
	Software and hardware components	8
2	PRODUCT FUNCTIONALITY	9
	Security filtering	9
	Application filtering	11
	URL filtering	12
	Other filtering options	13
	Single-engine scanning	14
	Blocking “call home” traffic	15
3	SETUP	16
	Installation	16
	Configuration	18
	The end-user experience	19
4	MANAGING THE APPLIANCE	21
	Management console and dashboard	21
	Monitoring, alerting, and notification	22
	Updates	23
	Configuration backup and restore	23
	Managing user feedback	25
	Additional search capabilities	26
	Active Directory integration	27
5	REPORTING	28
	Dashboard reports	28
	Reports page	29
	Reporting using log data	30
6	SUPPORT	31
	The Managed Appliance	31
	Warranty	33
	Standard Sophos support	33
	APPENDICES	
	I Default policy settings	34
	II Managed Appliance service levels	35

1: INTRODUCTION

Overview

The WS1000 Web Appliance is a secure web gateway solution providing fully integrated protection against spyware, viruses, Trojans, worms, phishing, and unwanted or offensive web content. The WS1000 is built on a robust hardware platform, delivering high-capacity, high-availability security with unrivaled simplicity and control. Staying ahead of the rapid evolution of threats, the WS1000 keeps networks free of web-based threats and helps maintain network performance and employee productivity.

The core components of the WS1000 include:

Advanced threat discovery and protection: The WS1000 is powered by SophosLabs, a global network of threat detection and analysis centers. The network proactively scans billions of web pages a day, discovering more than 17,000 new sources of malware and over 15,000 new phishing sites each week. New threat definitions and malicious URLs are automatically downloaded to the appliance every five minutes, ensuring the most up-to-date protection available.

Genotype® technology blocks families of viruses, providing protection against previously unseen threats even before specific signature-based detection is available. Behavioral Genotype Protection provides pre-execution host intrusion prevention (HIPS) without the need to install and manage a separate system. Genotype and Behavioral Genotype definitions are also downloaded automatically every five minutes.

Single-engine, risk-sensitive scanning for greater performance and no latency: Sophos's award-winning scanning technology delivers complete protection against all web-based threats with a single engine, resulting in faster scans, no latency, and only one engine to update. Having just one point of policy enforcement also means you spend less time managing web gateway security.

Application filtering: The WS1000 enables greater control over costly bandwidth by blocking downloads of potentially unwanted applications, including dialers, remote administration tools, and system monitors. It also allows control over file types such as executables, streaming media, and ActiveX controls.

URL filtering: You can also easily implement category-based acceptable web-use policies that further reduce the risk of compromising your organization's customer privacy, intellectual property, and compliance with regulations.

Monitoring and alerting: As a Managed Appliance, the WS1000 features built-in monitoring and alerting for easier management, quicker issue resolution, and enhanced peace of mind. More than 40 different settings and conditions are constantly monitored for peak performance. Alerts are sent both to the system administrator and to Sophos, so that corrective action can be executed and web security maintained. If further assistance is required, administrators can also take advantage of on-demand remote assistance and let Sophos support troubleshoot the appliance directly.

Efficient web gateway protection

The Sophos Web Appliance provides maximum protection for your web gateway with minimum administrative effort.

“Three clicks to anywhere” management console: Complementing these powerful technologies is a web-based management console that simplifies administrative tasks and provides better insight and control over web security. The management console is designed to provide instant access to relevant, actionable information so that administrators can make informed decisions about traffic levels, system performance, and browsing behavior.

Management highlights

The Sophos Web Appliance offers a range of features that simplifies the management of secure web browsing:

- A fully web-based console for quick and easy system management
- Definable policies for controlling access by category and risk level
- Powerful, relevant reporting on traffic, suspect computers, and malware trends
- Microsoft Active Directory® integration for easy setup, policy enforcement, and authentication
- Built-in hardware and software maintenance and alerting
- Proactive “heartbeat” monitoring by Sophos to ensure uptime and security integrity
- On-demand remote assistance available 24x7x365 for quicker issue resolution.

Three clicks to anywhere

Built on a strict discipline of minimal navigation, every feature of the management console is no more than three clicks away, and command-line access is *never* required.

Core features and benefits

Feature	Benefit
Platform-independent	Easily fits into any existing network infrastructure
Unrivaled visibility into web-based threats	The SophosLabs security network scans billions of web pages a day, looking for malware in more places than any other security vendor
Complete malware detection	Blocks spyware, phishing, viruses, Trojans, worms, adware, and other malware, including “call-home” traffic from infected machines
Genotype and Behavioral Genotype proactive protection	Blocks evolving malware variants and unknown threats before they can execute or install
High capacity	Easily handles web traffic of up to 200 concurrent users on a single appliance
High performance	Single-engine scanning detects and blocks threats faster and more efficiently than multiple-engine solutions
Regulatory compliance and productivity filtering	Blocks access to offensive and illegal web content, and allows control over access to a wide range of other categories
Global protection	Protects global organizations from web-based threats in multiple language message streams
Sophos Managed Appliance	Reduces administrative burden, automates security and software updates, and provides remote system health monitoring for reliable, round-the-clock protection
Comprehensive support	Includes 24x7x365 support for the duration of the software license, and Sophos can be contacted for one-to-one assistance at any time

Software components

The WS1000's built-in software includes the following major components:

- Sophos full-spectrum scanning engine, protecting against spyware, viruses, and unwanted applications
- Sophos URL filter
- Management console and dashboard
- System alerting and notification
- Active Directory integration.

The WS1000 is built on a hardened Linux operating system (OS), optimized for the hardware platform and for the embedded Sophos software. Linux is an extremely stable and reliable OS, and offers excellent speed and performance for network security appliances. The Linux kernel has been optimized for maximum security and hacking prevention, with the absolute minimum number of ports kept open.

Hardware components

The WS1000 is engineered for small to mid-sized networks, built on a robust hardware platform that can handle up to 200 concurrent users. The appliance features the following hardware components on a dedicated 1U server:

- Intel Pentium D Dual core 3.4 GHz processor
- Two 160 GB, 7200 rpm SATA hard drives
- 4 GB memory
- 260 W, 110-240 V power supply.

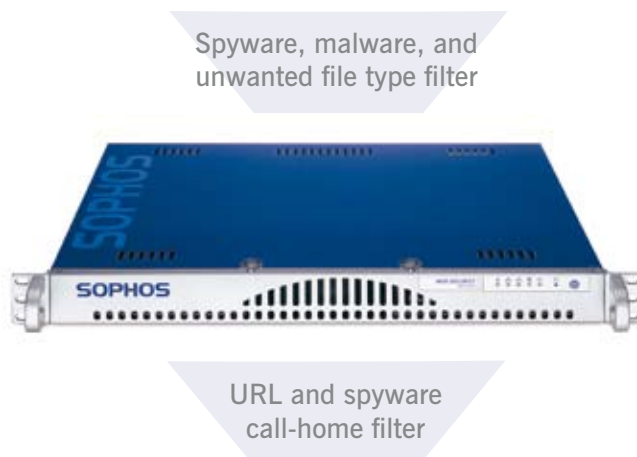
2: PRODUCT FUNCTIONALITY

Overview

The WS1000 Appliance is a plug-and-protect web gateway solution offering complete security and control. It fits easily into any network configuration, and since it has a self-contained operating system, you do not need to have any knowledge of UNIX, Linux, Solaris, or other server platform language.

