

# SOPHOS

## SafeGuard PortProtector 3.30 SP6 Reviewer's guide

Document date: March 2010



## Important Notice

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Sophos. Such information is supplied solely for the purpose of assisting explicitly and properly authorized SafeGuard PortProtector users, reviewers and evaluators.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the express prior written permission of Sophos.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this guide is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and on express understanding that Sophos shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

Boston, USA | Oxford, UK

© Copyright 2010. Sophos. All rights reserved. All trademarks are the property of their respective owners.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

## About This Guide

The reviewer's guide presents an overview of SafeGuard PortProtector 3.3, provides an explanation of how it works, and guides you to an understanding of how to use SafeGuard PortProtector to guard your network endpoints.

The following issues are covered in this guide:

- About Sophos
- The Need
- The SafeGuard PortProtector Solution
- Features and Benefits
- Product Walk through

# Contents

1	About Sophos .....	5
2	The Need.....	5
3	The SafeGuard PortProtector Solution.....	6
4	Features and Benefits.....	8
5	Product Walkthrough.....	14
6	SafeGuard PortProtector Implementation Workflow .....	29

# 1 About Sophos

Sophos software solutions protect an organization's confidential information from loss and theft by monitoring, detecting, and restricting data transfers from the endpoint. SafeGuard PortProtector and SafeGuard PortAuditor provides organizations with the visibility needed to assess and manage vulnerabilities in an enterprise's PCs and laptop environment by identifying and logging all devices that are or have been locally connected.

SafeGuard PortProtector guards against corporate data loss while facilitating compliance with regulatory data security and privacy standards by monitoring real-time traffic and applying customized, highly-granular security policies over all physical, wireless and storage devices. SafeGuard PortProtector provides an additional layer of security by ensuring that mobile users' data is secure by encrypting any data written to removable storage devices and CD/DVDs or by enforcing the use of hardware encrypted flash drives only.

Sophos' solutions, available through channel partners worldwide, are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe.

# 2 The Need

Enterprise networks are currently characterized by a proliferation of easily accessible computer ports, such as USB, FireWire and PCMCIA. In addition, a variety of communication adapters (such as Bluetooth, IrDA and WiFi) and device types (such as storage devices, printers, digital cameras, smart phones and PDAs) all enable effortless access to endpoints using these ports and devices.

These devices enable optimal accessibility and productivity, but they leave endpoints wide open to infiltration. With the amount of corporate data residing on endpoints estimated at over 60%, endpoints may be the most valuable, and vulnerable, part of the enterprise network.

Today, enterprise IT is focusing on the tradeoffs between productivity and security. Enterprises' need for productivity attracts them to innovative devices and security concepts. But they are severely challenged to maintain the ultimate precautionary measures against leakage, theft, fraud, virus invasion, eavesdropping and the general misuse of information and resources.

According to Vista research, 70% of IT security breaches originate from within the enterprise. Thus, enterprises today are making internal security, especially internal access to network resources, their highest priority, even above gateway solutions like antivirus and firewalls. Today's greatest enterprise security challenge is providing access to key information without exposing it to risk and trusting internal users while retaining enough control over their actions to verify their reliability.

It's simply too easy to connect a smartphone, MP3 player, digital camera, or memory stick – and walk away with sensitive or confidential material. The damage: almost \$50 billion to US companies last year alone (The Economist).

Existing endpoint security solutions either leave endpoint ports completely inaccessible – lowering productivity – or rely wholly on the assumption that policy will be obeyed. As a result, organizations today must choose between endpoint accessibility and endpoint security.

In order to secure vulnerable endpoints and maintain data integrity and regulatory compliance, organizations need to achieve both visibility and control over endpoints. Sophos develops comprehensive endpoint data leakage prevention solutions that enable organizations to enjoy the productivity benefits of mobile computing – without sacrificing security.

### 3 The SafeGuard PortProtector Solution

Together with SafeGuard PortProtector Auditor, SafeGuard PortProtector provides a comprehensive solution that identifies endpoint vulnerabilities with complete visibility into port and device activities and enforces granular security policies to protect data in use, in motion and at rest.

SafeGuard PortProtector guards confidential data stored on enterprise PCs and laptops against loss, tampering and theft by both monitoring the transfer of sensitive data as well as controlling access to removable storage devices and wireless communication ports, including:

**Physical interfaces:**

USB

FireWire

PCMCIA

Secure Digital (SD)

Parallel

Serial

Modem

Internal Ports

**Wireless:**

WiFi

Bluetooth

Infra Red (IrDA)

