

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 ensuring that security is transparent. SafeGuard Management Center 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, individuals and groups on a variety of different devices in mixed IT environments.
- It is easy to manage and distribute security policies to users' endpoint devices quickly and conveniently. You can easily import users, groups, devices and organizational units that are 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 help desk burden.

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
- Access 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

Key benefits

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
- » Multi-tenancy support (managing multiple separate SafeGuard installations from one console)

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 third-party smartcards and tokens
- XML/SOAP-based communication: no firewall reconfigurations, supports traffic load balancing

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

¹Successfully 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.

Help desk options

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

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 help desk applications

Real-Time Status, Logs and Security Reports

- All client activities/status, administrator actions and security events are logged and centrally stored
- Types 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 [NAC] solutions)

System requirements**Operating systems (32 bit)¹**

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

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

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 by Administrators

- » Activate new SafeGuard modules by simply updating the license
- » Track usage of SafeGuard Enterprise modules for license compliance
- » Types of logs and storage location are user-defined SOAP-based web services

Supported Databases

- » Microsoft SQL Server 2005, 2008, Express
- » Encrypted communication between database and management centers

For full details, visit www.sophos.com