The WS1000 uniquely combines complete malware protection at page level (rather than just domain level), plus control over adware, streaming media, and unwanted applications. It also includes customizable access policies based on web site categories. By monitoring both outbound page requests and inbound data, the WS1000 allows administrators to ensure network safety and to enforce acceptable web-browsing policies easily and efficiently with a single appliance.

This section provides an introduction into how the WS1000 enforces web security policy.



Security filtering

With the evolution of high-bandwidth communications and web-based applications, web browsing is recognized not only as an essential communication medium for organizations of all sizes and types, but also as a major point of weakness in network security. Most organizations today could no longer carry out regular operations without giving users access to web browsing. Unfortunately, this freedom is well known to malware writers, as is the fact that most organizations have not yet put adequate web security measures in place. The explosive growth of spyware and phishing attacks over the last few years is evidence of the vulnerability of uncontrolled web browsing.

The WS1000 is first and foremost a security appliance. It draws on more than 20 years of expertise gathered by Sophos as a security vendor, and its

primary purpose is to prevent infection from web-based malware, including spyware, Trojans, viruses, worms, and phishing attacks. Protection is achieved by scanning all inbound HTTP traffic as it enters the organization before it reaches the end user's browser. If malware is encountered, it is removed, with the remaining clean content passing smoothly to the browser.

Malicious content can appear on virtually any web site, but to scan content from all sites all the time is impractical and would introduce excessive latency, negatively impacting the end-user experience. To overcome this challenge, which would normally force a trade-off between security and performance, the Sophos Web Appliance uses innovative risk-sensitive scanning technology to adapt the depth of the scan to the relative risk of the web page.

Determining the risk of a web page

Risk-sensitive scanning is dependent on Sophos's unique ability to determine the risk level of billions of web pages a day. The SophosLabs security network scours the web for sources of malicious code, on average adding more than 17,000 new URLs each week. As domains and web pages are visited, risk levels and actions are assigned as follows:

Risk level	Site characteristics	Action
High	Currently hosting malicious content	Block
Medium	History of poor privacy and/or security practices that may compromise network security	Block or scan
Low	No recent history of malicious content or behavior, as reviewed periodically by SophosLabs	Scan

The ability to differentiate between medium- and low-risk sites is key to delivering a seamless end-user experience that doesn't compromise on security. Using risk-sensitive scanning, the WS1000 will perform a more comprehensive scan on medium-risk sites than it will on low-risk sites. For example, images and HTML on medium-risk sites are scanned, but those on low-risk sites are not, since these elements rarely contain malware.

The WS1000 uses two other categories relating to risk: Trusted sites and Unclassified sites. The Trusted site list is an administrator-controlled list of web sites that are known to be safe, and are therefore not scanned at all. This list, which may include intranets, vendor portals, and government sites, can be managed locally.

Unclassified sites are sites that have not yet been analyzed by SophosLabs. The administrator has the option to assign these sites to one of the three major risk classes – High, Medium, or Low – and assign actions accordingly.

Risk-sensitive scanning

The depth of the scan of inbound content varies, based on the assessed risk of the web page – the riskier the page, the more thorough the scan.

Application filtering

The WS1000 provides better management of bandwidth usage related to web browsing. The appliance can block the download of a range of file types that could consume bandwidth and slow down web traffic. Using a simple point-and-click policy manager in the management console, administrators can control the following file types:

File type	Details	
Executable	DOS command (com) Java applet (Class) Javascript (js) ActiveX control (ocx)	Visual Basic extension (vbx) Windows executable (exe) Windows library file (dll) Other executables
Document	Adobe PDF (pdf) Microsoft Excel (xls) Microsoft Powerpoint (ppt) Microsoft Word (doc)	Microsoft Project (mpp) Rich Text Format (rtf) WordPerfect (wpd)
Streaming audio	Midi (midi) MPEG audio (mp3) RealAudio (ra)	Wave (wav) Windows Media Audio (wma)
Streaming video	Audio Video Interleave (avi) MPEG video (mpg, mpeg) QuickTime video (mov)	RealMedia (rm) Windows Media video (wmv)
Archive	Java archive (jar) RAR archive (rar) Stuffit (sit)	Tarball (tar) Zip archive (zip) Other archive (bz2, gz, Z)

In addition to these common file types, the WS1000 can also block a range of applications labeled by Sophos as potentially unwanted applications (PUAs). These applications, which include adware, hacking tools, dialers, remote monitoring tools, and system monitors, may not be malicious by design but could consume valuable network bandwidth and client processor resources, and so might not be wanted. PUAs can be blocked by checking the tick box on the Policy:Downloads page in the management console (see Figure 1).

Unwanted applications

Sophos defines potentially unwanted applications (PUAs) as those that are not appropriate in a business environment, and which might negatively impact network or desktop resources.

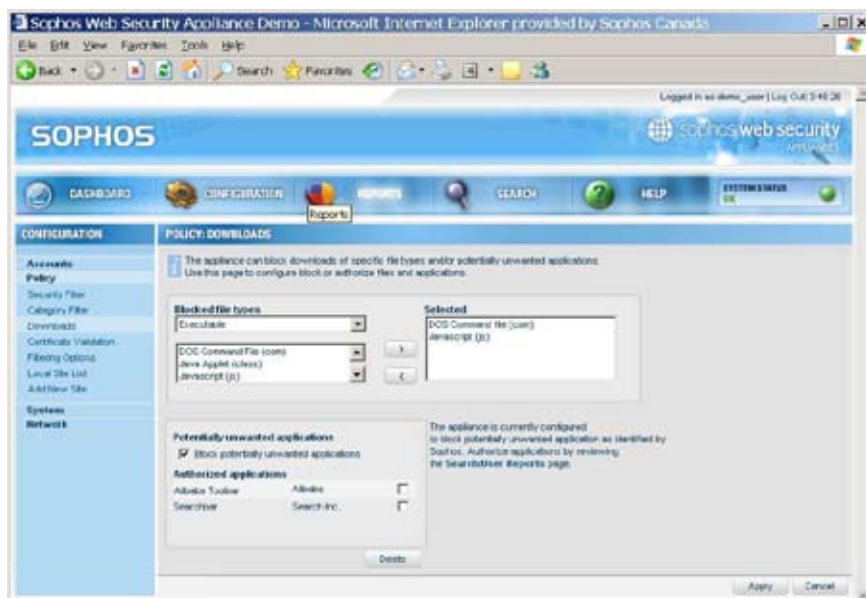


Figure 1: Setting download policy to block specific file types

As with web pages, administrators can allow exceptions to the list of blocked file types or applications by manually approving them based on user requests (**Feedback users** must be enabled for unblock requests to be made – see Section 3). User requests are accessible from the **Search** page in the management console, as shown below.

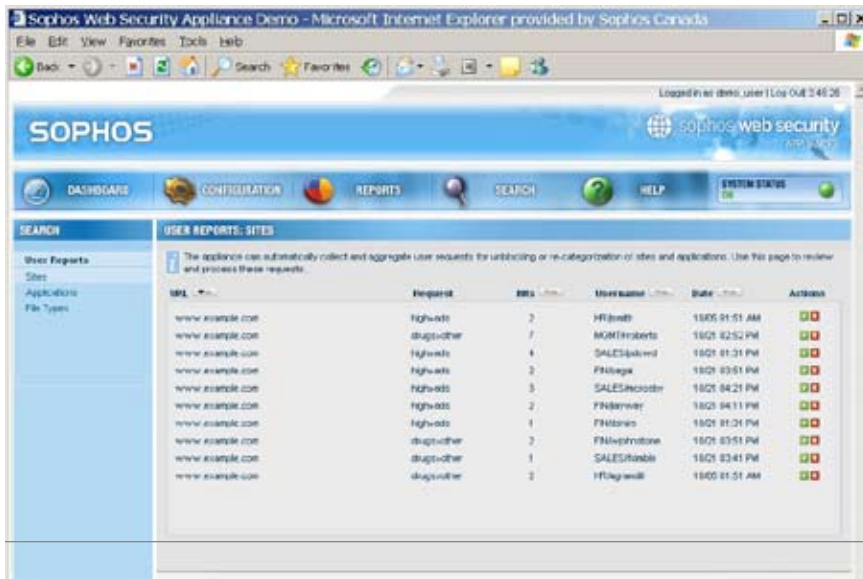


Figure 2: Feedback users' requests for site reclassification

URL filtering

For a variety of reasons, many organizations do not wish to allow their employees access to unlimited web browsing. Some content is deemed inappropriate for the workplace, for the following reasons:

- Concerns about productivity and the personal use of time and organizational resources
- Concerns about legal liability resulting from the appearance and/or distribution of offensive and/or illegal content.

