



Winmagic SecureDoc Enterprise Server 4.3.1

Common functionality

CRYPTAS it-Security GmbH

Modecenterstrasse 22/B2
A-1030 Wien

www.cryptoshop.com

www.cryptas.com

Winmagic SecureDoc Enterprise Server's (SES) functions in general

SecureDoc Enterprise Server by Winmagic is a highly performant application protecting an enterprises confidential data by means of encryption. The product's main characteristics consist in its excellent ability to be integrated into Microsoft environments, such as Active Directory, Windows PKI, MS-SQL, its scalability, its easy maintenance, and not at least the particular good protection of data through strong encryption and the support of strong authentication.

Strong encryption:

SES is using AES 256 (Advanced Encryption Standard – this is an algorithm with 256 key length) for symmetric encryption of data. These symmetric keys are protected by asymmetric encryption (digital certificates). Only the owner of the secret (private key) has access to a key file, containing the symmetric keys. The certificates can be issued either by an already existing PKI (e.g. Microsoft Windows 2K Server or newer) or by the onboard certification authority of the SES...

Strong authentication:

Instead of authenticating with username and password, to access the key file (weak authentication), advanced technologies like smartcards or smart tokens can be used optionally. In this case, the user's secret (the private key) to access the key file will be carried on the card or on the token and can not be taken away from the device. No vulnerable information is remaining on the user's computer (strong authentication)

“Something you have (token, smartcard) and something you know (pin)”

Applications:

SecureDoc Enterprise Server allows administration of the functionalities of SecureDoc in an enterprise environment. Such as:

- Encrypting hard disks of client computers and servers. Optionally whole hard disks or single partitions can be encrypted. If you decide to encrypt whole hard disks, the user has to authenticate before the start of the operating system (pre boot authentication).
- “Container encryption” – there is an option to set up encrypted areas on hard disks, that are mounted as “drive”.
- “File and folder encryption” - single files or folders on hard disks, removable media or on server shares can be encrypted for single users or user groups.
- “Media encryption” - the content of CD /DVD, usb volumes and even floppy disks can optionally be offered or required.
- “Selfextractor” – in special cases, files or folders can be transfered to external users encrypted. In this case, the information is protected by password only, but the recipient does not have to be member of the internal organisation. He just needs to have the self extractor, which is free available.

Scalability:

SecureDoc Enterprise Server also meets requirements of huge organisations:

- Reliability: SES' components support redundancy
- SES supports multiple sites architectures and so called "offline clients" (computers, that never access the corporate networks)
- In addition, data can be protected not only on client computers and servers, but also on PDAs.
- The owner of an IT environment is free to decide, which functionalities are provided to specific groups of computers. Thus, it is possible to meet the requirements of sites and classes of users and computers according to their role in the corporate environment. (For example: a desktop computer in a head office is likely subject to very different threats than a field technician's notebook and therefore it needs a total different set of configurations and functionalities)

Administration of access to encrypted information:

Access to resources, encrypted data and computers, is administrated by defined administrators using a "management-console". Therefore users can be assigned to administrate groups or containers, which stand for a set of resourced or devices. Users and groups can be imported from Microsoft Active Directory (AD) and stay synchronised with it. The local key files on the computers are automatically updated whenever a key is added or removed in the object properties settings in the SES database (management console). Additional to this, the helpdesk has access to a user friendly and secure password recovery / key recovery tool.

Administration of Client-settings:

Permissions, provided functionalities and other client specific settings are defined in profiles. Those settings are distributed automatically to all assigned clients whenever a configuration has changed. Thus, single computers and groups of devices with similar demands can be administrated in an easy and comfortable way.

Integration in Microsoft environments:

- SES uses MS SQL as database server
- SES can use MS Active Directory a source for user accounts, groups and containers as well as the administration structure.
- SES can use certificates, issued by MS PKI
- SES can use the Windows integrated smartcard authentication
- Installation packages for SecureDoc client software, created by SES, can be distributed and installed by MS SMS and its follow up products.

Support of other environments:

- SES can import user accounts and groups from any available LDAP directory
- SES can use certificates of any X.509V3 compatible PKI
- SecureDoc installation packages can be distributed to client computers by any software distribution systems.

Components of SecureDoc Enterprise Servers (SES)

SecureDoc Enterprise Server consists of at least 3 (optional 5) components

In the background there are:

- The SES database
- The SES Management Console

In the front there are:

- SD Connex
- SD Active Directory Sync (optional)
- Online Password Recovery (optional)

The SES Database:

SecureDoc Enterprise Server stores all information, group membership, object properties, passwords and access keys in an encrypted database. This database can be hosted on any existing SQL server as additional database or run in an instance of SQL desktop edition (SQL 2000 MSDE or SQL 2005 Express Edition). Administrative rights on the SQL server are not necessary after the creation of the database.

SES Management Console:

The Management Console is used to access and display the encrypted content of the database. In the Console the assigned administrator can setup configurations, administer user accounts and keys, prepare installation packages and follow up events. It can be installed on the workstation of the assigned administrators. Multiple consoles can access one SES database.

SD Connex

This is the communication service of SecureDoc Enterprise Server. It connects SecureDoc client software and the SES database. It has to be visible to all “online clients” in an organisation. In huge organisations, there can be multiple SD Connex servers. “Offline clients” communicate with the database using email, CD or USB medias.

Active Directory Sync (optional)

This service synchronises user accounts, groups and container with Active Directory. Changes, made in AD are automatically taken into the SES database. The other way round, changes on objects in the SES database are not written back into AD.

Online Password Recovery (optional)

The OPR is a web interface, that allows the helpdesk team (or optional the user himself) to recover forgotten passwords or unlock locked computers in a secure way without contacting the SES administrator.

CRYPTAS it-Security GmbH
Modecenterstrasse 22/B2
A-1030 Wien, Austria
T +43 (1) 798 96 96 – 0
F +43 (1) 798 96 96 – 99
info@cryptas.com

www.cryptoshop.com
www.cryptas.com