DECEMBER 2013

Sophos SafeGuard Device Encryption

Product Description

1. SafeGuard Enterprise - Device Encryption is the disk encryption module of Safeguard Enterprise. It provides cryptographic confidentiality, authentication, and access control to both in-built and removable magnetic and solid state data storage devices. This includes hard disks, SSD media, and USB Mass Storage Devices. Device Encryption can be run either in stand-alone mode, or be centrally managed by the SafeGuard Enterprise – Management Centre module.
2. ASD has examined and certified for use the following product versions:
   a. SafeGuard Enterprise 5.6 - Device Encryption for Microsoft Windows XP Professional and Microsoft Windows 7, with management allowed by the Management Centre module.
   b. SafeGuard Enterprise 6.0 - Device Encryption for Microsoft Windows XP Professional and Microsoft Windows 7, with management allowed by the Management Centre module.

Evaluation Scope

3. The scope of the ASD Cryptographic Evaluation (ACE) included the SafeGuard Enterprise - Device Encryption module, and the SafeGuard Enterprise – Management Centre's role in managing the Device Encryption module.
4. The following functionality was investigated:
   a. Key generation and management on the Management Centre server.
   b. Key generation and management on Device Encryption clients.
   c. Data transit between the Management Centre server and Device Encryption clients.
   d. Encryption of user data.
   e. Access control of user data.
   f. Password/key recovery.
   g. User authentication methods.

Common Criteria Certification - Summary

5. At the time of this Consumer Guide's publication:
   a. SafeGuard Enterprise 5.6 - Device Encryption has completed a Common Criteria (CC) evaluation at the EAL 4 level.
   b. SafeGuard Enterprise 6.0 - Device Encryption is undergoing but has not completed a CC evaluation. ASD advises this product may still be used in accordance with this Consumer Guide.

ASD Findings and Recommendations

6. SafeGuard Enterprise - Device Encryption was found to be suitable for reducing the storage and physical transfer requirements of magnetic or solid state storage devices containing PROTECTED information to UNCLASSIFIED in accordance with the Cryptography section of the Information Security Manual (ISM).
7. Device Encryption does not support encryption of optical media.
8. Administrators must use the 'volume based' media encryption mode when creating encryption policies.
9. Any communications between the Device Encryption client and Management Centre server are considered PROTECTED information and must be handled accordingly as per the ISM.
10. Where the Management Centre used, all associated network infrastructure must be accredited for PROTECTED.
11. The storage device on which Device Encryption is to be installed must not have contained classified information prior to the installation of Device Encryption.
12. Passphrases for user accounts must have a minimum length of 12 characters. Passphrases must include at least one character from each of: lower case, upper case, numbers and special characters.
13. Usernames and passphrases must be used for user authentication. Other authentication methods such as tokens, Smart Tokens or fingerprint scanners must not be used.
14. Administrators must disable and not use the Local Self Help password recovery mechanism.
15. If the Challenge/Response password recovery mechanism is used, the Challenge and Response codes are considered PROTECTED information. Agencies must handle the transmission of the Challenge and Response codes as per the Cryptography chapter of the ISM.
    a. If an adversary gains access to the Challenge and Response codes for a user's password reset, the user's account must be considered compromised.
    b. Challenge/Response method is especially vulnerable to targeted Social Engineering attacks due to the reliance on out-of-band authentication.
    c. Agencies are referred to the Resetting Passphrases section of the Access Control chapter of the ISM for advice on how to minimise the risks of using out-of-band authentication.
16. The Management Centre must not be used to manage other encryption products when securing classified information.
17. The pass-through login to Windows functionality must be disabled.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

ISM

The advice given in this document is in accordance with the Information Security Manual 2013. Australian Government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/infosec/ism/index.htm

Consumer Guide

This Consumer Guide was issued on 13th DECEMBER 2013 by ASD.
This Consumer Guide was updated on 18th FEBRUARY 2014 by ASD.