The most efficient way to prevent staff from viewing unwanted or dangerous content, while granting them access to other content, is to block access to web sites based on their categories (e.g. shopping, entertainment, games, banking, pornography, etc).

Controlling productivity

Workers spent around 20 percent of their internet time on personal business or for entertainment.

*Burstein
2005 internet usage study*

The WS1000 is equipped with a database of more than 2 million web sites and domains in the following categories:

Category	Sub-category	
Communications	Cell phones	Ringtones, graphics, and other add-ons
	Chat	Online chat services
	IM	Web-based instant messaging sites
	Webmail	Web-based email
Entertainment	Banking	Banking and other financial services
	Dating	Dating or introduction services
	Games	Online gaming
	Shopping	Shopping or auction sites
	Sports	Sports information and news
	Other	General information and entertainment
Media	Ads	Online advertising
	News	Coverage of news and current events
	TV	Streaming audio and video sites
Search	Search engines	Internet search engines
	Job search	Job search services and online career postings
Questionable	Adult material	Nudity and other sexual content
	Alcohol	Information about alcohol
	Drugs	Information about drugs and supplements
	Gambling	Online gambling and gaming services
	Weapons	Information on weapons, hate, etc

The administrator can set access policy (Block, Allow) for each sub-category. (Note: the WS1000's security filter will still scan allowed content for malware – see page 11.)

If a page request is denied based on established policy, the appliance provides the option to notify the individual requesting the page of the reason why the request was denied. Refer to End-user notifications on page 19 for details.

If an organization is already using a separate URL filtering product, the WS1000 can work in tandem with the product and ensure that security against web-based threats is enforced alongside the productivity-driven focus of the URL filter.

Other filtering options

The WS1000 offers additional policy capabilities, including:

Operational mode	Passthrough or Full. The latter mode allows exemptions to filtering policy by IP address and/or user group
Cache settings	Minimum and maximum cacheable object size
SophosLabs	Data sharing with SophosLabs (non-identifiable by user or IP)
Logging mode	Including username and IP when viewing reports, search results, and logs
Additional options	Allow/deny public IP address; allow unscannable and encrypted files; allow large files without scanning

Up-to-date security

SophosLabs scans billions of web pages a day to update the WS1000's built-in database of over 2 million suspect websites.

Single-engine scanning

At the heart of the WS1000 is Sophos's advanced single-engine scanning technology – the same engine that protects more than 100 million Sophos users around the world. Our technology delivers faster, more efficient security by checking for all web-based threats simultaneously in a single pass. This approach eliminates the need for separate engines for spyware, viruses, and URL filtering, and also reduces page latency for the end-user. The result is a substantial reduction in the administrative burden associated with managing and creating policy for multiple engines.

The Sophos Web Appliance provides the ideal mix of automation and control to support enterprise web-browsing security needs. It combines automated threat definition updating with quick and easy administrative capabilities and exception-driven alerting. This combination of functions minimizes the day-to-day administrative load while providing the insight and control that administrators need.

The WS1000 also benefits from the extensive exposure of SophosLabs to the threat landscape – enabling proactive protection through faster analysis of new threats, multiple detection/update techniques, and complete management of the entire threat lifecycle.

Using Sophos Web Appliances, organizations benefit from:

- Reliable protection against new threats, **and** unknown threats
- Reduced administrative workload
- Greater peace of mind knowing that the web-browsing infrastructure is protected.

Protection throughout the threat lifecycle

SophosLabs protects throughout the threat lifecycle, from malware discovery to distribution and further evolution.

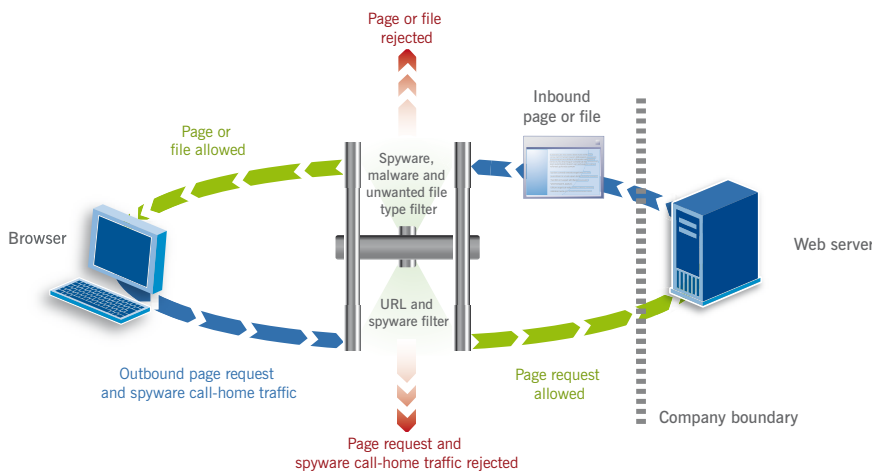


Figure 3: The WS1000's scanning technology in action

Award-winning protection

The excellence of Sophos security is regularly recognized by a wide variety of independent test bodies, including ICISA, West Coast Labs, Veritest, and av-test.org

Blocking “call home” traffic

Taking advantage of Sophos's ability to detect and analyze malware from a wide range of sources, the WS1000 is also able to prevent client computers infected with spyware from transmitting data back to waiting servers (“calling home”). When SophosLabs discovers a URL that serves as the repository for information stolen from infected computers, it adds the URL to the list of high risk web sites, and prevents computers from reaching it. In the event of infection prior to installing the WS1000, or infection via other means, the administrator would be able to identify compromised computers simply by viewing the **Suspect Machines** report in the management console (see below).

Spyware protection

Even when they are infected with spyware, computers are blocked from contacting URLs known to store stolen information.



Figure 4: Suspect Machines report

3: SETUP

Overview

This section covers basic setup of the appliance, including configuration, Active Directory setup, end-user preferences, and default policy settings. It is not a substitute for the WS1000 setup guide, but is intended to demonstrate the appliance's simplicity and ease of administration.

Installation

As a gateway appliance, the WS1000 is typically installed in the DMZ, inside the network firewall and upstream from client computers.

There are three typical installation scenarios – Explicit proxy, Transparent proxy, and Bridge mode.

Explicit proxy mode

Explicit proxy mode offers the greatest security and functionality. Deploying in this mode enables HTTPS certificate validation, as well as the use of Active Directory for opting out and reporting. Explicit mode requires configuration of the firewall, routers, and client browsers.

