SecureDoc™ by WinMagic

SecureDoc™

Removable Media Container Encryption (RMCE)

Enterprise key management for removable storage:

no passwords | no gaps | no compromises

The Challenge

Removable media is a persistent gap in enterprise data protection. USB drives and external storage move between endpoints, teams, and locations – often outside the visibility of IT security controls.

Password-based encryption addresses the threat in principle but introduces operational risk at scale: shared credentials undermine access control, forgotten passwords result in data loss, and employee turnover leaves encrypted media either exposed or permanently unrecoverable.

The Solution

WinMagic's SecureDoc RMCE eliminates these risks by replacing passwords with enterprise key management. Authorized users on managed endpoints access encrypted media automatically, no password prompts, no helpdesk calls, no security workarounds needed. When an employee leaves, their key is revoked instantly. When data must be shared externally, a built-in Media Viewer provides secure access on any device.

How It Works

1 **Create a container**

Users create an AES 256-bit encrypted container on any removable media (USB, external drive, network share, or CD/DVD) of up to 4 TB.
Administrators specify how much space to allocate, leaving the remainder available for unencrypted use.

2 **Dual drive letters mount automatically**

When the media is inserted on a managed endpoint, it mounts with two drive letters:
- one for the encrypted container
- one for the unencrypted space
Disc Access Control (DAC) policies apply separately to each.

3 **Keys unlock, not passwords**

Group-based cryptographic keys unlock the encrypted container automatically. Users open File Explorer without using a password and see their files, with no delay.
SecureDoc supports company-wide, group, and personal keys, all configurable per profile.

4 **Share securely beyond your network**

For unmanaged recipients, SecureDoc embeds a Media Viewer and Key File directly on the media. External partners, contractors, or agencies access the encrypted container with a password, no SecureDoc installation required.

✓ If a password is lost, Challenge/Response recovery with an admin restores access.

Supported Media & Platform

Supported Media
- USB flash drives
- External hard drives
- Shared/network containers CD/DVD media

Supported Platforms
Windows and macOS endpoints (managed and unmanaged)

Management
Centrally managed through SecureDoc Enterprise Server (SES)

Encryption
AES 256-bit

Key Capabilities

Automatic Key Unlocking

Group-based keys unlock encrypted removable media on managed endpoints without using passwords, eliminating helpdesk burden and the security risk of shared credentials.

Disc Access Control (DAC)

Enforce encryption on all writes. Configurable policies for unencrypted space: no access, read only, or “read only if not encrypted”, ideal when external devices write unencrypted data.

Key Labeling

Human-readable labels link encryption keys to users, departments, or groups. Administrators can identify the correct key for any container instantly even years after it was created. This ensures long-term data recoverability that password-based systems cannot provide.

Trusted Device Allow List

Only drives that IT has pre-approved are allowed to connect. When you insert a USB drive, Port Control checks it against the authorized device list.
If it's not on the list, it is blocked before anything on the drive can be opened.

Granular Policy Control

Policies are applied at the device level, with user and key associations managed through the SES console. Administrators can assign specific profiles to individual devices and associate users and keys, accordingly, providing fine-grained control over removable media and encryption behavior.

File Activity Logging

SecureDoc logs the names of all files written to removable media both to the encrypted container and to the unencrypted free space on managed devices.
These logs are transferred to the SES console, providing a clear audit trail for compliance with HIPAA, GDPR, PCI DSS, and other regulatory frameworks.

Partial Encryption with Dual Drive Letters

RMCE splits removable media into encrypted and unencrypted space, each mounted as its own drive letter (Windows). DAC policies apply separately to each.
The unencrypted drive letter can be set to read-only (or “read only if not encrypted”) while all writes are forced to the encrypted container.

RMCE for Unmanaged Devices

RMCE embeds a Media Viewer and Key File directly onto the media. Recipients on an unmanaged device insert the drive and access the encrypted container with a password, no SecureDoc installation required. This enables secure data exchange with external partners, contractors, courts, and agencies.
If the password is lost/forgotten, the user can perform Challenge/Response recovery with the admin to regain access to the encrypted data.

Group Keys & Key Rings

SecureDoc supports company-wide keys, group keys, and user keys – all configurable per profile. Multiple users or Active Directory groups can each have their own unique cryptographic key file to unlock the same encrypted container.
Users collaborate securely without sharing passwords. When an employee leaves, their key is revoked – no passwords to change, no data exposed.

Executable Quarantine

When removable media contains executable files on unencrypted space, SecureDoc automatically renames them to .quarantine, preventing them from running on managed endpoints.
This neutralizes a common attack vector, malware delivered via USB, without relying on antivirus detection or user judgment.
The original files remain intact and recoverable by an administrator, but cannot execute unless explicitly restored.

Password-based Encryption vs. SecureDoc™ RMCE

Capability	Password-Based Solutions	SecureDoc™ RMCE
Multi–User Access	Users share a single password to collaborate on a USB drive.	Each user or group is assigned the key to unlock the specific container.
Employee Departure	Password must be changed on all shared drives, or data remains exposed.	Revoke the individual's key. No passwords to change, no data exposed.
Forgotten Credentials	Data is lost or requires costly recovery procedures.	Automatic key unlocking on managed endpoints. Challenge/Response recovery on unmanaged devices.
Key Identification	Backend database only. Identifying the correct key years later is difficult.	Human-readable Key Labels link keys to users or groups for instant identification.
Encryption Model	File-based encryption leaves the USB file system exposed to unencrypted writes.	Container-based encryption claims drive space. DAC prevents unencrypted writes.
Audit Trail	Password access provides no per-user audit trail.	File-level activity logging with per-user identity.
Offline Access	Often requires a server connection or hidden metadata that can be corrupted.	Embedded Media Viewer and Key File enable access on any device, online or offline.
Policy Granularity	Typically device-level or user-level only.	User + device level policies. Configurable per specific user on a specific device.

Ready to eliminate password-based USB encryption?

Contact us to learn how SecureDoc RMCE delivers enterprise-grade protection for every removable device in your organization.

SecureDoc™ by WinMagic