**Storage:**

Removable Storage Devices

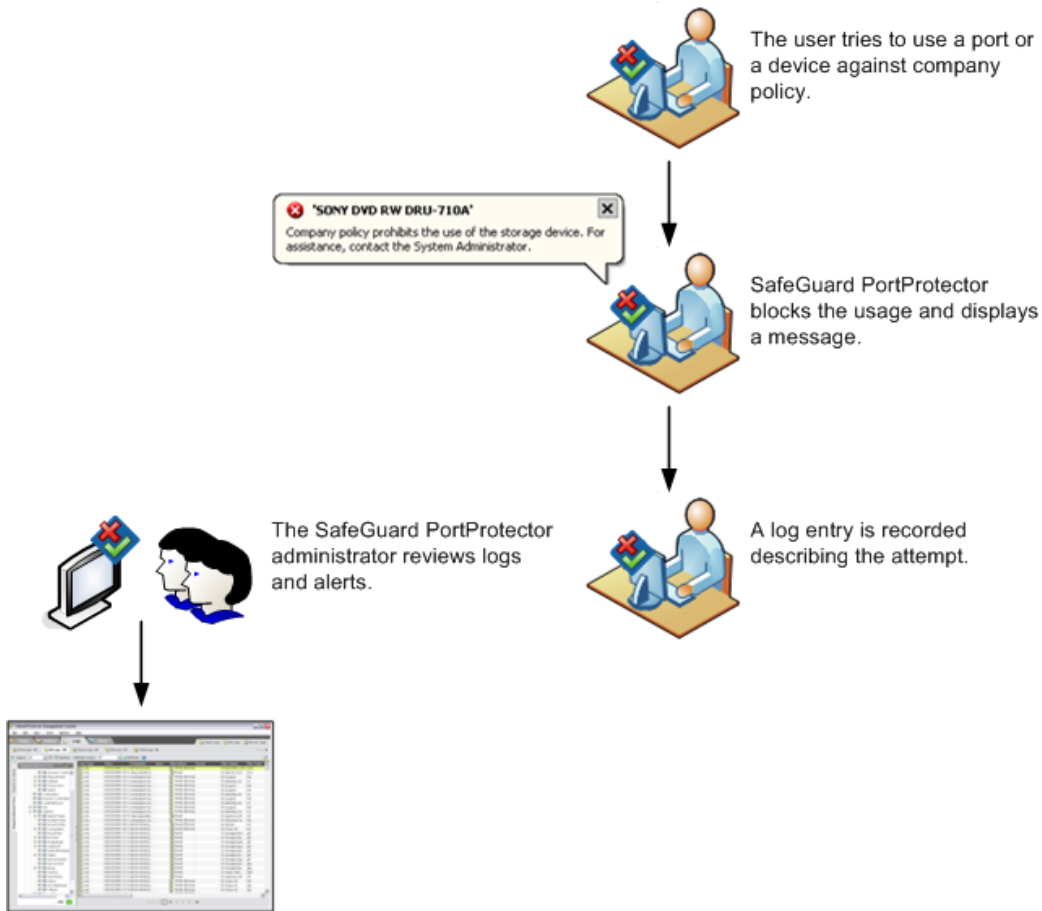
External Hard Drives

CD/DVD Drives

Floppy Drives

Tape Drives

SafeGuard PortProtector provides granular control by allowing, blocking or restricting access by device type, model or even specific device serial number. For storage devices, SafeGuard PortProtector allows security administrators to either block all storage devices completely, permit read-only access, encrypt all data on devices as well as the ability to monitor and regulate which files are read from or written to these devices. WiFi controls are based on MAC address, SSID, or network security level.



Various customized policies can be defined and automatically distributed according to any of the organizational object (OUs, Groups, computers and users) already defined in your Active Directory or Novell eDirectory.

This functionality provides the missing link in corporate security solutions by providing secure, smart, intuitive and central control over an organization's ports, devices and storage devices. SafeGuard PortProtector thus ensures that users will only be able to use approved devices through permitted ports.

## 4 Features and Benefits

- **Granular control** - detects and restricts data transfers by device type, device model, unique serial number, file type as well as actual content.
- **Policy flexibility** - separate policies can be defined for any domain, group, computer, or user; policies are easily associated with Active Directory or Novell organizational objects.
- **Data protection** – protects corporate data in motion by encrypting data on external storage devices and tracking offline use.
- **Advanced policy enforcement** - via independent, kernel-level, real-time analysis of low-level port traffic.
- **Secure agent** - silent deployment, redundant multi-tiered anti-tampering prevent security policy circumvention.
- **Intuitive management** - seamlessly integrates into Active Directory or other network management software.
- **Easy auditing and visibility** - Encrypted logs and alerts can be viewed in the Management Console or integrated with third-party software for comprehensive analysis or immediate notifications.

## 4.1 Feature List

Following are the main features of the product:

### 4.1.1 Security Features

- **Port Control** – SafeGuard PortProtector can intelligently allow, block or restrict the usage of any or all computer ports in your organization according to the computer on which they are located, the user who is logged in and/or the type of port. Sophos controls: USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (e.g. dialup, 3G etc.), WiFi, IrDA and Bluetooth ports.
- **Device Control** – Highly granular identification and approval of devices, including a comprehensive list of device types and robust white listing of device models and even distinct devices (by serial number).
- **Storage Control** – Special control over external and internal storage devices including Removable Media, External Hard Drives, CD/DVD, Floppy and Tape drives. Policy can block usage of device types, models and even distinct devices (by serial number), restrict usage for read only, or enforce encryption (see below).
- **Removable Media Encryption** - Unique to the SafeGuard PortProtector solution is the ability to restrict the usage of encrypted storage devices to company computers by use of encryption. This extends the security borders of organizations and **prevents** rogue employees from deliberately leaking data through removable storage and media.
- **Password Protected Access of Encrypted Devices**: Enables users to use their encrypted removable storage devices outside of the organization by protecting secure data with a password. When entering an encrypted device into an unprotected computer, the user will be prompted to enter a password. Access to encrypted data will be allowed only by using the correct password. A special administrator-assisted challenge-response mechanism allows recovering forgotten access passwords.
- **Configurable Password Policy**: Administrators can define the security criteria for the device access password. Administrators can predefine password parameters such as minimal password length and the types of characters it contains, in order to comply with the organization's security guidelines.
- **Track Offline Usage of Encrypted Devices** - SafeGuard PortProtector provides administrators with improved visibility on the usage of encrypted devices outside the organization. With this unique feature, every offline access to an encrypted device is tracked, providing a comprehensive log of each file transfer to/from this device. With this powerful log, administrators can audit users' actions even on non-company computers, in order to validate legitimate use of corporate data.

- **File Type Control** – This feature provides an additional layer of granularity and security by inspecting files for their type as they are transferred to/from external storage devices. This technology allows for highly reliable classification of files by inspecting the file header contents rather than using file extensions, thus preventing users from easily bypassing the protection by renaming file extensions. With over 180 built-in file extensions covering all popular applications categorized into 14 file categories, policy definition has never been easier.
- **File Name Logging** - Creates forensic logs of all data moving in and out of the organization via removable media and CD/DVD's.
- **File Shadowing** - The ability to track and collect copies of files moved to/from external storage devices. It is possible to set policies requiring shadowing of all data on each of the inbound and outbound channels separately as well as require shadowing for specific file types. Collected shadow files are securely stored in a central repository and available for review by authorized administrators.
- **Granular WiFi control** - by MAC address, SSID, or the security level of the network.
- **Block Hybrid Network Bridging** - SafeGuard PortProtector allows administrators to control and prevent simultaneous use of various networking protocols that can lead to inadvertent or intentional hybrid network bridging (such as WiFi bridging and 3G card bridging). Configuring SafeGuard PortProtector Clients to block access to WiFi, Bluetooth, Modems or IrDA links while the main wired TCP/IP network interface is connected to a network enables users to employ the various networking protocols only when they are disconnected from the network - avoiding the creation and potential abuse of a hybrid network bridge.
- **U3 and autorun control** - Turns U3 USB drives into regular USB drives while attached to organization endpoints, and protects against dangerous auto-launch programs by blocking autorun. Refer to *U3 Smart Drive and Autorun Control* for further details.
- **Block USB and PS/2 Hardware Key-Loggers** - Blocking USB hardware key loggers which can tap and record every keystroke in your endpoints as well as render PS/2 hardware key loggers useless.
- **Tamper Resistance** - To achieve true endpoint security, a solution needs to be virtually impossible to circumvent, disable, or uninstall. The solution needs to enforce the security policies set by administrators, without fail. Safend Protector includes redundant, multi-tiered anti-tampering features to guarantee permanent control over enterprise endpoints.

