SOPHOS

simple + secure

SafeGuard Enterprise
Manual for certification-compliant operation

Product version: 5.60
Document date: November 2011

Content

1 Preface 2

2 Certification of SafeGuard Enterprise Device Encryption 3

3 Secure operation of SafeGuard Enterprise Device Encryption 7

4 Technical Support 18

5 Legal notices 19

1 Preface

This document is a supplement for the SafeGuard Enterprise user help and the SafeGuard Enterprise administrator help.

It especially addresses those users who intend to use SafeGuard Enterprise Device Encryption as a certified security software product.

References

- SafeGuard Enterprise user help, Sophos Group, 2011
- SafeGuard Enterprise administrator help, Sophos Group, 2011
- SafeGuard Enterprise installation manual, Sophos Group, 2011

2 Certification of SafeGuard Enterprise Device Encryption

SafeGuard Enterprise Device Encryption Version 5.30, and SafeGuard Enterprise Device Encryption Version 5.60 have passed a certification process according to Common Criteria (CC), version 2.3.

The Common Criteria provide a standard criteria catalog for the security evaluation of products and systems for information technology. The Common Criteria have been commonly prepared by governmental organizations of Australia/New Zealand, Canada, France, Germany, Japan, the Netherlands, Spain, the United Kingdom and the USA and are accepted as an international standard.

The certifications have been performed by the German BSI ("Bundesamt für Sicherheit in der Informationstechnik") as a certification body.

The Evaluation Assurance Level of SafeGuard Enterprise Device Encryption 5.60 is "EAL4", the level for SafeGuard Enterprise Device Encryption 5.30 is "EAL3+". The specified minimum strength of the security functions of SafeGuard Enterprise Device Encryption, Versions 5.30 and 5.60, is "SOF-medium".

2.1 Evaluation Assurance Level

In the scope of the Common Criteria, the Evaluation Assurance Level (EAL) specifies the accuracy and the effort used to analyze and verify the correct implementation of the security functions of a certified product.

The Common Criteria specify seven different Evaluation Assurance Levels. Level "EAL1" defines the lowest, "EAL7" the highest Evaluation Assurance Level.

Depending on the EAL, different objectives and specified security criteria have to be fulfilled and verified. For level "EAL3+", this comprises providing a Security Target document including an analysis of the security functional requirements, a functional and interface specification and an informal architecture description (High Level Design) of the product to be evaluated. Furthermore, independent testing of the security functionality, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results and a vulnerability analysis demonstrating resistance to penetration attackers with a standard attack potential are required. User and administrator guidance must comply with specified requirements. Additionally, an automated configuration control system supporting development, appropriate measures for securing the development environment as well as an approved distribution method have to be applied.

"EAL4" adds the requirement for closer inspection of the low-level design and source code as well as a more detailed vulnerability assessment based on this additional information.

2.2 Information concerning the Common Criteria

The Common Criteria originate from separate IT security criteria catalogs published by national authorities for the evaluation of IT security products and systems.

The following countries take part in the definition of the Common Criteria: Australia/New Zealand, Canada, France, Germany, Japan, the Netherlands, Spain, the United Kingdom and the United States of America. The Common Criteria are based on the following single criteria catalogs: CTCPEC (Canada), FC, TCSEC (both USA) and ITSEC (Europe).

The Common Criteria ensure comparable evaluations of IT security products and systems in all these countries. An automatic mutual approval of granted certificates was established in May 2000.

The Common Criteria were issued on an international level by ISO/IEC JTC 1/SC 27/WG 3 and as an international standard titled ISO/IEC 15408 "Evaluation Criteria for Information Technology Security" in December 1998.

2.3 Information concerning the certification process

The following parties are involved in the certification process according to the Common Criteria: the certification body, an evaluation facility and the producer or the distributor of the product.

The certification body for SafeGuard Enterprise Device Encryption is the BSI ("Bundesamt für Sicherheit in der Informationstechnik"), Bonn, Germany. The evaluation facility is SRC GmbH, Bonn, Germany.

The certification process is initiated on the request of the producer or distributor. The main part of the process is the technical assessment (evaluation) of the product according to the criteria catalog. Technical assessment is performed by an evaluation facility licensed by the certification body. Afterwards, the certificate is issued by the certification body on the basis of an Evaluation Technical Report (ETR) prepared by the evaluation facility.

