



Stopping Data Leakage through Endpoints and Removable Media

Preventing your valuable information investment from loss – accidental or malicious – requires that removable storage devices, physical and wireless interfaces, as well as users be covered in your security solution. **SafeGuard Configuration Protection** controls and secures endpoints and devices over every interface and guarantees flexible, 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:** WiFi, 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 or permit read-only access on devices
- Offer ability to monitor, block, and/or log files that are written to, or read from, devices
- 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 Utimaco's powerful SafeGuard Management Center console.

SafeGuard Enterprise – Your Central Key to Information Protection

About Utimaco – The Data Security Company.

Utimaco is a leading global provider of data security solutions, enabling mid-to large-size organizations to safeguard their data assets against intentional or accidental data loss, and to comply with privacy laws. Utimaco's complete range of data security solutions provide full 360 degree data protection for data at rest, data in motion and data in use. Utimaco offers its customers comprehensive on-site support via a world-wide network of certified partners and subsidiaries. Utimaco Safeware AG, with headquarters in Oberursel, near Frankfurt, Germany, is listed on the Frankfurt Stock Exchange (ISIN DE0007572406). For more information please visit www.utimaco.com

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, and unique serial number
- Inspects files and controls the transfer of unauthorized file types to and from external storage devices
- Protects enterprise data in motion on external storage devices and tracks offline use
- Blocks both USB and PS/2 hardware key-loggers

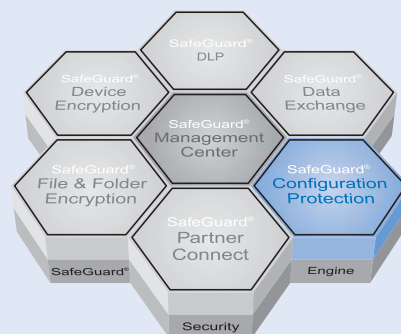
Easy to manage

- Define separate policies for any domain, group, computer or user
- Enable 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

- End-user transparent with no change in work productivity

SafeGuard® Enterprise



SafeGuard Configuration Protection

is a module of **SafeGuard Enterprise** – a centralized solution for managing data security in mixed IT environments.

SafeGuard® Configuration Protection

System Requirements

Operating systems

- Microsoft Windows XP (Service Pack 2, Service Pack 3)
- Microsoft Windows Vista™ (Service Pack 1)

Product Requirements

- SafeGuard Management Center

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
- Internal Ports

Wireless Interfaces

- WiFi
- Bluetooth
- Infrared (IrDA)

Storage Devices

- Removable Storage Devices
- External Hard Drives
- CD/DVD Drives
- Floppy Drives
- Tape Drives

Key Features/Functionality

Security Features – Usage Control

- Port Control
- Device Control
- Storage Control
- Granular WiFi control
- Block Hybrid Network Bridging
- Internal Port control
- Block USB and PS/2 Hardware Key-Loggers

Security

- **Granular control:** detects and restricts data transfers by device type, device model, unique serial number, file type or by content
- **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 WiFi 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 on-line, protecting against loss and theft
- Communication with the SafeGuard Management Center via advanced XML/SOAP protocols
- Secure "Wake on LAN" to allow 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. Type of logs and storage location are user-defined
- Administrators can filter, view, print, and export logs and reports with the SafeGuard Management Center console

Further information

- For more information about Utimaco Safeware and our complete line of SafeGuard solutions, visit www.utimaco.com. To learn more about all of the modules that comprise SafeGuard Enterprise, visit www.utimaco.com/sgn

Utimaco Safeware Partner:



Copyright Information

© 2007-2008 – Utimaco Safeware AG

SafeGuard® Configuration Protection version 5.35

All SafeGuard products are registered trademarks of Utimaco Safeware AG. All other named trademarks are trademarks of the particular copyright holder. Individual functions may have different characteristics according to the different capabilities of the operating systems.

www.utimaco.com



EMEA
Utimaco Safeware AG
Hohemarkstrasse 22
DE-61440 Oberursel
Germany
Phone +49 (61 71) 88-14 44
info@utimaco.com

NORTH & SOUTH AMERICA
Utimaco Safeware Inc.
10 Lincoln Road
Foxboro, MA 02035
USA
Phone +1 (508) 543-10 08
sales.us@utimaco.com

ASIA PACIFIC
Utimaco Safeware Asia Ltd.
Unit 602, Stanhope House
734 King's Road, Quarry
Bay
Hong Kong
Phone +852 25 20 26 08
info@utimaco-asia.com

JAPAN
Utimaco Safeware K.K.
Nisso 16 Building, 3F
3-8-8 Shin Yokohama, Kohoku-ku
Yokohama 222-0033
Japan
Phone +81 (0) 45 470-1430
info.jp@utimaco.jp