## 4.1.2 Management Features

- **SafeGuard PortProtector Management Server** - Enhances the Safend Protector system by keeping all of its data in one secure central location and ensuring its proper management. A single Management Server can be used to manage tens of thousands of endpoints, and can be accessed through the Safend Protector Management Console. Safend Protector also allows for installing a cluster of Management Servers which seamlessly share the load of traffic from the endpoints as well as serve as a hot backup for each other.
- **SafeGuard PortProtector Management Console** - all of our management tools are now combined into a single Management Console, which can be installed and run from any computer on your network. The Management Console provides unified management of policies, logs and Clients. The management console supports one-click deployment from the server website.
- **Extensive logging** - enables you to view and analyze the logs collected from all the endpoints in your organization, both immediately and over time.
- **Policy Server** – this feature enables automatic distribution of policies from the Management Server to endpoints using the existing SSL infrastructure. To facilitate this, policies are associated to the AD or Novell objects from within the Management Console, as part of the process of defining a policy. With this feature, Sophos maintains and strengthens its highly granular policy management with the ability to set policies which are more general (to OUs or Groups) as well as policies which pinpoint the specific user or computer.
- **Distribute Policies via Active Directory GPO** – SafeGuard PortProtector features tight integration with Active Directory for publishing policies via the GPO (Group Policy Objects) mechanism. This complements the ability to distribute policies directly from the Management Server, and is extremely useful for large organizations interested in leveraging existing AD infrastructures. Policies are saved as a GPO object in the AD and can be applied on users and computers. Administrators can also select a specific domain in their Domain Forest for publishing policies. This is useful for networks spread over multiple geographic locations.
- **Policy Merging** – Administrators can apply several policies to a computer or user, and the SafeGuard PortProtector Client can merge the permissions of all the policies applied to a computer/user. This is mainly useful when associating policies to user groups or for building hierarchies of permissions.
- **Policy Summary** - allows you to view and save a printed copy of your policies for backup as well as for review by people without access to the Management Console.
- **Client Management** - allows you to browse the status of your Clients and check whether they are protected by the latest version of the Client, what policy they are using, when they were last updated and more. You can manage your Clients tighter by pushing policies and collecting logs at any time, with one click.
- **Role-Based Access** Allows administrators to create role-based access to the various parts of the system. Safend also enables administrator to define Domain Partitions, with different user permissions for each Domain Partition. This accommodates the needs of large organizations which employ several security officers, each responsible for a different part of the organization.

- **Immediate Updates** – enable you to push a new policy to Clients without having to wait for the policy update interval to complete. The new policy becomes effective immediately on all connected Clients. In addition, collect all the logs that were accumulated by the Clients on endpoints immediately, without having to wait for the log sending interval to complete.
- **Active Directory Synchronization** - allows you to look at Logs and Clients from your native organizational units view, through the organizational tree. The tree is continuously synchronized with your Active Directory to ensure it remains current at all times.
- **Novell eDirectory Synchronization** - Similarly to its existing seamless integration with Active Directory, SafeGuard PortProtector supports full integration with Novell's eDirectory. With this integration the Management Server can be configured to connect the eDirectory in order to import the organizational tree, including OUs, Groups, Users and Computers. This enables viewing of directory objects (computers/user groups) through the Management Console for policy association, log filtering and Client management purposes. Administrators can also choose the root path when synchronizing with eDirectory.
- **Built-In Real-Time Alerts** – enable you to issue alerts of your choice (e. g. e-mail, SNMP and more) to desired destinations. Administrators can set the destinations for sending alerts on a per-policy basis. As an example, it is possible for alerts from different computers/users to be sent to different email addresses.
- **Configurable End User Messages** – Whenever SafeGuard PortProtector Client enforces policies on a client, a message is provided to the user in order to notify him of the policy violation. Each of these messages can be customized by the administrator on a per-policy or as a global setting. Messages can be defined in multiple languages.
- **Internal Database** – SafeGuard PortProtector includes a built-in MySQL database in order to simplify the installation of small-medium systems. This database is automatically installed with the Management Server and is fully maintained by the application. No user maintenance is required.
- **Database Management** – Administrators can set the amount of days for logs to be stored, as well as set a quota for the database files. SafeGuard PortProtector Management Server also features manual as well as scheduled backups for its keys, configuration and logs (logs backup only available for Internal Database). These backups can be used to when recovering from hardware failures as well as when upgrading hardware platforms.
- **External Database** - Customers with existing database infrastructures may prefer to use these for storing SafeGuard PortProtector configuration and log information instead of using the built-in internal database provided with the Management Server installation package. This provides higher system scalability and leverages existing infrastructures and know-how. Upon installation, SafeGuard PortProtector Management Server can connect to an existing Microsoft SQL (MSSQL) database instead of creating its internal database. Day-to-day maintenance of this database is still handled by SafeGuard PortProtector including indexing, purging, and key/configuration backup. However, in this case it is the administrator's responsibility to backup log data.

