

To protect your valuable information investment from loss—accidental or malicious—your security solution must cover removable storage devices, physical and wireless interfaces, and users. SafeGuard Configuration Protection controls and secures endpoints and devices over every interface, and guarantees flexible and easy-to-use information leakage prevention.

Among its benefits, SafeGuard Configuration Protection monitors real-time traffic and applies customized, granular security policies for all types of interfaces and external storage devices such as:

- Physical interfaces: USB, FireWire, PCMCIA, Parallel, Serial, etc.
- Wireless interfaces: Wi-Fi, Bluetooth, Infrared (IrDA)
- External storage devices: Removable media, CD/DVD, floppy drives, etc.

Administrators will benefit from its ease of use and management capability with features that:

- Detect and allow restrictions of device type, model or even specific serial number
- Enable administrators to block all storage devices completely
- Visualize who is connected to corporate endpoints with SafeGuard PortAuditor tool
- Enforce security policies that meet business needs

SafeGuard Configuration Protection is a module of SafeGuard Enterprise, a centralized solution for managing information protection in mixed IT environments. It is centrally managed by Sophos's powerful SafeGuard Management Center console.

Key benefits

Enhanced security

- » Prevents data leakage and theft, enterprise penetration and introduction of malware
- » Granular control detects and restricts data transfer by device type, device model, unique serial number and file type
- » Protects enterprise data in motion on external storage devices and tracks offline use
- » Blocks both USB and PS/2 hardware keyloggers

Easy to manage

- » Defines separate policies for any domain, group, computer or user
- » Enables easier administration with Microsoft Active Directory® integration
- » Logs are viewed in the management console for easy reporting and auditing, or exported to third-party analysis software

Easy to use

- » Transparent to end user with no change in work productivity

Benefits

Security features: usage control

- Port control
- Device control
- Storage control
- Read-only or read/write control for portable devices
- Granular Wi-Fi control
- Restricts file transfers based on file type
- Blocks hybrid network bridging
- Blocks USB and PS/2 hardware keyloggers

Security

- **Granular control:** detects and restricts data transfers by device type, device model, unique serial number and file type
- **Data protection:** protects corporate data in motion on external storage devices and tracks offline use
- **Secure agent:** silent deployment, redundant, multi-tiered anti-tampering prevents security policy circumvention

Auditing on endpoint security status

- Comprehensive visibility of who is connecting what to corporate endpoints
- Visibility over all USB, PCMCIA, FireWire and Wi-Fi ports
- Granular record of all current and past device connections
- Simple and powerful reporting

Powerful central administration

- Policy flexibility offers ability to define separate policies by domain, group, computer or user
- Integrates with Microsoft Active Directory® and supports Novell environments
- Advanced policy enforcement via independent, kernel-level, real-time analysis of low-level port traffic
- Devices that have not communicated with the management center at specified intervals can be blocked or locked down via policy while online, protecting against loss and theft
- Communication with the SafeGuard Management Center via advanced XML/SOAP protocols
- Secure Wake-On-LAN allows automated administrative activities (e.g., patch management)

Greater productivity and ease of use

- No need for changes to familiar working habits of users
- High level of acceptance by users: no additional training required

Logging and reporting

- All client activities/status and security events are logged and stored locally and centrally
- Types of logs and storage location are user-defined
- Administrators can filter, view, print and export logs and reports with the SafeGuard Management Center console

System requirements

Operating systems (32 bit)¹

- » Microsoft Windows XP (SP 2, SP 3)
- » Microsoft Windows Vista™ (SP 1, 2)

Product requirements

- » SafeGuard Management Center

Certifications

- » Common Criteria EAL 2

Language Versions

- » English, French, German, Hungarian, Italian, Japanese, Spanish
- » Unicode-based support for other local OS languages

Port Control Overview

Physical interfaces

- » USB
- » FireWire
- » PCMCIA
- » Secure Digital (SD)
- » Parallel
- » Serial
- » Modem

Wireless interfaces

- » Wi-Fi
- » Bluetooth
- » Infrared (IrDA)
- » Storage devices
- » Removable storage devices
- » External hard drives
- » CD/DVD drives
- » Floppy drives
- » Tape drives

¹ Successfully tested on Windows 7 Release Candidate. Windows 7 final version will be supported in the next release. 64-bit support will be available in the next release.