

SMARTCRYPT ENTERPRISE MANAGER

Organization-Wide Encryption and Discovery Administration

PKWARE's Smartcrypt is the only enterprise data protection solution that combines intelligent data discovery, persistent encryption, and streamlined key management. With Smartcrypt, organizations can secure sensitive data against internal and external cyber threats, and apply encryption policies across every enterprise operating system.

Exceptional Functionality and Ease of Use

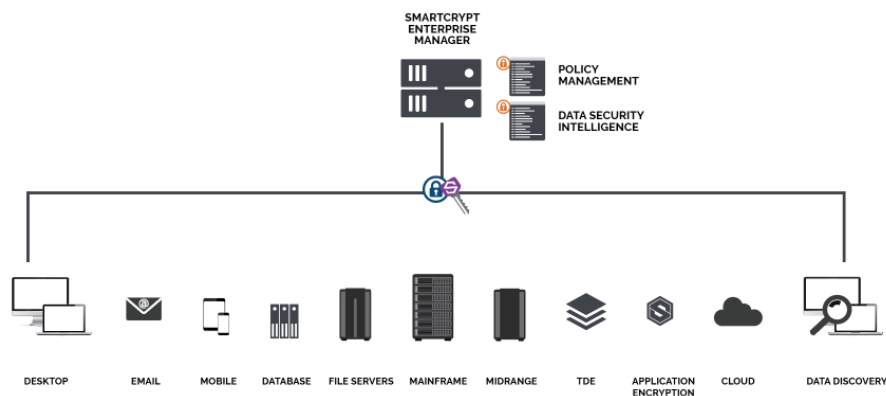
The Smartcrypt Enterprise Manager is the central component of the Smartcrypt platform, managing the Smartcrypt agents that are installed on an organization's servers, mainframes, and user devices.

The Smartcrypt Enterprise Manager allows administrators to define an organization's encryption and data discovery policies and apply them across the entire company. It controls encryption key management, key synchronization, and key delivery, as well as data discovery scanning and remediation.

Administrators can use the Enterprise Manager to grant or revoke user access to encryption keys at any time, and can define policy keys to be included in every encryption operation.

PRODUCT SUMMARY

- » Web-based administration console used to define and apply encryption and data discovery policies across the entire organization.
- » Manages Smartcrypt agents installed on user devices, servers, and mainframes.
- » Provides centralized key delivery and key exchange, automating the key management process for end users.
- » Policy groups allow for retroactive access to content, without the need for re-encryption
- » Data Security Intelligence tools provide detailed event reporting without the need for a third-party reporting tool.



Smartkey Technology

At the core of the Smartcrypt platform is PKWARE's revolutionary Smartkey technology. With Smartkeys, businesses gain across-the-board control of who can decrypt files and read data.

A Smartkey is a unique key generated by the Smartcrypt agent for a specific file, folder, or other protected asset. With Smartkeys, user access can be added or revoked at any time—even if the files have been shared, copied, renamed, transferred, or emailed—ensuring full lifecycle protection.

Intelligent Data Discovery

Smartcrypt provides sophisticated data discovery capabilities, allowing organizations to identify and protect sensitive data as soon as it appears in a shared file location or user device..

Administrators can use the Smartcrypt Enterprise Manager to define the organization's criteria for sensitive data, to specify the user devices and shared file locations to be scanned, and to select the remediation that will be applied when sensitive information is identified.

Data Security Intelligence

Smartcrypt's Data Security Intelligence tools provide complete visibility into which files are encrypted, which users have accessed them, and where the events took place.

Unlike other data protection products, Smartcrypt provides complete, easy-to-use reporting without the need for a third-party reporting tool. Administrators can run reports directly in the Smartcrypt Enterprise Manager console, or use the console to configure data for retrieval via SIEM agent or API.



TECHNICAL SPECIFICATIONS

(Please refer to Smartcrypt agent datasheets for more details on supported systems.)

OPERATING PLATFORMS

- » Windows Server 2008, 2008 R2, 2012, 2012 R2

INTERNET INFORMATION SERVICES

- » IIS 7.0, IIS 7.5, IIS 8.0

SQL SERVER

- » SQL Server 2008, 2008 R2, 2012, 2014

ALGORITHMS

- » Encryption:
AES256 (block level encryption in AES-CBC mode)
- » Signing:
RSA 2048 SHA 512 PSS (metadata)

KEY STORAGE AND RETRIEVAL

- » OASIS KMIP
- » PKCS#11

FILE ENCRYPTION CERTIFICATE AND KEY TYPES

- » Smartkeys
- » X.509 Digital Certificates
- » OpenPGP