



Utimaco DiskEncrypt



Together with its partner DriveLock SE from Munich, Aachen-based Utimaco GmbH has further developed the product Sophos SafeGuard Device Encryption / SafeGuard Easy, designed for Microsoft Windows 10, 64-bit (UEFI)

VS-NfD approval

- The product was designed and developed in compliance with the requirements of the German Federal Office for Information Security (BSI) for German government customers and the industry which is subject to the protection of confidential information. Hard disk encryption is approved for information classified VS-NfD, EU RESTRICTED (National) and NATO RESTRICTED.
- The operating conditions for the VS-NfD approval require that authentication in the UEFI-based Pre-boot authentication (PBA) incl. UEFI Secure Boot may only be carried out using a cryptographic smart card, which has been approved by the BSI.
- The administration concepts and components of the product remain unchanged for both the approved version as well as the enterprise version, so that all customers can easily and cost-effectively migrate from SafeGuard Device Encryption 5.60.3 VS-NfD to Windows 10 and the currently approved product Utimaco DiskEncrypt.
- Utimaco DiskEncrypt is authenticated as before using the DiskEncrypt Management Center and DiskEncrypt Client Configuration MSI files.



Utimaco DiskEncrypt 9.0 – VS-NfD Version

On the client:

- “Stand-alone” operating mode
- PBA login via smartcard
- Partition encryption:
 - Encryption algorithm: XTS-AES-256
 - Initial encryption using complete partition encryption or the time-saving “Fast Initial Encryption”
- Random number generator approved by BSI for VSNfD and integration of the smartcard in entropy generation

The central administrative backend:

- To ensure maximum security, communication between the Management Center and a DiskEncrypt client follows a strict offline policy via client configuration files (MSI format).
- The administrative actions of the various security officers in the DiskEncrypt Management Center are logged and stored in the central DiskEncrypt database.



Technical requirements

Client

- Windows 10 64-bit Pro or Enterprise and UEFI from version 1703 incl. Secure Boot.
- CCID-compatible smart card reader supported by DiskEncrypt.
- BSI-certified smartcard. CardOS 5 is implemented in the first version.
- CardOS 4 and 5 support.

DiskEncrypt Management Center

- Windows 10 64-bit Pro or Enterprise from version 1703
- Windows Server 2016 Standard 64-Bit

DiskEncrypt Server

- Windows Server 2016 Standard 64-Bit

DiskEncrypt-Database-Server

- Microsoft SQL Server 2017 Express, Standard or Enterprise 64-bit

DiskEncrypt supports both the Windows 10 Semi-Annual Channel (SAC) from version 1703 as well as the integrated Microsoft In-Place Upgrade mechanism. This offers simple upgrades from Windows 10 SAC to newer versions, even when the system partition is already encrypted with DiskEncrypt.




Utimaco DiskEncrypt 9.5 – Enterprise Version

For enterprise use, a non-VS-NfD version is available with full support for centralized management, similar to the “managed” mode known from SafeGuard Enterprise:

- Central user administration
- Central administration of security officers
- Logon with user name and password and via smartcard incl. OS login and SSO support
- Import of the Windows Active Directory
- Central policy administration
- Central key administration
- Recovery options
 - Via Challenge / Response
 - Virtual client
- Central inventory
- Centralized logging facility

Utimaco IS GmbH

 Germanusstraße 4
52080 Aachen, Deutschland

 +49 241 1696 200

 hsm@utimaco.com

For more information about Utimaco HSM products, please visit:
hsm.utimaco.com

© Utimaco IS GmbH 03/20

Utimaco® is a trademark of Utimaco GmbH. All other named Trademarks are Trademarks of the particular copyright holder.
All rights reserved. Specifications are subject to change without notice.