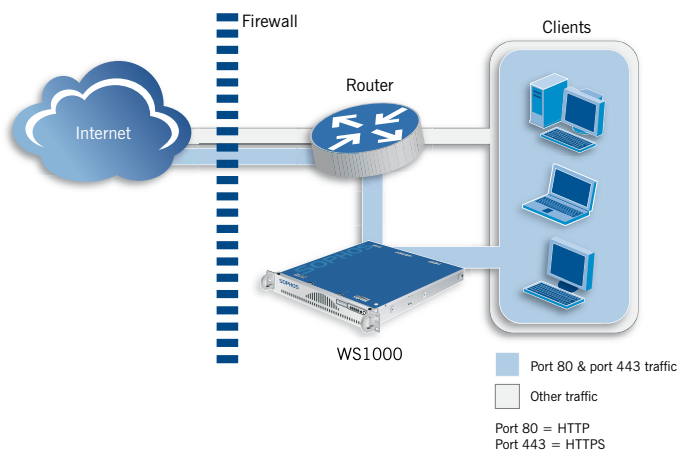


Figure 5: WS1000 installed in explicit proxy mode

Transparent proxy mode

In transparent mode, the WS1000 sits off-stream from the routers and firewall, with the latter configured to route traffic on port 80 to and from the appliance. Client browsers require no configuration, but client firewall and routers must be configured.

The main advantage of transparent deployment is the elimination of a potential single point of network failure. In addition, if total network traffic is too heavy (in terms of Mbps) for the WS1000, a transparent deployment will eliminate a potential bottleneck by dealing only with port 80 traffic. All other network traffic will be routed separately.

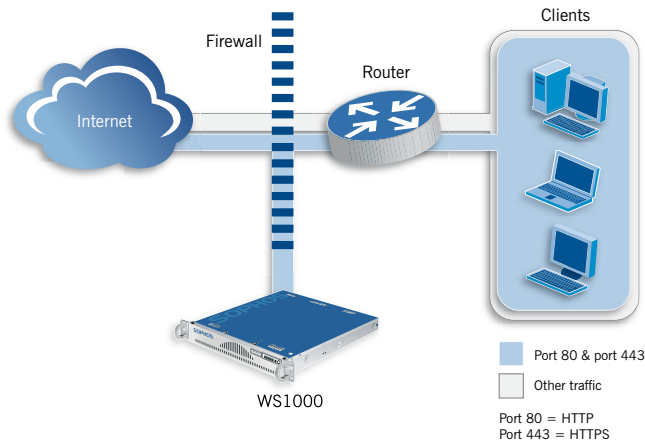


Figure 6: WS1000 installed in transparent proxy mode

Bridge mode

Bridge mode is the simplest installation scenario, requiring no changes to client or router settings. In bridge mode, traffic on all ports is routed through the WS1000, which internally pulls out traffic on port 80 only for scanning. If the appliance fails or is intentionally shut down, all traffic will continue to flow through, without any scanning taking place.

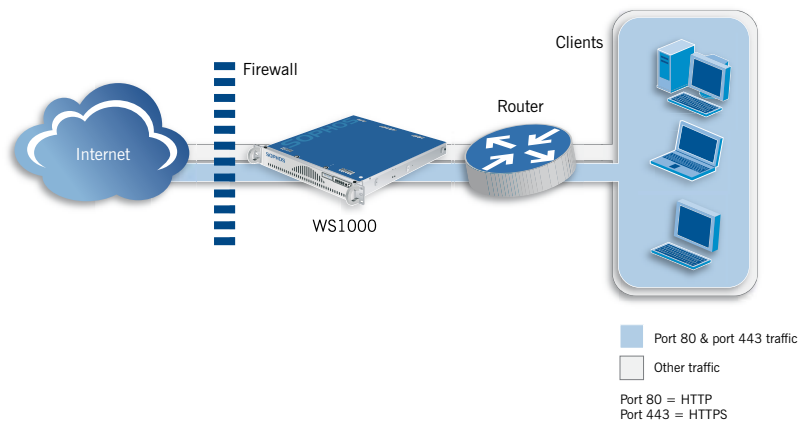


Figure 7: WS1000 installed in bridge mode

Although deployment is simple, bridge mode does limit the degree of network integration and security: the WS1000 cannot be integrated with Active Directory, nor can it validate certificates for HTTPS traffic (port 443). Opting out of scanning can only be done by specifying the IP addresses of the machines designated for opt-out. However, since only the appliance itself and the firewall need configuration, bridge mode is the easiest deployment option available.

Configuration

Configuring Sophos Web Appliances is easy and straightforward. Once installed and booted, a straightforward Setup Wizard leads you through 14 intuitive screens to complete the configuration process, reducing installation time to less than 30 minutes. The Wizard includes auto-detection of Active Directory settings, as well as a range of default policy settings, so that you can secure your web traffic quickly and easily.

Fast, easy setup

A simple setup wizard helps you get the appliance up and running in less than 30 minutes.



Figure 8: Changing configuration settings

Configuration settings can be changed at any time using the appliance's “three clicks to anywhere” management console.

The table below shows the specific configurable components of the WS1000:

Configuration area	Components	
Accounts	Administrators Exempt users	User notification options Feedback users
Policy	Security filter Category filter Downloads Certificate validation	Filtering options Local site list Add new site
System	Updates Backup Restore	Alert recipients Active Directory Time zone
Network	Network interface Hostname	Network connectivity

See Appendix I for a list of default settings.

The end-user experience

When it comes to browsing the web, users expect instant (or almost instant) access to desired content. Despite the fact that there can be several reasons why a page does not load – bandwidth shortage, routing delays, server overload, etc – users lack patience when they cannot get the information they are seeking. Web security often receives most of the blame, based on an assumption that scanning for threats is what slows the delivery of web content.

While file scanning can account for much of the latency with traditional web security solutions, this is not the case with the WS1000. Ensuring a smooth and latency-free end-user experience is a core design principle of Sophos Web Appliances. As discussed in Section 2, the appliance's scanning technology is built to minimize scan time and reduce page latency. When it comes to what the user sees, the experience is equally positive.

The WS1000 uses a series of end-user notifications and feedback routines to communicate effectively with browsers when a policy violation or content delay occurs. The following section provides detail on these tools.

End-user notifications

Whenever a policy violation occurs – such as an attempt to visit a site hosting malicious content, or a request to download an unwanted file type – the WS1000 will notify the user.

Notification pages are displayed for the following conditions:

- Malware detected
- Restricted site
- Policy violation
- Blocked application
- Blocked file type
- Patience (slow download from web server)
- Invalid certificate (HTTPS)

At the discretion of the administrator, the notification page can contain the following information:

- Requested URL
- Reason for denial of access
- Company logo

When attempting to download large files, end users will also see a patience page, complete with a progress indicator (effective from mid-2007).

The administrator can also set the language of the notification page (English, French, Spanish, German, or Italian), as well as the page title and additional comments. See Figure 9 on the next page for details.