Details of the certificate, for example the threats averted by the product, the scope of the certified security functions and possible requirements for the operation as a certified product, are published by the certification body in the certification report. The certification report and the Security Target document are made available to the public.

2.4 Scope of the certified product

The scope of evaluated parts of SafeGuard Enterprise Device Encryption consists of:

1. the installable program code of the Device Encryption client for SafeGuard Enterprise Version 5.60, English program version. The program code is a part of SafeGuard Enterprise, delivered on the SafeGuard Enterprise product CD-ROM and identified as "[SafeGuard® Enterprise 5.60.0.192 - Application for Windows XP / Vista / Windows 7]".
2. the guidance documentation consisting of:
   a) SafeGuard Enterprise User help
   b) SafeGuard Enterprise Administrator help
   c) SafeGuard Enterprise Installation manual
   d) SafeGuard Enterprise User and administrator help supplement: Manual for certification-compliant operation

Note: Only the device encryption client component of SafeGuard Enterprise is part of the certification. All other SafeGuard Enterprise modules - SafeGuard Enterprise Server, SafeGuard Management Center, SafeGuard Data Exchange, SafeGuard File & Folder Encryption, SafeGuard Configuration Protection and SafeGuard Partner Connect - are not part of the certification.

2.5 Scope of certified security functions

The following security features of SafeGuard Enterprise Device Encryption have been certified:

Power-on Authentication (POA):

Provides secure identification and authentication of authorized users by user name and password or by using a CryptoToken and the appropriate PIN.

Protection of data on protected devices (using device encryption):

User data on protected devices, which are under control of SafeGuard Enterprise Device Encryption, is protected against disclosure and intentional modification. This is achieved by encrypting the data on the maintained protected devices. The symmetrical encryption algorithms used comply with standards AES-128 (CBC mode) and AES-256 (CBC mode).

Secure server-based administration:

SafeGuard Enterprise Device Encryption is administrated via SafeGuard Enterprise Server and SafeGuard Enterprise Management Center. Administration data is securely transmitted between the client PC - with SafeGuard Enterprise Device Encryption installed - and the SafeGuard Enterprise Server.

Note: Please note that the functionality of SafeGuard Enterprise Server and SafeGuard Management Center is not within the scope of the evaluation.

Key generation:

Secure keys for cryptographic algorithms are generated by a built-in key generator.

3 Secure operation of SafeGuard Enterprise Device Encryption

3.1 System requirements

The certification of SafeGuard Enterprise Device Encryption is restricted to the operation of the client under one of the following operating systems:

- Microsoft Windows XP (32 bit) Service Pack 3
- Microsoft Windows 7 (32 bit and 64 bit)

3.2 Product identification

The product can be identified by the product name and version number printed on the CD media. The installation files (.msi) of the product are digitally signed with a VeriSign class 3 Code Signing Certificate. This certificate shall be checked prior to installation to verify the origin, integrity and authenticity of the received product material. In addition, the essential installation files can be verified using hashes as described in detail in the security target.

3.3 Measures for secure operation

To operate SafeGuard Enterprise Device Encryption in a certified configuration and to guarantee the highest available security, the following administrative and operational measures have to be taken.

3.3.1 Deployment measures: Administrator responsibilities

The administrative measures are to be considered during installation of SafeGuard Enterprise Device Encryption and as long as it is installed.

3.3.1.1 Operating environment

Installation and configuration

SafeGuard Enterprise Device Encryption shall be properly installed. Details concerning secure installation are as follows:

- Installation according to user and administrator guidance
- Providing a working network connection between SafeGuard Enterprise Device Encryption client and SafeGuard Enterprise Server after installation

- Setting secure attributes in administration and configuration data: A proper set of policies according to section *Configuring essential policies* on page 12 must be defined.
- Correct preparation of the client with the client configuration package (as described in the user guidance)

Note: In the **Properties** dialog of this MSI file, Windows will warn about the digital signature being invalid. This is expected, as the MSI template that was signed and shipped is modified by the Management Center by adding the actual configuration files. They are however protected by a signature issued by the Management Center in the process. If they are manipulated, they can be unpacked on the client, but the client will not accept them.

- Under Windows 7 the SafeGuard Enterprise Credential Provider has to be used. The usage of other credential providers and the SafeGuard Enterprise authentication application are not covered by the certification.

