



Centralized management enforces consistent policies, enables compliance, and eases administrative burden

Effective security and regulation compliance requires centralized management to configure and consistently implement policies, especially in mixed IT environments. Administrators need to continually modify policies to meet ever changing requirements while at the same time ensuring security is transparent. **SafeGuard Management Center** console lowers training costs and eases administrative tasks.

SafeGuard Management Center is a functional module of **SafeGuard Enterprise**, a centralized solution for managing data security in mixed IT environments. **SafeGuard Management Center** is the central administration platform and works in conjunction with other SafeGuard Enterprise functional modules to provide complete security and management control over all connected devices and users. It enables the management of full data encryption and data leakage prevention (DLP) from a single console for powerful multi-layered security.

Central management features include:

- Centralized security policies enforce consistent rules for encryption, authentication, user privileges, or for individuals and groups, on a variety of different devices in mixed IT environments.
- Easy to manage and distribute security policies to users' end-point devices quickly and conveniently. Easily import users, groups, devices, and organizational units already set-up in Microsoft Active Directory.
- Centralized key management in mixed environments allows users and administrators to easily share and recover data across groups and devices.
- Audit logs and reports guarantee compliance with internal policies and external regulations.
- Data/password recovery is compatible with standard forensic and recovery tools, minimizing helpdesk burden.

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

Centrally manage encryption and data leakage prevention (DLP) policies

- Manage data encryption and data leakage prevention from a single console
- Administer users and devices in mixed IT environments consistently
- Role-based user management enables granular policy enforcement
- Detailed, printable audit logs and reports for regulatory compliance
- Recover passwords and data easily
- Encrypt and manage desktops, laptops, and removable media

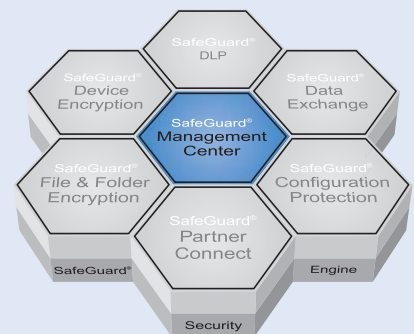
State-of-the-art key management

- Centralized key management from a single console
- Secure storage, exchange, and recovery of keys in mixed device and operating system environments
- Share data between PCs, removable media, PDAs, or e-mail attachments

Modular and flexible security architecture

- Grows with your needs with additional SafeGuard Enterprise modules
- Feature-rich management API for custom applications
- Supports Windows Vista™ BitLocker™ Drive Encryption
- Integration with Microsoft Active Directory®, directory service via LDAP. Supports Novell environments
- Compatible with 3rd party Smartcards, tokens
- XML/SOAP-based communication: No firewall reconfigurations, supports traffic load-balancing

SafeGuard® Enterprise



SafeGuard Management Center

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

SafeGuard® Management Center

System Requirements

Operating systems

- Microsoft Windows XP (Service Pack 2, Service Pack 3)
- Microsoft Windows Vista™ (Service Pack 1)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008 (32-bit)

Certifications

- FIPS 140-2
- Aladdin eToken enabled



Standards and Protocols

- Symmetrical encryption: AES 128/256 bit
- Asymmetrical encryption: RSA
- Hash functions: SHA-256, SHA-512
- Passwords, padding, PKCS #1, PKCS #5v2
- Smartcard / token: PKCS #11, PKCS #15, Microsoft CSP, PC / SC, Kerberos
- PKI: PKCS #7, PKCS #12, LDAP, X.509 certificates
- Data transfer: SOAP, XML, SSL

Language versions

- English, French, German, Japanese

Supported databases

- Microsoft SQL Server 2000, 2005, Express
- Encrypted communication between database and management centers

SafeGuard Management API supports

- Directory operations, automatic sync
- User-to-device assignment
- Key assignment to devices / users
- Logs, inventory and report processing
- Certificate and token management
- Challenge/response for custom helpdesk applications

Real-time status, logs & security reports

- All client activities/status, administrator actions and security events are logged and centrally stored. Type of logs and storage location are user-defined
- Administrators can filter, view and print log reports
- Optional standalone "SGNState" tool reports encryption status to external consoles (e.g., LANDesk or Network Access Control solutions)

XML/SOAP client-server communication

- Secure communication via XML/SOAP-based Web services. Benefits include load balancing of services in large environments. No changes to firewall settings

License management

- Administrators can activate new SafeGuard modules by simply updating the license
- Administrators can track usage of SafeGuard Enterprise modules for licence compliance

Key Features/Functionality

Centralized administration of security policies

- Centralized, multi-platform security administration with hierarchical definition of security policies
- Modular policy inheritance mechanisms allow utmost flexibility and efficiency in management
- Resulting Set of Policies (RSOP): the final inherited policy is calculated for every user or computer
- Automatic distribution of security policies across platforms
- Rules assigned to organizational units (OUs) and activated for user/computer groups
- Devices that fail to contact the server in a predefined time interval, or within a set number of login attempts, can be blocked. Unblocking is done via challenge/response.

Administration of security officers

- Role-based access. Predefined and custom security officer roles
- Dual-officer authorization for critical actions
- Optional two-factor authentication via tokens or smartcards
- SafeGuard security officers selectable from Active Directory
- Management console is multi-session-capable

Full Management of Windows Vista™ BitLocker™ Drive Encryption

- Consistent security policies are enforceable in mixed OS and device environments
- Centrally manage keys for backup and recovery
- BitLocker™ Drive Encryption selectable as an option
- SafeGuard Enterprise reports on BitLocker device status

Directory services support

- Infrastructure data (users, computers, groups, X.509 certificates, etc.) can be imported from LDAP directories
- Microsoft Active Directory support:
 - SafeGuard Enterprise specific user accounts not required
 - SafeGuard Enterprise security officers selectable from Active Directory users
- Supports Novell environments

Automated installation

- Supports standard software distribution mechanisms via MSI packages – distributed and installed automatically using existing software management systems (e.g., Altiris, Microsoft SMS, NetInstall)
- Default configuration settings enable quick implementation in test environments

Help desk options

- Integrated challenge/response recovery wizard for forgotten user passwords
- Web-based helpdesk for outsourced environments
- Web self help for end-users to reset passwords without contacting the help desk
- API for custom help desk integration

SafeGuard Enterprise system health monitoring

- SafeGuard Enterprise Management Pack for Microsoft System Center Operations Manager 2007 (optional add-on) monitors the health status of the SafeGuard management servers and database

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

© 2006-2008 – Utimaco Safeware AG
SafeGuard® Management Center 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.



a member of the Sophos Group

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