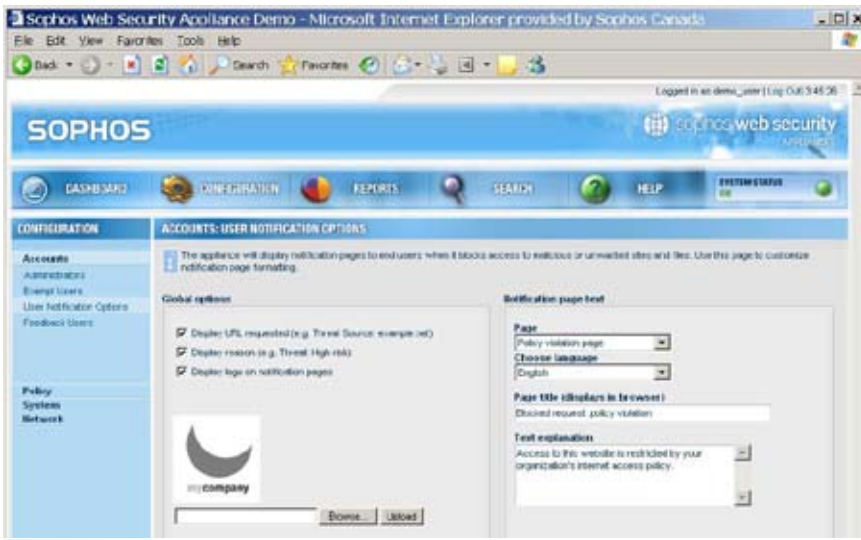


Figure 9: Notification configuration page

The WS1000's notification capabilities help to maintain a sense of transparency around an organization's web security policy, and demonstrate the effectiveness of the appliance in keeping malware and unwanted or dangerous content off the network.

Feedback users

Another way to ensure a safe and pleasant browsing experience for end users is to allow them to request modifications to the web security policy based on the notification system described above. The administrator can appoint Feedback users, allowing them to request policy changes such as risk reassessment, URL reclassification, and file type or application permission changes. Requests are made simply by clicking on a link in the notification page.

Administrators can extend this option from no users to all users, or they can configure a customized list of users and/or IP addresses that are able to submit these requests. If a reclassification request is approved, the new classification overrides the default classification provided by Sophos.



Figure 10: Feedback user selection

4: MANAGING THE APPLIANCE

Overview

As expected from an appliance, the WS1000 delivers maximum security with minimum administrative burden. Capitalizing on Sophos's extensive experience detecting viruses, spam, and other types of malware, the WS1000 features strong default policy settings that take the guesswork out of system configuration. If customization is required, the straightforward management console makes it quick and easy.

Ongoing administration and control of the web gateway is greatly simplified by the wide range of tools and settings designed to eliminate or automate the vast majority of administrative tasks, following a strict philosophy of exception-driven management. This section briefly outlines the daily administrative tasks involved in managing the WS1000.

Management console and dashboard

The management console is the secure graphical user interface between the system administrator and the appliance, enabling administrators to:

- Configure system, user, and network settings
- Configure the security and content filters
- Monitor system status and diagnose interruptions
- Manage user feedback
- Generate real-time reports on site access, user activity, threat encounters etc.

“ I was particularly impressed with the intuitive management console, which allowed me to quickly navigate and view web traffic statistics, usage and performance reports. ”

Wally Eisenhart,
Sungard Pentamation



Figure 11: Management console dashboard

The dashboard (see Figure 11) is the console's home page, providing an instant summary of overall system performance. From the dashboard, the administrator can check on web traffic, monitor protection status, measure system performance, and ensure system availability. Built on a strict discipline of minimal navigation, every feature of the console is no more than three clicks away, and command-line access is **never** required.

You can find more details on the WS1000's powerful yet easy-to-use management tools later in this section.

Monitoring, alerting, and notification

The WS1000 reduces the administrative burden by closely monitoring system status via an intricate network of more than 40 built-in system sensors. When a sensor is triggered, a visual alert and/or an email or text message is sent to the administrator. Logging in and clicking on the **System Status** button provides quick, at-a-glance feedback on the situation, together with recommended steps for resolution.

For a mission-critical condition requiring external assistance, (e.g. failed power supply), an alert is also sent to Sophos in order to fix the problem. Sophos can often resolve such a condition before the administrator is aware of it. See Section 6 for more details.

Put simply, if there are no alerts or notifications from the WS1000 or from Sophos, then everything can be assumed to be working as intended and no interaction or intervention is required. Administrators are notified only if something requires attention – otherwise, they can focus on other priorities in complete confidence that the web gateway is threat-free and operating efficiently.

Reduced administration

More than 40 system sensors keep track of the appliance so you don't have to.

Status checks

Administrators can instantly determine the overall status of the WS1000 by logging on to the management console and checking the **System Status** indicator at the top right of any page (see below, circled in red). Green (OK) indicates all systems are normal; yellow (Warning) indicates a temporary or low-level disruption; red (Critical) indicates a critical disruption.



Figure 12: System status page

In the event of a critical disruption, the WS1000 will also send an email alert to the named technical contact, as well as to Sophos.

Clicking on the System Status indicator leads to a complete set of details on the following environmental characteristics of the WS1000:

- **Traffic:** spikes in viruses and unwanted files and applications, page latency, scan queue length, and scan time
- **Hardware:** sensors covering hardware component performance, temperature, memory usage, etc
- **Software:** process health, protection status, connection to Sophos, system reboot, and system updates
- **Licensing:** time remaining on the software license.

As shown in Figure 12, the System Status page displays an indicator for each monitor, as well as a message that explains the current status, instructions for remediation, and the date and time of the last exception. If an exception occurred, the administrator would be able to click on it to see more details of what exactly happened and what action, if any, took place automatically.

From this one page in the management console, the administrator can check into every critical operation of the WS1000. The System Status page makes it easy to conduct spontaneous comprehensive reviews of overall performance and protection status, and to obtain guidance on how to rectify system interruptions.

Updates

The WS1000 connects to Sophos every five minutes to download updates to threat definitions, the Sophos list of rogue web sites, and the operating software. By default, these updates are downloaded and applied automatically. The administrator has the option of downloading and applying non-critical software updates on a fixed schedule, or conducting on-demand, one-click updating separately from the preset schedule. Non-critical updates can be deferred for up to seven days, and will be automatically applied within the update window selected by the administrator. Critical software updates such as vulnerability patches are applied immediately.

Configuration backup and restore

Administrators can set up the WS1000 to initiate automatic FTP backups of configuration data and system logs. These backups can take place on the following schedule:

- Daily at midnight
- Weekly on Friday at midnight
- Monthly on the first day at midnight.

Configuration data can also be backed up manually with one click on the **System Backup** page in the management console (see below).

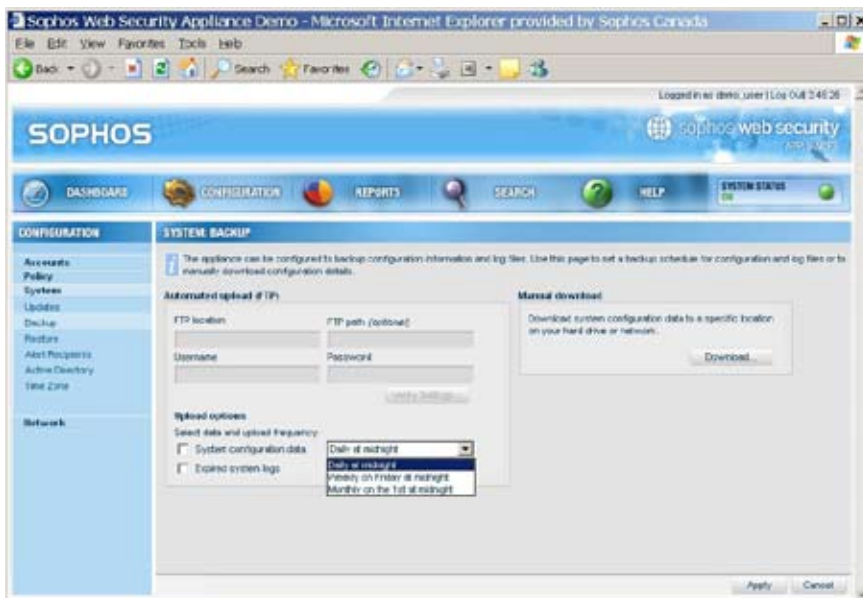


Figure 13: Configuration backup

The WS1000 uses automatic log expiry and archiving in order to maintain optimum performance and ensure adequate onboard storage capacity. If the data on the hard disk reaches 70% of capacity, data will be automatically archived so that a minimum of 40% of disk capacity is available.