Client-Server connection

The data connection between SafeGuard Enterprise Device Encryption and SafeGuard Enterprise Server has to be secured by a Secure Socket Layer (SSL) connection fulfilling the following requirements:

- Usage of Secure Socket Layer v3 or higher or Transport Layer Security (TLS)
- The used implementation of SSL/TLS has to be trustworthy and has to be kept up-to-date. In particular, it has to be ensured that all relevant patches are installed.
- Usage of strong cryptographic algorithms
  Guidelines for the choice of algorithms and key lengths are published on a regular basis by the German Federal Network Agency (Bundesnetzagentur) at *www.bundesnetzagentur.de*[1] or the US National Institute of Standards and Technology (NIST) at *http://csrc.nist.gov*[2]. Similar guidelines are published by the respective information security agencies of many other countries.

Note: Encryption and integrity protection of all transmitted data as well as server authentication are mandatory in SSL/TLS and cannot be turned off if properly configured.

1.See *http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Algorithmen_sw.html* for lists of approved algorithms and key sizes (in German).

2.The Implementaion Guidance for FIPS Pub 140-2 and the Cryptographic Module Validation Program, which is jointly published by the US National Institute of Standards and Technology (NIST) and Canadian Communications Security establishment (CSE), provides a good overview on the algorithm requirements for North American countries.

Opal-compliant, self-encrypting hard drives

SafeGuard Enterprise also supports management of Opal-compliant, self-encrypting drives. These can be managed together with the standard encryption clients from the same console. The same client is used to manage both. Since Opal drives are not included in this evaluation however, the clients must be installed to skip Opal support even if an Opal drive is detected. This can be done by setting the MSI property OPALMODE=2. One way to do that is to install with a command line like

```
msiexec /i <client package> OPALMODE=2
```

This makes sure that the Opal mode is not used even if the drive supports it. Instead, the certified software encryption will be used on every client.

BitLocker Drive Encryption

SafeGuard Enterprise also supports environments comprising SafeGuard Enterprise Device Encryption clients and BitLocker Drive Encryption clients. All these clients can be administered centrally using SafeGuard Management Center. Only SafeGuard Enterprise Device Encryption has been evaluated and certified. Thus, to operate a client in a certification-compliant mode, only SafeGuard Enterprise Device Encryption shall be used. Make sure that the BitLocker feature is not selected when you install the client MSI.

Avoiding network shares

No partitions/drives/volumes, directories or files on the local hard disk of the PC secured by SafeGuard Enterprise Device Encryption shall be shared with other users, when the PC is connected to a network. This is to avoid installing untrusted software onto the secured PC by using those network shares.

Preventing password disclosure

The client PC on which SafeGuard Enterprise Device Encryption is installed and the environment in which the PC is operated by any authorized user has to be secured against devices capable of recording the password entered by an authorized user. Such devices may be keyboard grabbers placed between keyboard and PC, which are able to record keystrokes, as well as video cameras capturing the user during password entry.

Token or smartcard policy

If tokens or smartcards are used for authentication, they shall have certain properties. The token or smartcard shall

- implement a secure key storage space for the user's private key in hardware using a secure firmware (card operating system). The firmware shall require a successful PIN authentication before any operation with the private key can be performed. In addition, it shall not allow the private key to be read regardless of a successful PIN authentication.
- enter a blocked state after a maximum of 5 failed PIN entry attempts, preventing any further PIN entry or attempts of data access.
- support on-chip RSA operations with a key length of at least 2048 bits.

If the key pair is generated on the token or imported from outside the TOE (for example from a PKI), the operator shall verify that the keys are generated using at least a class K3 RNG as defined in AIS 20.[1]

Password policy

When password-based authentication is used, it has to be assured that the used passwords are of a certain quality that ensures that passwords can neither be guessed nor determined using a dictionary attack. An adequate password policy shall be defined that can be enforced using SafeGuard Management Center.

Running the administration server

All components of the administration server, which maintains the client PC with SafeGuard Enterprise Device Encryption installed, shall run in a secure environment where only authorized persons have access.

Persons authorized to maintain the SafeGuard Enterprise configuration via the administration server and the SafeGuard Management Center are considered reliable and are expected not to bypass security functions intentionally.

Removal of rights

In some cases, a user's right to access a specific encrypted device may be removed. This may for example be the case, when an employee moves to a different position within the company or leaves the company. In this case, the User-Machine-Assignment (UMA) has to be changed to ensure that the user cannot access this specific device. Furthermore, a complete re-encryption of the respective device shall be performed.