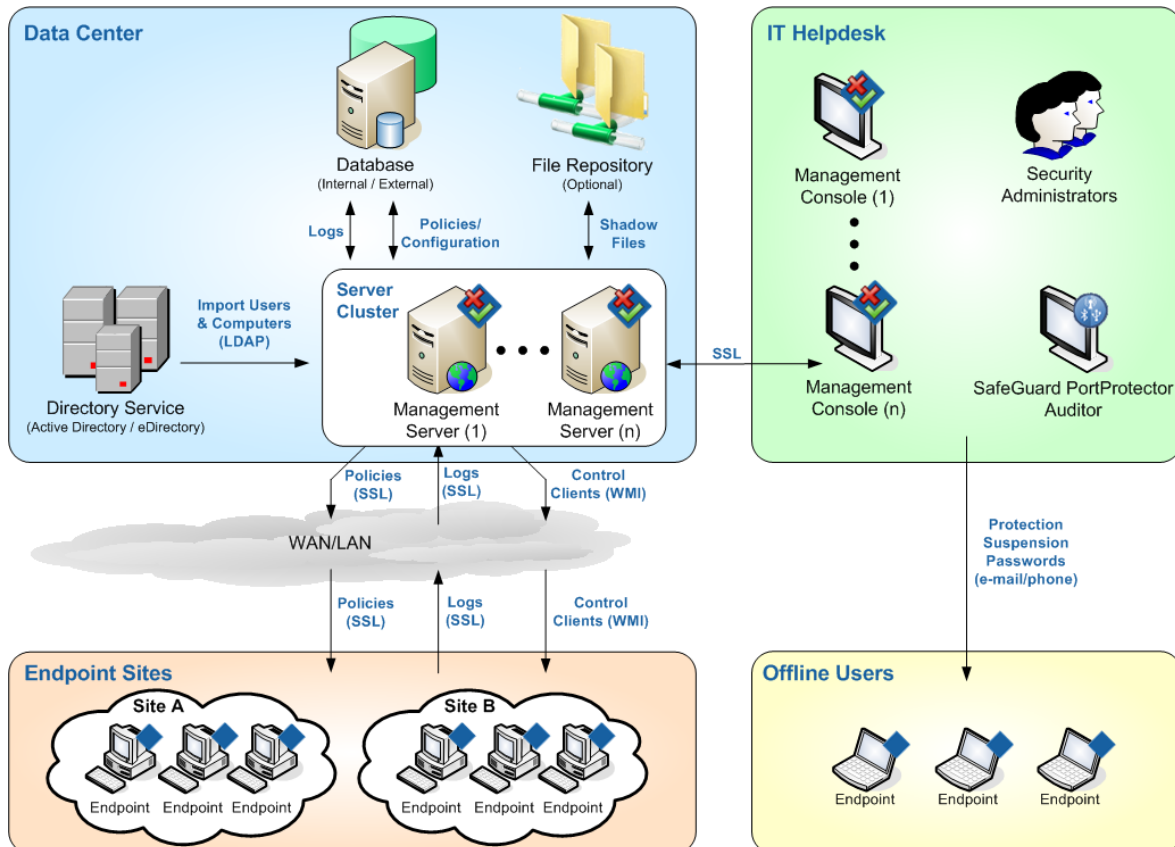
### 4.1.3 Additional Features

- **Built-In policies for Regulatory Compliance** - SafeGuard PortProtector 3.3 assists organizations in complying with regulatory requirements such as HIPAA, SOX, PCI and FISMA. Version 3.3 includes detailed guidelines on how to configure, operate, and maintain the product for compliance. SafeGuard PortProtector Version 3.3 includes built-in policies with the recommended settings for each regulatory standard. These built-in policies can be applied "as is" or can be modified to better accommodate the specific organization's security and business needs. To assist with this customization of policy settings, SafeGuard PortProtector 3.3 includes detailed guidance explaining the specific impact of the policy security settings and the associated mapping of these settings to regulatory policy statements.
- **Tamper Resistance** - To achieve true endpoint security, a solution needs to be virtually impossible to circumvent, disable, or uninstall. The solution needs to enforce the security policies set by administrators, without fail. SafeGuard PortProtector includes redundant, multi-tiered anti-tampering features to guarantee permanent control over enterprise endpoints.
- **MSI Based Client Deployment** – The client installation is packaged in an MSI file, featuring silent as well as manual installation. The client can be deployed with any 3<sup>rd</sup> party tool for MSI deployment, and more specifically Active Directory GPO, Microsoft SMS and IBM Tivoli.
- **Suspend Client** – enables you to suspend Client operation temporarily, without having to uninstall it, even when the endpoint does not have any Internet connection. This allows access to any device for the duration of the suspension, after which the original policy enforcement is resumed.
- **Stealth Mode** – SafeGuard PortProtector Client can be configured to be invisible on endpoints. In this mode, the user doesn't see the product icon and no end user messages are shown.
- **Multilingual** - SafeGuard PortProtector speaks your language, allowing easier local administration.

## 5 Product Walkthrough

### 5.1 System Architecture

The system architecture is presented in the following figure:



The system consists of the following components:

- SafeGuard PortProtector Management Server/s:** the SafeGuard PortProtector Management Server stores policies and other definitions, collects logs from Clients, enables Client management and distributes policies to Clients. The Management Server uses either an internal or an external database for its repository (see below).

The Management Server uses IIS to communicate with Clients and Management Consoles (over SSL). Clients can also be controlled by means of WMI outside the predefined server-client communication intervals. LDAP compliant protocols are used to synchronize with the existing organizational objects stored in Active Directory/Novell eDirectory.

The Management Server typically distributes policies directly to Clients (via SSL). It also supports an alternative distribution method that employs Active Directory GPOs. GPOs representing policies are written to Active Directory. After they are linked with the Organizational Units (OUs), the policies are downloaded and applied to endpoints.

You can install a single Management Server, or a cluster of Management Servers that share a single external database (with or without a database cluster). All the above-mentioned tasks are shared by the servers and each server performs every type of task so that the load is shared among all the servers in the cluster. Consequently, in the event that an individual server fails, the other servers automatically compensate for the loss, so that no information is lost.

- **Internal/External Database:** Standard databases are used for storing system configuration, policies and log data. Administrators may opt to use an internal MySQL database supplied in the Management Server installation package or to connect to existing MSSQL database infrastructures. While using the internal database is simpler and maintenance free, connecting to an external database provides better performance and scalability.
- **SafeGuard PortProtector Management Console:** SafeGuard PortProtector's Management Console is a unified management tool to be used by your IT and/or security departments for defining permissions through policies, manage Clients and monitor port, device and network usage in your organization. The Management Console integrates with your Active Directory or Novell eDirectory so that you can easily associate policies with your network computers and users.

The SafeGuard PortProtector Management Console is automatically installed on the same machine as your SafeGuard PortProtector Management Server during Server installation, and can be installed on additional computers as needed, supporting one-click deployment from the server website.

The Management Console uses SSL when communicating with the Management Server.

- **SafeGuard PortProtector Client:** protects and monitors the endpoints in your organization, and alerts/reports on port activity. The Client communicates with SafeGuard PortProtector Management Server using SSL.
- **File Repository (optional):** Shadow files collected from endpoints are stored in a central repository. The files are stored under their original file names and format in a standard file system. For the central repository, administrators define one or multiple network shares used to store the shadow files.
- **SafeGuard PortAuditor:** Although not an integral part of SafeGuard PortProtector, SafeGuard PortAuditor is a lightweight clientless tool that goes hand in hand with SafeGuard PortProtector and complements it by providing you with a full view of the ports, devices and networks currently being used (or previously used) by your organization's users. You utilize the output of a SafeGuard PortAuditor scan to select the devices and networks whose usage you want to approve.

## 5.2 Policy Definition

### 5.2.1 What Does a Policy Define?

Each policy defines two types of information: **Security** definitions and policy **Settings**, as follows.