Administrators can also restore system configuration and the local site list from a previous backup quickly and easily. The management console includes a simple interface for restoring these settings (see Figure 14).

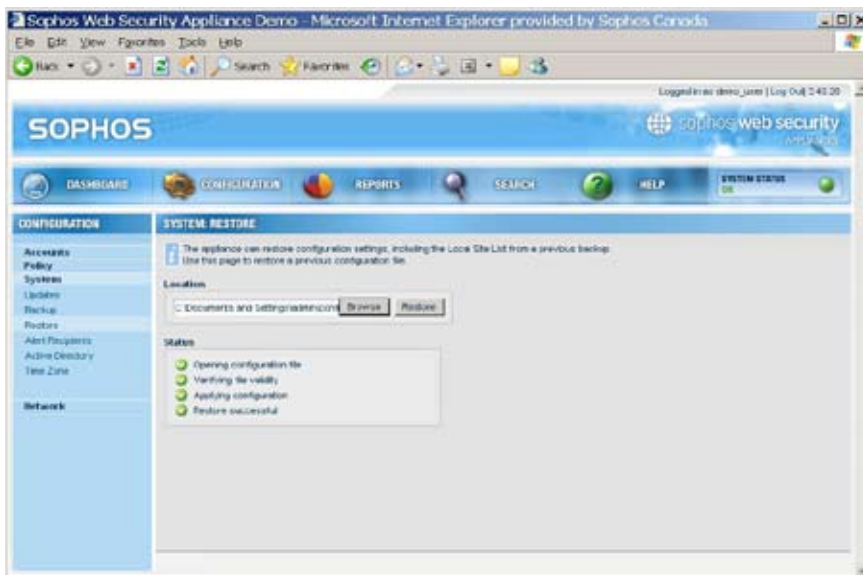


Figure 14: System restore

Managing user feedback

As discussed on page 20, administrators can allow a specified list of users to provide feedback on policy settings. When these users encounter a notification page relating to a policy violation, they can click on a link to create a request for the administrator to adjust the policy. For example, if users attempt to reach a web page that is blocked due to incorrect classification, they can submit a request for reclassification and/or unblocking.

All user feedback appears within the **Search** function on the management console, divided into three categories under User Reports:

- Sites
- Applications (e.g. browser plug-ins, toolbars, media players, etc)
- File Types (e.g. archives, documents, executables).

The administrator can approve or deny requests simply by clicking on an **Actions** button (circled in red below) at the far right of the screen. Approved URL changes will automatically appear on the local site list. Approved applications and file types will appear on the relevant policy exception list in the Configuration section of the management console.

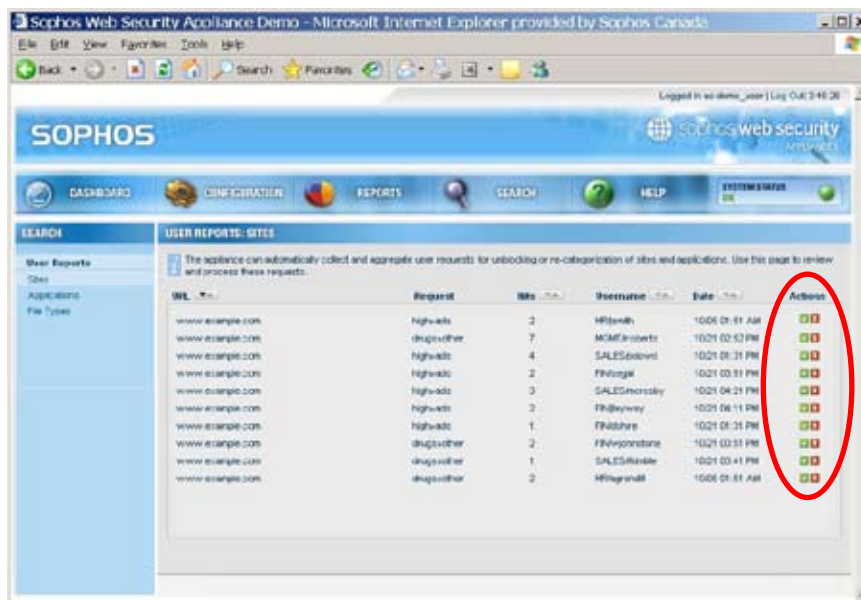


Figure 15: User requests for site approval or reclassification

Active Directory integration

The WS1000 enables rapid setup of users and user groups through advanced integration with Active Directory (AD), enabling user authentication in policies and reports, as well as opt-outs based on AD usernames.

On the Active Directory configuration page, the administrator can automatically detect and import AD settings, or settings can be entered manually.

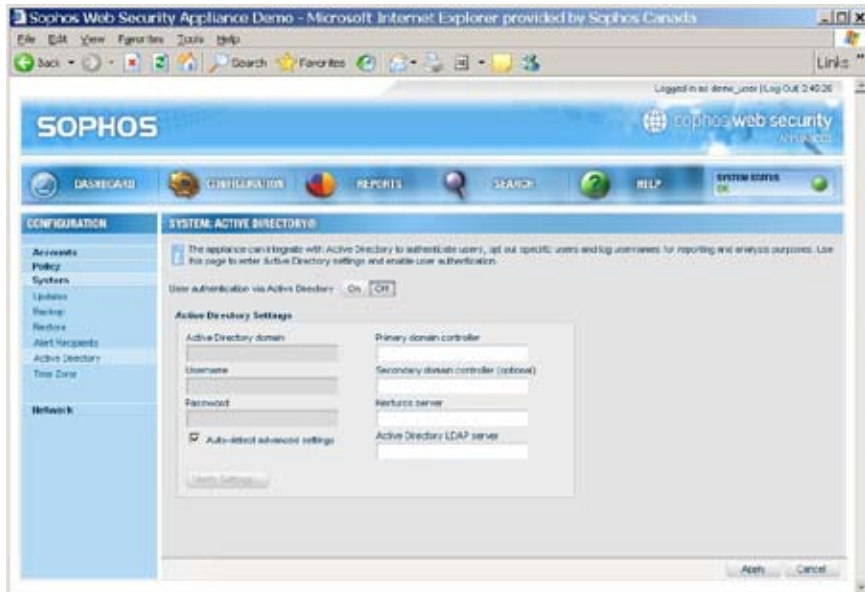


Figure 18: Active Directory configuration page

For security purposes, the WS1000 does not store a local synchronized copy of the Active Directory database. As an added safeguard, if authentication is enabled, the appliance will alert the administrator if the AD server is inaccessible.

5: REPORTING

Overview

In order to maintain control and visibility over the web gateway, administrators need a detailed understanding of what is happening with web traffic. Simply knowing that the network has up-to-date protection from spyware and viruses is not enough; administrators are often called upon by senior management to provide a more complete analysis of the web gateway, and this requires them to delve more deeply into the traffic, browsing behavior, and how the hardware and software are performing. The WS1000's real-time reporting capabilities make it easy to acquire this level of awareness, leading to more informed management and smarter system administration.

While it is important to understand what is happening currently, it is at least as important to understand what is changing over time. The WS1000 provides a wide range of relevant, actionable reports to help you understand what goes on at the web gateway, and to help you plan for future capacity requirements as your system grows.

