

Configuration Protection module

To protect your valuable information 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 data loss prevention.

Enhanced security

- Prevents data loss 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
- Restricts U3 (autorun) feature for removable media
- Prevents security policy circumvention through secure agent: silent deployment, redundant, multi-tiered anti-tampering

Security features: usage control

- Ports: allows/blocks usage
- Devices and storage media: provides whitelisting by type, model and serial number
- Offers read-only or read/write control for portable storage media
- Blocks USB and PS/2 hardware keyloggers
- Files: restricts file transfers based on file type
- Wi-Fi: provides whitelisting by SSID
- Blocks hybrid network bridging

Auditing on endpoint security status

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

Key benefits

Improved system security

- » 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.
- » Controls read/write access based on file type groups

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 what is connected to corporate endpoints with SafeGuard PortAuditor tool
- » Enforce security policies that meet business needs

Greater productivity and ease of use

- » No need for changes to users' familiar working habits
- » High level of acceptance by users: no additional training required
- » Improved system stability by preventing unwanted devices and drivers

Powerful central administration

- Policy flexibility offers the ability to define separate policies by domain, group, computer or user.
- User/computer information is imported via integration with directory services (e.g., Microsoft Active Directory).
- Advanced policy enforcement is enabled 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.
- Advanced XML/SOAP protocols enable communication with SafeGuard Management Center.
- All client activities/status and security events are logged and stored locally and centrally. Log types and storage locations are user-defined. Administrators can filter, view, print and export logs and reports by using the SafeGuard Management Center console*.

Easy, centrally managed installation

- Installation packages can be distributed and installed centrally and unattended via standard MSI packages.
- Network rollout is easy—user involvement is not required.

* SafeGuard Enterprise Management Center module is required for central administration. Please visit www.sophos.com for more information.

System requirements

Operating systems

- » Microsoft Windows 7 (32 and 64 bit)
- » Microsoft Windows Vista (32 bit; SP 1, 2)
- » Microsoft Windows XP (32 bit; SP 2, SP 3)

Product requirements

- » SafeGuard Management Center

Certifications

- » Common Criteria EAL 2

Language versions

- » English, French, German, 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