- **Security** definitions specify the policy (blocked, allowed, restricted or other) for accessing the ports on your organization's endpoints:
- **Port Control** specifies your organization's policy regarding port access on endpoints.
- **Device Control** specifies your organization's policy regarding the devices that are allowed to access USB, PCMCIA and FireWire ports on endpoints.
- **Storage Control** specifies your organization's policy regarding the storage devices that are allowed to access your endpoints (includes encryption of removable storage devices).
- **File Control** specifies your organization's policy regarding files transferred to/from external storage devices. This controls transfers by file type as well as actual content.
- **WiFi Control** specifies your organization's policy regarding the WiFi links that endpoints are allowed to access.
- **Settings** specify how the policy behaves on the endpoint:
- **Logging** specifies the logging settings for the policy, such as the frequency at which log entries are sent to SafeGuard PortProtector Management Server from a protected endpoint.
- **Alerts** selects the destinations to which alerts for the policy should be sent.
- **End-user Messages** enables you to edit the default messages that appear on a protected endpoint during ongoing usage and when a policy violation occurs.
- **Media Encryption** determines the system's behavior when removable storage device permissions require encryption.
- **Shadowing** specifies the file shadowing settings for the policy, such as the size of the local repository on the protected endpoint on which the shadowed files are stored until sent to the Management Server, and the maximum size of the files that will be shadowed.
- **Options** enables you to define various behavioral aspects of the policy, such as how it disconnects active devices when the need arises.

## 5.2.2 How Do You Define a Policy?

SafeGuard PortProtector Policies are defined in the SafeGuard PortProtector Management Console. You can define one policy for your entire organization, or define customized policies for each organizational unit (computers and/or users) defined in your Active Directory or Novell eDirectory.

Policies need to be defined once and then updated on an as-needed basis when the need arises in your organization. To define a new policy, simply define each of the policy aspects described above and save the policy. You can choose to create an entirely new policy, or custom tailor an existing policy from the SafeGuard PortProtector's built-in list of policies.

There are several options for distributing policies: directly from the server, via Microsoft's Active Directory GPO or through registry files.

Once you have defined and distributed a policy to SafeGuard PortProtector Clients you can view activity logs from each Client through the Logs World in the SafeGuard PortProtector Management Console. Log entries include a variety of information, such as:

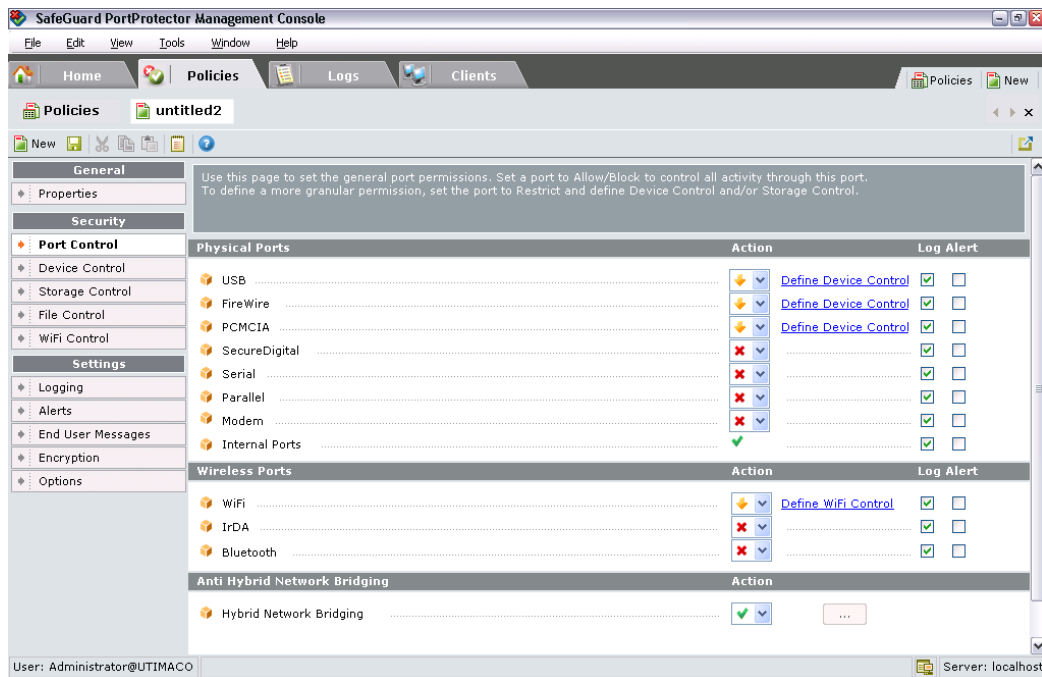
- Policy violations. For example: an attempt to use a blocked device.
- Use of read-only storage devices.
- Distribution of new policies.

After analyzing the logs, you may wish to adjust your policies.

## 5.3 Port Control

SafeGuard PortProtector can intelligently allow, block or restrict the usage of any or all computer ports in your organization according to the computer on which they are located, the user who is logged in and/or the type of port. Sophos controls: USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (e.g. dialup, 3G etc.), WiFi, IrDA and Bluetooth ports.

A blocked port is unavailable, as if its wires were cut. An indication that a port is blocked is given when the computer boots or when a policy is applied that disables a previously allowed port.



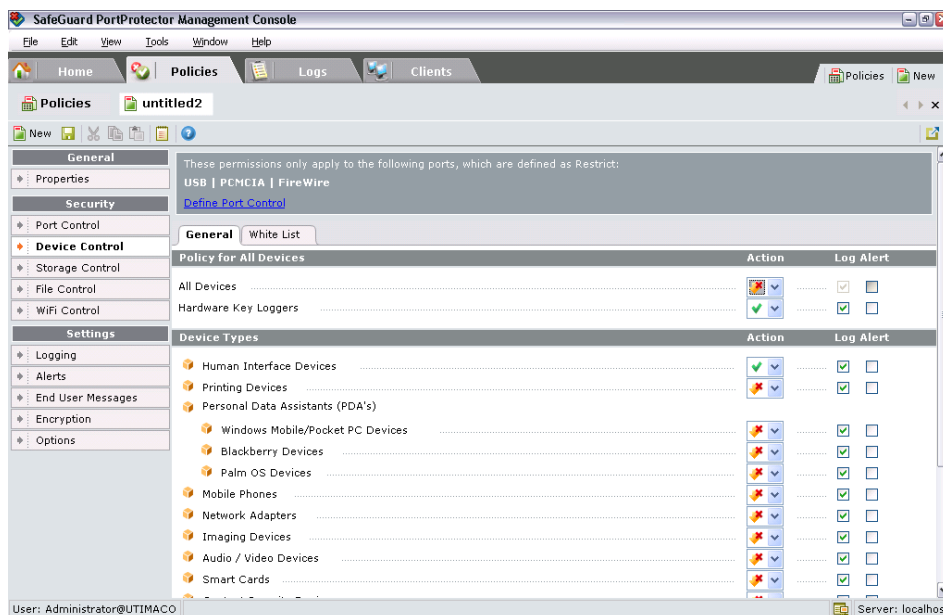
## 5.4 Device Control

In addition to controlling port access, SafeGuard PortProtector provides another level of granularity by enabling you to define which devices can access a port.