Aggregate reports are delivered in two locations within the management console. Key statistics such as data transfer and threat behavior are summarized on the dashboard (see Figure 11 on page 22) for quick, at-a-glance viewing. More complete statistics covering a wider spectrum of information are accessible from the **Reports** page. Both areas are discussed below.

Dashboard reports

The dashboard is designed to provide a quick summary of live system performance, automatically refreshing the data every five minutes. The dashboard groups this data into three sections: Summary Statistics Today, Web Traffic, and Traffic Patterns – providing easy access to the most frequently referenced statistics.

Summary statistics today

To the right you can see the summary statistics panel that appears at the far left of the dashboard. These statistics reveal daily and peak users, latency, and aggregate data on bandwidth and data transfer. These statistics quickly demonstrate key characteristics of your web traffic since midnight.



Web traffic

In the lower middle section are two dials measuring throughput (kbps) and latency, or the time it takes the WS1000 to scan and deliver a page request.

These dials provide an instant picture of the speed of web traffic flowing through the WS1000, and how long it is taking the WS1000 to process page requests. If the dial on the left (throughput) is topping out, it could indicate a surge in web downloads. If the latency dial is topping out, it could indicate a network connection problem.



Traffic patterns

On the bottom right of the dashboard are three line graphs that measure daily throughput, virus levels, and attempted visits to high-risk sites. This information is useful in gaining a comparative view of today's traffic versus the previous seven days.

The white fill area represents up-to-the-minute daily traffic flow (midnight to midnight), while the red line represents a running seven-day average. If there is a noticeable difference between the two patterns, there could be a traffic spike or virus outbreak (white higher than red), or a connection/relay problem (red higher than white). Note that since these graphs measure the true nature of the traffic flow, a spike in viruses or high-risk sites would indicate that the WS1000 is intercepting these threats, keeping them off the network.



Reports page

Clicking on the **Reports tab** on the management console navigation bar reveals a greater scope and depth of reports. From this section of the console, administrators can obtain a highly detailed account of browsing habits and system performance, providing excellent insight into what the organization's users are doing on the web, and what danger their behavior may pose to the network.

The navigation pane at the left of the **Reports page** links to a wide range of customizable, dynamically generated reports. These reports are grouped into three categories, as shown in the table below:

Category	Report name	Description
Trends	Volume	Breaks down the web traffic into risk components ¹
	Suspect computers	Spyware "call home" traffic by IP address
Performance	Latency	Average time (in seconds) for WS1000 to scan and deliver content
	Throughput	Amount of data (Mbps) passing through the WS1000
Traffic patterns ²	Sites	The most frequently visited web sites
	Blocked sites	The sites most blocked, by request volume
	Users	The top web browsers and their top 5 destinations
	Site categories	The most visited site categories
	Downloads	The top downloaded files and applications

1 High risk, Medium risk, Low risk, Trusted sites, Uncategorized sites, Policy violations, Blocked files and viruses.

2 The top five appear in a pie chart, with other listings appearing only in the table.

The following options can be applied to every report listed in the table on the previous page:

Parameter options	Data plotted (where relevant)
Today	Sites visited
Yesterday	Bytes consumed
Last x days	Unique users
Last x weeks	
Last x months	
Custom date range	

These reports run in real time, and can be customized by the administrator to reflect a specific period of time. Each report can be exported (in csv format) for further offline analysis. For example, an exported report can be included in a presentation to senior management or to the compliance officer to demonstrate the effectiveness of the WS1000 in maintaining web security.

Of particular interest is the second Trends report, **Suspect Machines** – a simple yet highly useful report that pinpoints machines on the network that are infected with spyware. It identifies the IP address of any machine attempting to call home to known spyware sites, either to receive malware updates or to upload stolen information. With the information gathered in this report, administrators can determine precisely which machines need to be taken off line and cleaned up.

See Figure 4 on page 15 for details of the Suspect Machines report.

Reporting using log data

There can be occasions when administrators need to go further back than the time frame allowed via on-box searching (logs are backed up and expired according to a set schedule). For example, there might be a need to explore the browsing history of an individual user suspected of breaching the organization's acceptable use policy. In such a case administrators can review exported log data. The data is exported in standard Squid format, and can be analyzed using a range of free and effective analysis tools such as Kraken (www.krakenreports.com).

Note: log exporting will be available from mid-2007 and is a free upgrade to all WS1000 users. Sophos does not support any analysis tools provided by other parties.

6: SUPPORT

The Managed Appliance

Sophos Web Appliances introduce a new concept in network security: the Managed Appliance. A Managed Appliance combines the advantages of an appliance solution – ease of use, platform independence, robust security – with the advantages of a managed service – outsourced security, high availability, high capacity. The Managed Appliance, however, resides within your own network, preserving the control and visibility that is sacrificed through a managed service. Merging these two form-factors into one product provides peace of mind and confidence that cannot be obtained elsewhere.

The concept of exception-driven management is a cornerstone of Sophos Managed Appliances. The WS1000 will initiate contact with the administrator only when action is required – if there is no contact from the WS1000, then all is well and the administrator can focus on other priorities.

The sections below provide an outline of the features that distinguish the WS1000 as a Managed Appliance.

Automatic updates

In order to maintain up-to-date threat protection, most competitive appliances initiate a data lookup every 30 or 60 minutes. With the increasing pace and rapidly evolving scope of web-based threats, this practice can introduce considerable lags in gateway security. The WS1000 eliminates these lags and improves security by automatically downloading new threat definitions from SophosLabs every five minutes.

Updating at this frequency enables Sophos to narrow the gap between discovering a new threat and offering protection against it. It also reduces bandwidth consumption by requiring significantly smaller update file sizes – an important factor in the timing and effectiveness of protection. The result is the most reliable and dependable web security available.

New threat definitions and critical software upgrades are applied automatically upon download. Non-critical software upgrades can be applied instantly, or according to a schedule determined by the administrator. See Figure 19 on the next page for details.

Heartbeat monitoring

Security made simple

If there are no alerts generated by the appliance, then web security is performing as expected and there is no need for intervention.

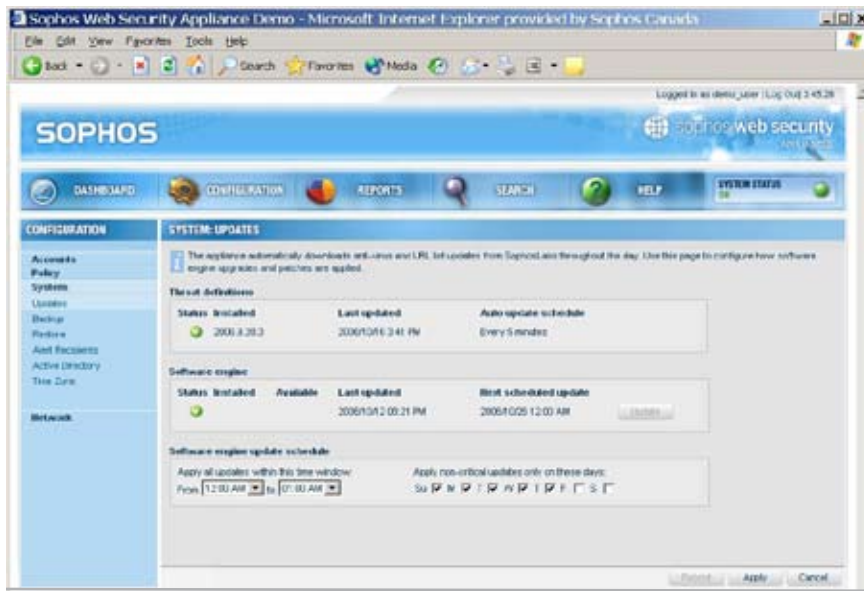


Figure 19: System Updates page

Frequent downloads go a long way to ensuring the best security possible. Sophos takes this concept one step further by remotely verifying that each appliance is equipped with the most up-to-date threat definitions. Sophos does not simply push out scheduled updates – instead, Sophos appliances pull updates from a central repository. The repository actively checks to make sure every installed WS1000 appliance “phones home” and downloads the updates on schedule. If a WS1000 fails to make contact for more than two hours, the repository alerts the Sophos support team to contact the administrator and investigate the situation.

