

Management Center module

Effective data security and regulatory compliance requires centralized management to configure and consistently implement policies, especially in mixed IT environments. Administrators need to continually modify security 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 module of SafeGuard Enterprise, a centralized solution for managing data security in mixed IT environments. SafeGuard Enterprise provides full disk encryption, removable media encryption, PC port control for data loss prevention (DLP) and management of other encryption products, all from a single console, for powerful multi-layered security.

Centralized administration of data security policies

- Centralized, multi-platform security administration features hierarchical definition of security policies—for full disk encryption, removable media encryption and port control DLP—from a single console.
- Integration with Active Directory takes advantage of user, device and group information, but does not mandate it.
- Modular policy inheritance mechanisms allow the utmost flexibility and efficiency in management.
- Resulting Set of Policies (RSOP): The final inherited policy is calculated for every user or computer and is easily verifiable by console administrators.
- Security policies are automatically distributed across platforms.
- Rules are assigned to organizational units (OUs) and activated for user/computer groups, such as for Active Directory; easy to understand for administrators and very flexible to match even special use cases.
- 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.

State-of-the-art key management

- Key management is centralized from a single console.
- Keys are securely stored, exchanged and recovered in mixed device and operating system environments.
- Automatic key assignments for groups enable group-based encryption and sharing.
- Securely share data between PCs, removable media and email attachments.

Administration of security officers

- Role-based access: Predefined and custom security officer roles are available.
- Dual-officer authorization for critical actions is provided.
- Two-factor authentication via tokens or smartcards is optional.
- Security officers are selectable from Active Directory.
- Security officers can be hierarchically grouped, allowing group-based policy inheritance and assignments.
- Administrative rights can be delegated.
- Management console is multi-session-capable.
- Multi-tenancy support: Manage multiple separate SafeGuard installations from one console.

Key benefits

- » Lower administrative costs by centrally managing mobile data encryption and port control (DLP) policies from a single console.
- » Administer users and devices in mixed IT environments consistently while enforcing compliance policies.
- » Role-based user management enables granular policy enforcement, improving IT efficiency.
- » Access detailed, printable audit logs and reports for regulatory compliance.
- » Recover passwords and data easily for secure productivity, while lowering help desk costs.
- » Provide comprehensive security by encrypting and managing desktops, laptops and removable media.

Modular and flexible security architecture

- Additional SafeGuard Enterprise modules enable the solution to grow with your needs.
- Feature-rich management API is provided for custom applications.
- The solution integrates with Microsoft Active Directory via LDAP and supports Novell environments.
- Third-party smartcards and tokens are compatible.
- Secure XML/SOAP-based client-server communication is provided; no firewall reconfigurations, supports traffic load balancing.

Management of BitLocker Drive Encryption in Windows 7 and Vista

- Consistent security policies are enforceable in mixed OS and device environments.
- Keys can be centrally managed with secure backup and recovery.
- BitLocker Drive Encryption is 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 capable Microsoft Active Directory directories without mandating it.
- SafeGuard Enterprise specific user accounts are not required.
- SafeGuard Enterprise security officers are selectable from Active Directory users.
- Novell environments are supported.

License management by administrators

- Activate new SafeGuard modules by simply updating the license.
- Track usage of SafeGuard Enterprise modules for license compliance.

Automated installation

- Standard software distribution mechanisms via MSI packages are supported—distributed and installed automatically using existing software management systems (e.g., Altiris, Microsoft SCCM, NetInstall).
- Default configuration settings enable quick implementation in test environments.
- A server installation wizard simplifies installation of both SafeGuard and Microsoft server components.

Password recovery and help desk options

- An integrated challenge/response recovery wizard assists with forgotten user passwords.
- A web-based help desk for outsourced environments is included with the Management Center license.
- An API is available for custom help desk integration.
- A local self-help option to recover forgotten passwords eliminates the need to call the help desk. Local self-help options and challenge questions/answers are configurable via the Management Center.

SafeGuard Management API supports:

- Directory operations, automatic sync
- User-to-device assignment
- Key assignment to devices/users
- Log, 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 to assist in compliance audits.
- Types of logs and storage locations are user-defined.
- Administrators can filter, view and print log reports.
- An optional standalone SGNState tool reports encryption status to external consoles (e.g., LANDesk or network access control [NAC] solutions).

System requirements

Operating systems

- » Microsoft Windows 7 (32 and 64 bit)
- » Microsoft Windows Vista (32 and 64 bit; SP 1/2)
- » Microsoft Windows XP (32 bit; SP 2, SP 3)
- » Microsoft Windows Server 2008 and 2008 R2 (32 and 64 bit)
- » Microsoft Windows Server 2003 (32 bit)

Certifications

- » Uses FIPS 140-2 validated SafeGuard Cryptographic Engine
- » Aladdin eToken enabled

Standards and protocols

- » Symmetrical encryption: AES 128/256 bit
- » Asymmetrical encryption: RSA
- » Hash functions: SHA-256, SHA-512
- » Password hashing: 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 2005, 2008, Express
- » Encrypted communication between database and management centers