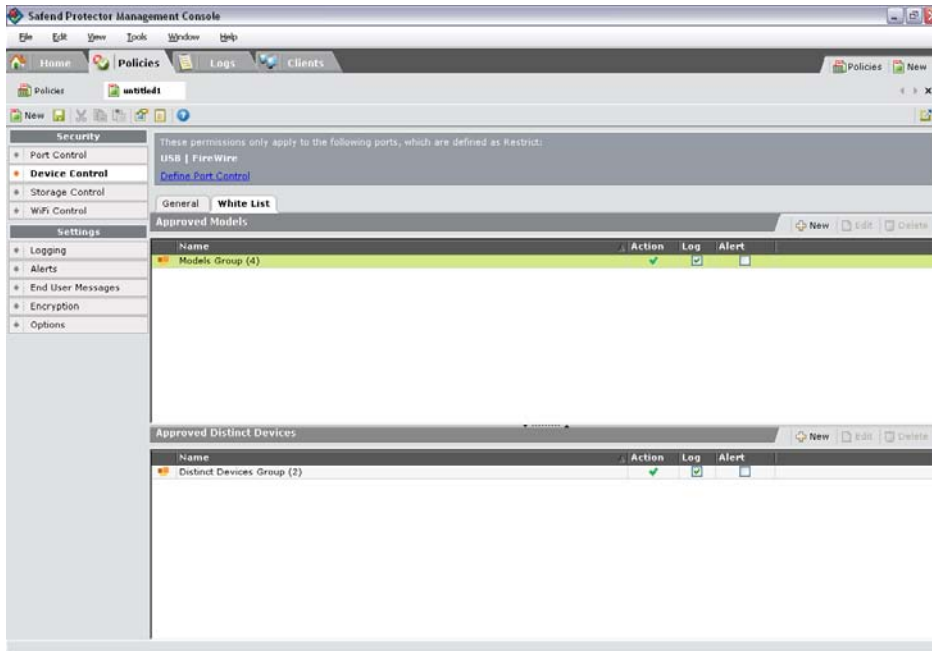
For USB, PCMCIA, FireWire ports you can define which device types, device models and/or distinct devices can access a port, as follows:

- Devices Types:** This option enables you to restrict access to a port according to the type of device that is connected to it. Examples of device types are printing devices, network adapters, human interface devices (such as a mouse) or imaging devices.

The device types that are available for selection are built into SafeGuard PortProtector. If you would like to allow a device that is not of one of the types listed here, you can use the **Models** or the **Distinct Devices** option, described below.



- Models:** This option refers to the model of a specific device type, such as all HP printers or all M-Systems disk-on-keys.
- Distinct Devices:** This option refers to a list of distinct devices each with their own unique serial number, meaning each is an actual specific device. For example: the CEO's PDA may be allowed and all other PDAs may be blocked.



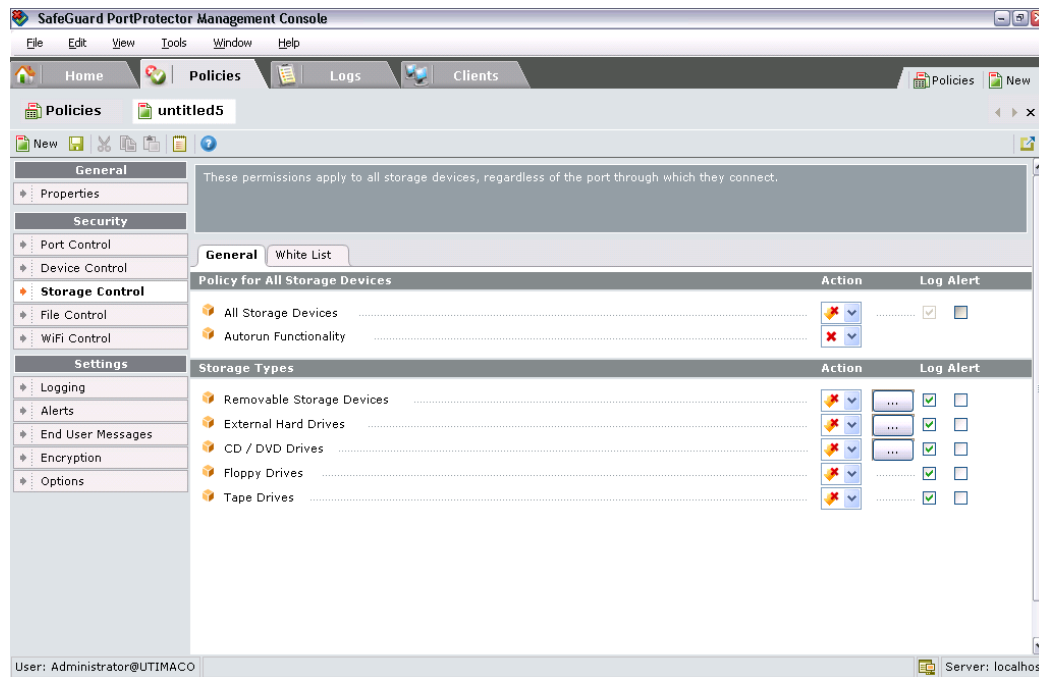
### 5.4.1 Protection against Hardware Key Loggers

Hardware Key Loggers are devices that can be placed by a hostile entity between a keyboard and its host computer in order to tap and record keyboard input and steal vital information, especially identity and password.

With SafeGuard PortProtector you can immunize your users against this threat by blocking the use of both USB and PS/2 key loggers.

## 5.5 Storage Control

Storage control provides an additional level of detail in which to specify the security requirements of your organization. This can apply to all storage devices regardless of the port they are connected to. You can block storage devices completely, allow read-only access or encrypt the device.



The Storage Control window includes two tabs: the General tab, which you use to specify which storage types are allowed access and whether internal disk encryption is activated. The White List tab, enables you use to specify which device models or distinct devices are allowed access. Similarly to non-storage devices, described in the previous section, storage devices can be also approved according to their type, model or distinct ID.

The Storage Control window, General tab includes the following sections:

- **Policy for All Storage Devices (top section):** in this area you can Allow, Restrict or Block access to all storage devices. If you select Allow or Block for All Storage Devices, the rest of the window is disabled.

This is where you set log and alert definitions for storage device activity, if all storage devices are allowed or blocked.

You can also determine whether you want to allow or block the Autorun feature available on some storage devices such as CD/DVD media.