This unique “heartbeat” monitoring provides valuable reassurance to administrators, who no longer have to worry about whether or not their web gateway security is up to date.

Alerting

The WS1000 uses more than 40 different sensors to monitor everything from Active Directory synchronization to virus spikes. Most of these sensors appear on the System Status page in the management console. If a sensor detects behavior outside the normal operating parameters of the appliance, it generates an alert that appears on this page, along with a recommended course of action for remediation. The System Status button on the navigation bar also changes color as a visual indicator – green for normal, yellow for a warning, and red for a critical alert. Clicking on the button leads to the System Status page, where further details can be found and, if required, corrective action can be initiated.

The nature and severity of the condition can also trigger an email alert to the administrator (or other assigned individual). This provides the advantage of not requiring the administrator to be logged in to the appliance in order to check on its status.

Depending on the condition itself, the WS1000 can also send an alert directly to Sophos support, as a step toward more rapid remediation. When

Proactive alerts

Alerts can be sent to an assigned individual when the administrator is not available, and mission-critical conditions automatically alert Sophos to take pre-emptive action.

this occurs, Sophos can initiate corrective action without contacting the administrator. For example, if one of the two power supplies fails, Sophos can initiate delivery of a replacement before the administrator even knows of the failure.

Appendix I provides a list of the built-in sensors and the alerts they can trigger.

On-demand remote assistance

Sophos Web Appliances feature a robust, searchable Help index to assist with troubleshooting. If the administrator cannot resolve a system problem, a request can be made for live, secure remote assistance from a Sophos engineer. The remote assistance session, which can only be initiated by an administrator with proper security clearance, allows the Sophos support representative to access the WS1000 to assist with troubleshooting. The session uses Secure Shell (SSH) technology that does not require any change to firewall settings, and expires automatically after four hours for additional security. Furthermore, every modification made to the WS1000 by the Sophos engineer is fully logged and recorded, right down to the keystrokes, as an exhaustive compliance measure. This safeguard ensures that remote assistance sessions do not materially compromise the integrity of your web security.

Warranty

Sophos offers an Advance Replacement Warranty on every Web Appliance, for up to three years. Should the appliance fail due to a manufacturer's defect during normal use while running with a valid software license, Sophos will automatically send a replacement unit to the customer before they are required to send the defective unit back. This warranty, standard on every WS1000, demonstrates the confidence that we have in our appliances, and provides the peace of mind administrators deserve.

There is never a need for a customer to open the lid of the WS1000 for servicing or maintenance. For security purposes, opening the lid will void the product warranty and trigger an alert to Sophos.

For complete details on the WS1000 warranty, please consult the End-User License Agreement.

Standard Sophos support

Sophos offers the most accessible and dependable live support in the industry. With offices in the UK, USA, Canada, and Australia, we can deliver live telephone support or email to customers around the world, 24 hours a day, 7 days a week. This service is standard with every Sophos product. Sophos support is **not** outsourced, and never closes – if you need to talk to an engineer, we're always just a phone call or email away.

Industry-leading support

The excellence of Sophos support services is unrivaled in the security industry – it's what sets us apart from other vendors.

APPENDIX I: DEFAULT POLICY SETTINGS

Security filter: This first layer of defense is applied to every user request. It determines whether the request is allowed and how the subsequent response is evaluated for security threats.

Risk level	Description	Default action
High	These sites have been analyzed by SophosLabs and have been found to host malicious content that can compromise network security.	Block
Medium	These sites have been analyzed by SophosLabs and have a history of poor privacy/security practices that may compromise network security.	Block
Low	These sites are periodically reviewed by SophosLabs to verify site contents. They have no recent history of malicious content or behavior. For optimal performance, the appliance will scan only vulnerable file types.	Scan
Trusted	These sites will not be analyzed or reviewed by SophosLabs. Allow without scanning any files.	Allow
Unclassified	For optimal performance, unclassified sites are treated by default with the same policy as low-risk sites.	Low risk

Category filter: The second layer of defense is applied to user requests that are allowed through the security filter.

Risk level	Description	Default action
Entertainment	Includes sites that provide non-business-related content, like online games, shopping, and dating services (e.g. ebay.com, games.yahoo.com, match.com).	Allow
Communications	Includes sites that provide online communication tools or services like chat rooms, forums, and webmail (e.g. chat.yahoo.com, messenger.msn.com, webmail.aol.com).	Allow
Media	Includes sites that provide news, current events coverage, and advertising (e.g. bbc.com, www.rightmedia.com).	Allow
Search	Includes search engines, portals, and job search sites (e.g. google.com, monster.com).	Allow
Questionable	Includes sites that provide adult material, and information on alcohol, drugs, gambling, and weapons.	Block

Download filter: The third layer of defense is applied to specific file types that are allowed through the other filters.

- All files types allowed (once evaluated for security threats).

Certificate validation: This feature provides added security against threats traveling over HTTPS by evaluating certificate validity.

- Disabled.

APPENDIX II: MANAGED APPLIANCE SERVICE LEVELS

Sophos Managed Appliances deliver both proactive and reactive support to ensure greater system availability and performance, and greater peace of mind.

Proactive support is initiated whenever a condition arises that prevents the appliance from operating normally – including any hardware-related failure as well as critical software or OS-related failures. Proactive support depends on the array of sensors built into each appliance that monitor its health and performance.

There are two types of alert generated by the appliance: they are denoted as critical or non-critical, depending upon the specific event or condition. For critical alerts, Sophos will notify the customer by email or text message **within one hour** of receiving the alert. For non-critical alerts, Sophos will notify the customer by email **within two hours** of receiving the alert.

Reactive support responds to inbound customer inquiries or requests for remote assistance – including live telephone support available 24x7x365, and email-based support. Inbound Help requests are handled by trained Sophos support technicians located in our offices around the world. Sophos customers are always able to talk live to Sophos support staff – if the nearest support center is closed, calls are rerouted to the most appropriate location, based on time zone. The same methodology is used for resolution. If a support request is not closed during normal business hours, it is forwarded to the next available center, and so on, until it is resolved. This follow-the-sun approach provides the fastest and most dependable support service level in the industry.

Example support scenarios:

Support level	Example condition	Response time	Response type
Proactive	Communication between appliance and software repository severed for more than 60 minutes (Heartbeat)	1 hour from Support receiving alert (no more than 2 hours from the time the condition occurs)	Standard support: Email or text message Premium/Platinum support: Phone
	Complete failure of hardware where no websites are filtered	1 hour from Support receiving alert*	Standard support: Email or text message Premium/Platinum support: Phone
	Software error causing minor loss of functionality, with no direct impact on website filtering	2 hours from Support receiving alert	Email/text message (all support levels)
Reactive	Configuration error	Live 24x7x365	Phone, email, online knowledgebase, built-in Help
	General operating procedures	Live 24x7x365	Phone, email, online knowledgebase, built-in Help

* New hardware can only be shipped during business hours.

SOPHOS

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

warg070411/070814



security and control