1. Application Notes and Interpretation of the Scheme (AIS) 20, Functionality classes and evaluation methodology for deterministic random number generators, Version 1, Bundesamt für Sicherheit in der Informationstechnik, 2 December 1999

ReadyBoost

ReadyBoost is a system feature of the Microsoft Windows 7 operating system that uses flash storage as disk cache to speed up hard disk access times.

ReadyBoost was not tested during the evaluation and shall not be used in certification-compliant operation.

Secure Wake on LAN (WOL)

The Secure Wake on LAN functionality shall be deactivated for all clients. This is to ensure that the Power-on Authentication (POA) is active at all times.

3.3.1.2 Configuring essential policies

To deploy the SafeGuard Enterprise Client in certification-compliant operation mode, at least the following policies must be defined. If necessary, they can be exported to the configuration package as an initial set of policies.

Policy setting	Required value
Activate logon recovery after Windows local cache corruption	**Yes**, as the corruption could be due to tampering and this setting ensures the administrator is notified of any issue.
Enable Local Self Help	**No**, as this amounts to an alternative logon method that has not been evaluated.
User may only boot from internal hard disk	**Yes**
Logon mode	**User ID/Password** or **Token**, depending on your setup.
Lock screen after X minutes inactivity	**5** minutes
PIN rules	No specific recommendation possible as permissible PINs depend on token/smartcard capabilities.
Min. password length	**10**
Min. number of letters/digits/special characters	**1** for each
Case sensitive	**Yes**, this and the previous three settings maximize the key space for the password.
Keyboard row/column, 3 or more consecutive characters, user name as password forbidden	**Yes**
Password expires after (days)	**60**
Media encryption mode	**Volume-based** for each drive (**file-based** for removable drives where the former is not supported)
Algorithm to be used for encryption	**AES-256**
Key to be used	Depends on the level of user management in the administrative setup. To ensure the user does not need to choose keys, select **Defined key on list** or **Defined machine key**. The latter key is guaranteed to be available to any authorized user.

Policy setting	Required value
Reaction to unencrypted volumes	**Accept all media and encrypt**
User may add or remove keys to or from encrypted volume	**Must be set to No.**
Fast initial encryption	**No**, unless you are absolutely sure the drive has never held any sensitive data before.
Initial encryption of all files	**Yes**
Enable Power-On Authentication	**Yes**
Secure Wake on LAN (WOL)	Disabled
Uninstallation allowed	**No**

3.3.2 Deployment measures: User responsibilities

Lenovo Rescue and Recovery™ (RnR)

Lenovo Rescue and Recovery™ was not tested during the evaluation and shall not be used in certification-compliant operation.

Authentication at Microsoft Windows 7

Logon to Microsoft Windows 7 using a combination of non-SafeGuard Enterprise credential providers and the SafeGuard Enterprise Authentication Application was not tested during the evaluation and shall not be used in certification-compliant operation.

3.3.3 Measures during operation: Administrator responsibilities

The operational measures have to be taken as long as SafeGuard Enterprise Device Encryption is installed on a client PC.

Administration server connection

To update security rules, administration and configuration data, the client PC is to be connected to the administration server in regular intervals.

Preventing usage of incompatible software

Software which does not use the respective Application Programming Interface of the OS platform for disk access must not be placed on the client PC's storage device or executed while the computer is operated.

SafeGuard Enterprise Device Encryption works in combination with all application software released for the mentioned operating system platforms. However, application software which is not using the respective Application Programming Interface of the OS platform for disk access, but circumventing some layers of the disk access system, may read encrypted data from storage devices and therefore may not recognize the file structure correctly. Such software may also write plain text data directly onto a protected device. This data is then not protected against unauthorized disclosure by SafeGuard Enterprise Device Encryption.

Incompatibilities of this kind are only known for certain virus scanners and backup programs.

Mixed encryption states

All local hard disk partitions shall be encrypted. This ensures that all temporary files, swap files as well as files in the recycle bin or in personal folders like "My Documents" are always encrypted and reduces the possibility of faulty operation by the user.

3.3.4 Measures during operation: User responsibilities

Keeping passwords confidential

Users must keep their password secret. Passwords should not be written down, neither manually nor electronically, to prevent unauthorized persons from obtaining a valid password.

Mixed encryption states

If systems use both encrypted and unencrypted devices or partitions at the same time, it is the user’s responsibility to ensure that sensitive data is only written to encrypted devices.

Adequate user behavior

Authorised users shall neither actively nor negligently compromise the security of the computer on which the TOE is installed.