- **Storage Types (middle section):** if you have selected the Restrict option for All Storage Devices as described in the previous paragraph, this option enables you to allow or restrict access to a storage device according to its type. In this screen you can also enforce the encryption of detachable media (Removable storage devices, External hard drives and CD/DVD drives)

The device types available for selection are built into the Safend Data Protection Suite and include the following:

- Removable Media: Applies to all plug-and-play storage devices, such as USB thumb drives, Digital Camera, Portable MP3 players and so on.
- CD/DVD Drives
- Floppy Drives
- Tape Drives

### **5.5.1 U3 Smart Drive and Autorun Control**

Certain USB-Sticks, such as U3 devices, offer smart functionality in addition to their basic storage functionality. This functionality allows them to store and run applications once connected to a host computer.

With SafeGuard PortProtector, you can let your end-users use their new sophisticated storage devices, while ensuring your endpoints are not exposed to potential exploits and risky applications these devices may carry as part of their U3 and smart storage capabilities. You can easily block both U3 and auto-launch activities as part of your security policy. Using Sophos's unique granular Client technology, you can still allow smart storage devices to be used as simple storage devices, so long as they comply with the rest of your storage policy, and block only their smart functionality which may be unsafe.

## 5.5.2 SafeGuard PortProtector Removable Storage Encryption

SafeGuard PortProtector Media Encryption allows administrators to mandate the encryption of all the data being transferred off organization endpoints to approved storage devices such as USB flash drives, memory sticks and SD cards, as well as CD/DVD media and external hard drives. This provides organizations with comprehensive protection from both accidental data loss and deliberate leakage of corporate assets.

Unique to the SafeGuard PortProtector solution is the ability to restrict the usage of encrypted devices to company computers. This extends the security borders of organizations and prevents rogue employees from deliberately leaking data through these high-capacity devices.

Within the organization, media encryption is completely transparent. End-users are able to read and write to storage devices just as they would normally do<sup>1</sup>. However, when the same device is plugged to a computer that is not part of the organization, the data on it will not be accessible.

SafeGuard PortProtector Media Encryption is designed to work company-wide. Encrypted devices can be read and used interchangeably on any computer in the organization, while existing control based on device vendor/model and Serial Number still applies.

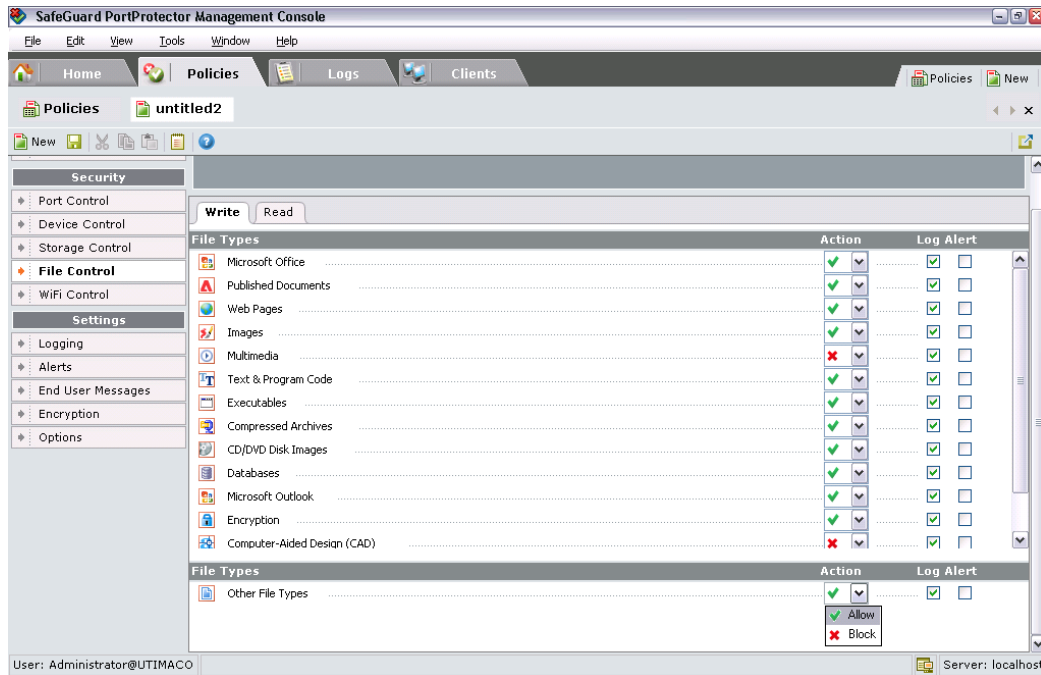
The SafeGuard PortProtector administrator can choose whether or not to allow specific users password-protected access to the data on non-authorized computers. If allowed, individual users are able to set their own device password, which is required for accessing the device on non-company computers. When plugging the device outside the organization, a utility residing on the device is used to validate this password and provide access to encrypted information.

---

<sup>1</sup> One exception is the burning of CD/DVD media. Here users are required to create an encrypted container on their machine and then to burn it to the media.

## 5.6 File Control

File Control includes an additional layer of granularity and security by monitoring and controlling file transfers to/from external storage devices. Definitions are set at the level of file type providing the ability to allow or block specific file transfers as well as to generate logs, and alerts, or even to send a hidden copy of the file to the Management Server.



### 5.6.1 File Type Control

With File Type Control a highly reliable classification of files is performed by inspecting the file header contents rather than using file extensions, thus preventing users from easily bypassing the protection by renaming file extensions. With over 180 built-in file extensions covering all popular applications categorized into 14 file categories, policy definition has never been easier.

By inspecting both files downloaded to external storage devices and those uploaded to the protected endpoint, multiple benefits can be achieved:

- An additional protection layer for preventing data leakage
- Prevention of viruses/malware introduction via external storage devices
- Prevention of inappropriate content introduction via external storage devices. Examples of such content:
  - Unlicensed software
  - Unlicensed content (e.g. music and movies)
  - Non work-related content (e.g. personal pictures)

## 5.6.2 File Logging and Shadowing

An additional level of monitoring the activity in your organization is provided in the File Logging feature, which enables you to log information written to or read from removable media devices or CD/DVD.

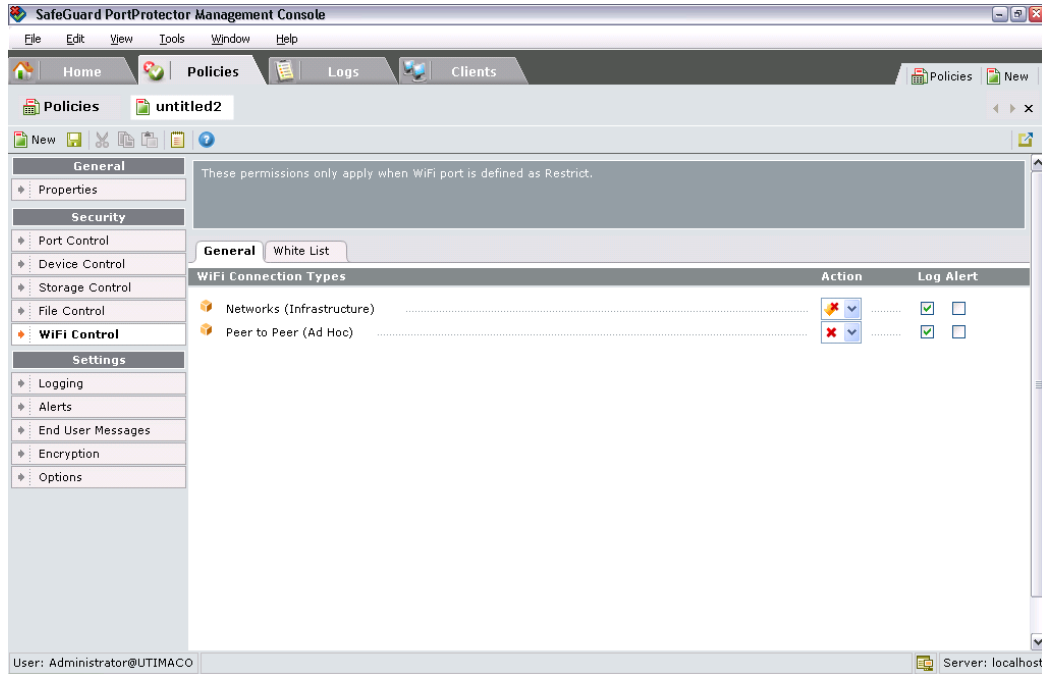
This option provides you with an audit trail of what data is transferred in and out of the organization, and may be used to analyze security incidents, as well as keep track over people's activity, and notice potential abuse of portable storage devices. It will help you better comply with security regulations you may be bound by, and will enhance your visibility into how your organizational data flows.

For highly sensitive sections of your organization, or for specific users who require special attention, you can also use the File Shadowing feature which allows you to collect copies of files moved to/from external storage devices. The files are stored in a central repository and can be viewed by authorized administrators. Please note: using this feature will influence both network utilization and storage resources. Therefore, use it with caution, preferably on small, well defined sections of your organization.

Using file name monitoring and file shadowing affords administrators the freedom to create policies that do not restrict usage of devices, yet allows full visibility of the activity and content transferred to removable media.

## 5.7 WiFi Control

WiFi control ensures that users only connect to approved networks. You can specify which networks or ad hoc links are allowed access by MAC address of the access points, SSID of the network, authentication method and encryption methods to define approved links.



## 5.8 SafeGuard PortAuditor

SafeGuard PortAuditor is a tool that goes hand in hand with SafeGuard PortProtector and complements its capabilities by providing you with the visibility needed to identify and manage endpoint vulnerabilities - a full view of what ports, devices and networks are (or were previously) in use by your organization's users. Organizations can use the output of a SafeGuard PortAuditor scan to select the devices and networks whose usage they want to approve.

**Audit Results Summary**

Report:

Report1

	Total	Connected
Total Computers	1	
Accessed Computers	1	
Successfully Audited	1	
Protected by SafeGuard	1	
USB Devices	3	3
PCI/PCMCIA Devices	14	10
FireWire Devices	0	0
Internal Storage	0	0
WiFi Networks	0	
Storage Devices	0	0
Communication Adapters	2	1

More detail is provided in the *SafeGuard PortAuditor User help*.

## 5.9 SafeGuard PortProtector Policy Enforcement – SafeGuard PortProtector Client

SafeGuard PortProtector Client constantly *monitors* real-time traffic on protected ports and applies customized, highly-granular security policies over all physical, wireless and removable storage interfaces. It *blocks* unauthorized activities (such as plug device, write to storage, connect to WiFi networks), *protects* data written to storage devices, *alerts* administrators about unauthorized usage attempts and *logs* events for future viewing and analysis.

SafeGuard PortProtector Client is a lightweight software package that transparently runs on endpoint computers, at kernel level, and enforces protection policies on each machine on which it is applied. It has a minimal footprint (in terms of file size, CPU and memory resources) and includes redundant, multi-tiered anti-tampering features to guarantee permanent control over endpoints.

SafeGuard PortProtector Client can be silently installed on all endpoints.

Policy distribution to endpoint computers can be handled either by the Management Server via SSL, or by using Microsoft's Active Directory's Group Policy Management Console or using any third-party tool that your organization has for distributing software.

Once policies have been distributed, the Client immediately starts protecting the ports of that computer without requiring a reboot.

When a violation of a SafeGuard PortProtector policy occurs or during certain usage activities, a message is displayed on the endpoint computer. A policy violation means that someone has tried to use a port, device or WiFi link that was blocked on a computer on which SafeGuard PortProtector is applied. The end-user can simply click to acknowledge that the messages were read. A log entry may be created to record this event, according to the preferences you defined in your policy.

If you wish, you may install the Client in Stealth Mode, hiding both Sophos tray icon and messages and making SafeGuard PortProtector Client invisible to the user at the endpoint.

## 6 SafeGuard PortProtector Implementation Workflow

The following is an overview of the workflow for implementing and using SafeGuard PortProtector.

- **Step 1: Install the SafeGuard PortProtector Management Server and Console**, as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 2: Install Additional Management Consoles**, as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 3: Define General SafeGuard PortProtector Administration Settings**, such as the method in which policies are published, as described in *SafeGuard PortProtector User help*.
- **Step 4: Scan Computers and Detect Port/Device Usage**. Use SafeGuard PortAuditor to detect the ports that have been used in your organization and the devices and WiFi networks that are or were connected to these ports, as described in the *SafeGuard PortAuditor User help*.
- **Step 5: Define SafeGuard PortProtector Policies**. In this stage you define the blocked, allowed and restricted ports, devices and WiFi networks according to the security and productivity requirements of your organization as described in *SafeGuard PortProtector User help*.
- **Step 6: Install SafeGuard PortProtector Client on Endpoints**, as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 7: Distribute SafeGuard PortProtector Policies to Endpoints**: in this stage, you can either associate policies to users and computer and distribute directly to endpoints (via SSL), or use Active Directory's GPO feature to distribute SafeGuard PortProtector Policies or any other third-party tool, as described in *SafeGuard PortProtector User help*.
- **Step 8: Endpoints are Protected by SafeGuard PortProtector Policies**: in this stage, only approved devices and WiFi networks can be used, through permitted ports. Logs about port, device and WiFi network use and attempted use, as well as tampering attempts, are created and sent to the Management Server as described in *SafeGuard PortProtector User help*.
- **Step 9: Monitoring Logs and Alerts**, view and export the log entries generated by SafeGuard PortProtector Clients, as described in *SafeGuard PortProtector User help*.