In particular, they shall not

- place malicious software (like programs containing viruses or Trojan horses) on the computer,
- modify the TOE program or data files,
- modify the hard disk with tools circumventing the TOE transparent encryption interface or
- leave a computer secured by the TOE unattended while being in operational state.
- if they use tokens or smartcards for authentication, leave them with their computers when they are not in the same room. Users should take tokens or smartcards with them or store them in a secure place separate from the computer when not in use.

3.3.5 Secure states

Systems protected by SafeGuard Enterprise Device Encryption are considered to be in a secure state, if the system is in power-off or in hibernation mode. SafeGuard Enterprise Device Encryption does not protect running systems. In this context, systems in stand-by mode or systems with locked screens are considered running systems. Running systems should be protected by additional security controls.

Volumes that are not fully encrypted are considered not to be in a secure state. This may be the case during the initial volume encryption as part of the installation process or during the decryption of volumes as part of the uninstallation process. Initial encryption and decryption can be suspended by shutting down or hibernating a system. The encryption respectively decryption process will automatically restart on system restart.

Even systems in power-off or hibernation state with partly encrypted volumes are not considered to be in a secure state. This is the case only if the encryption process has been finished completely. We therefore recommend not to interrupt the initial encryption process and the decryption process prior to uninstallation to avoid situations where the TOE is active, but certain volumes are not fully encrypted.

It is essential that a computer secured by the TOE ist not left under temporary physical access of an attacker. If it is suspected that unauthorized users had access to a running system or if it is suspected that unauthorized users have tampered with a system in power-off or hibernation mode, the system should be considered compromised. These systems should be inspected thoroughly prior to further use.

3.3.6 Uninstalling the SafeGuard Enterprise Client

3.3.6.1 Prerequisites

- Uninstalling the SafeGuard Enterprise Client must be permitted on the client computer. Permission for uninstallation is granted via policies. In the SafeGuard Enterprise default setting, uninstallation is allowed.
- If uninstallation is not permitted as per a policy assigned, a new policy, which explicitly allows uninstallation, has to be created in the SafeGuard Management Center.
  - Ensure that the policy becomes effective on the client prior to starting the uninstallation process.
- Encrypted data (with the exception of the boot volumes) has to be decrypted prior to starting the uninstallation process.
  If data is not decrypted prior to uninstallation, it remains encrypted. In this case, the data can no longer be accessed on this client.

3.3.6.2 Encrypted data

To be able to access data encrypted by SafeGuard Enterprise after uninstallation, the data has to be decrypted prior to uninstallation.

Volume based encryption

- A volume based encrypted boot volume will be decrypted automatically during the uninstallation process.
- Any other volume based encrypted volumes will not be decrypted automatically.
  If the user is allowed to decrypt the volume, they can decrypt the volume manually, or the decryption process can be initiated by a policy.
- If the user is not allowed to decrypt the volume, the decryption process **must** be initiated by a suitable policy.
  The policy must be created in the SafeGuard Management Center and has to be transferred to the client. As soon as the policy becomes effective on the client, the encrypted volumes are decrypted automatically.

Note: If besides the boot volume any additional volume based encrypted volumes are detected during the uninstallation process, a message will be displayed. The message states that the volumes concerned will not be decrypted during uninstallation. You can cancel the uninstallation process at this point.
If you continue, the volumes remain encrypted.

3.3.6.3 Uninstallation on the client computer

If the prerequisites described are fulfilled, you can start the uninstallation process on the client computer by selecting **Start** > **Programs** > **Control Panel** > **Add or Remove Programs** > **SafeGuard Enterprise Client** > **Remove**.

3.3.6.4 Uninstallation via software distribution mechanisms

If uninstallation is to be performed via software distribution mechanisms, you have to ensure that all required data has been decrypted prior to uninstallation.

Note: You cannot perform an uninstallation process while a decryption process is running.

3.3.6.5 Best practice

1. Create a policy in the SafeGuard Management Center which

- allows uninstallation.
- decrypts all volume and file based encrypted data.

2. Distribute the policy to the clients concerned.

Note: Start the uninstallation only after you have made sure that the policy has become effective on the clients and that the data has been decrypted.

3. Initiate uninstallation via software distribution mechanisms.

4 Technical Support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk forum at http://community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at http://www.sophos.com/support/
- Download the product documentation at http://www.sophos.com/support/docs/
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

5 Legal notices