



## External Media Shield

CMG External Media Shield (CMG EMS) is a component of CMG Enterprise Edition that provides enforced access controls and encryption for external media. Organizations whose employees use USB thumb drives, memory cards, CD or DVD media, compact flash cards, or iPods and MP3 players to store corporate data must ensure that these mobile endpoints are secured at all times to meet data security regulations.

### Overview

CMG EMS extends the enterprise encryption that has been in CMG for several years by installing a modified version of the CMG Shield along with encrypted key material and policies onto external media, allowing the security policies to travel with the data.

Integrated with CMG Enterprise Edition, CMG EMS provides automatic encryption of data on external media accessed via any Windows laptop, desktop, tablet PC or handheld device running a supported operating system. When an unprotected media device is inserted into the desktop, laptop or handheld, the user is prompted to Shield that media device and set a password that will be used to protect the data on that device. With the CMG EMS password defined, the Shield, encrypted key material and policies are automatically copied to the external media. Then, if specified by policy, the device is scanned, and existing data is encrypted according to Intelligent Encryption policies. Administrators can establish policies to encrypt all data or allow encrypted and non-encrypted data to coexist—a critical option due to the ever increasing popularity of device use for personal audio and video files.

Supported media devices include any externally connected data storage such as USB sticks, SD cards, Compact Flash, iPods and MP3 players as well as USB connected hard drives with FAT, FAT32 or NTFS file systems. CD and DVD media, when burned with supported software, is also encrypted if specified by policy. Additional security for CD and DVD media is available via CREDANT Protector, including expanded burning software support and port controls.

### How It Works

CMG EMS ensures security of sensitive data as it flows beyond the protected computer, guaranteeing expansive data mobility while ensuring data protection and privacy. When the administrator enables EMS for an individual user or group of users, the system places the CMG EMS client on every piece of removable media inserted into a CMG-protected computer or handheld device. During this Shielding process, which occurs whenever an unprotected media device is inserted in the computer, the user is prompted to define a password that will control access to that media device. Password strength is enforced per administrator-defined policies, including password length and whether special characters or numbers are required in the password. An installer is also copied to the media to enable a clientless or a one-time client install so users can securely read and edit encrypted data from a computer not protected by CMG. This access to encrypted external media from “UnShielded” (unprotected by CMG) computers can be disabled by the administrator via policy.

CMG EMS automatically encrypts any files added to or edited on the media, no matter where that data is saved on that media. Administrators can set policy so any existing files on the media are encrypted during the Shielding process or those existing files can be left unencrypted. Policies can also be defined to exclude certain file types from encryption. This is a useful option when allowing employees to access personal media devices like iPods from their corporate computer.

### Key Features

EMS extends CMG’s unique policy-based Intelligent Encryption and centralized administration to external storage devices, such as iPods, USB drives, CD/DVD media and memory cards. Fully enforceable, flexible and easy to use, CMG EMS key features include:

- centralized management via CMG Enterprise Edition
- local policy enforcement to secure and control all mobile endpoints no matter where they travel
- flexible access options (restrict use to CMG Shielded computer only, or allow “clientless” option for non-company locations)
- automatic Policy-based Intelligent Encryption
- locally enforced, strong passwords
- user-transparent encryption
- option to control encryption by file type
- help desk support for easy, reliable, remote data recovery in case of forgotten passwords
- fail-safe options such as cool down periods between authentication attempts or automatic deletion of encryption keys to protect against brute force attacks
- simple, intuitive user interface

## How It's Different:

### Strong Security with Increased Data Portability

Centrally administered by CMG Enterprise Server, CMG EMS has rich EMS specific policy controls to ensure data privacy and recovery while controlling the encryption algorithm, the key used to perform encryption, password strength and a variety of access control options (Figure 1). These policies are then enforced locally on the media device so the data remains encrypted no matter where the external media device goes, even on machines that are not running the CMG Shield. In addition, CMG EMS may be restricted by policy to only grant access to encrypted data from a machine running the CMG Shield. CMG EMS also supports the same administrator assisted challenge-response recovery mechanism previously supported by the CMG Handheld Shield.

Key examples of EMS encryption policies available to administrators include:

#### EMS Encrypt External Media

If *True*, enables encryption on external media using the encryption algorithm defined by policy (default is AES-256).

#### EMS Encryption Rules

This policy allows you to granularly define what data should or should not be encrypted. The default "blank" rule set encrypts everything on external media. Examples in the Administrator help explain how to set these rules to encrypt data files on iPods without encrypting files needed for the operation of the iPod.

#### EMS Allow Read-access to unShielded Media

When *True*, allows read-access to existing files on unShielded external media, but will not allow any files to be edited on or added to the external media unless it is Shielded. This policy is extremely useful when working with partner or customer media that can't be Shielded. It allows users to copy presentations or other data from the partner's media to a corporate laptop, but prevents leakage of corporate data to the unprotected media.

#### EMS Scan External Media

If *True*, scans external media on insertion and encrypts or decrypts its contents based on the Encrypt External Media policy value. When this policy is *False* and Encrypt External Media is *True*, the Shield only encrypts new and changed files so any files on the media before it was Shielded remain decrypted.

#### EMS Access Encrypted Data on UnShielded Device

If *True*, allows the user to access encrypted data on external media whether the computer is Shielded or not. When this policy is *False*, the user will be able to work with encrypted data when logged on to any Shielded device, regardless of the Enterprise Server the user activated against. The user won't be able to work with encrypted data via any unShielded computer.

#### EMS Exclude CD/DVD Encryption

If *False*, EMS encryption will also be applied to CD/DVD media when burned via supported software, which currently includes Nero InCD for Windows XP and Windows 2000 and Vista's native Live File System (LFS) burning software. If *True*, EMS encryption will be applied to all external media devices except CD/DVD drives. We recommend setting this policy to *True* when using CREDANT Protector's advanced CD/DVD functionality.

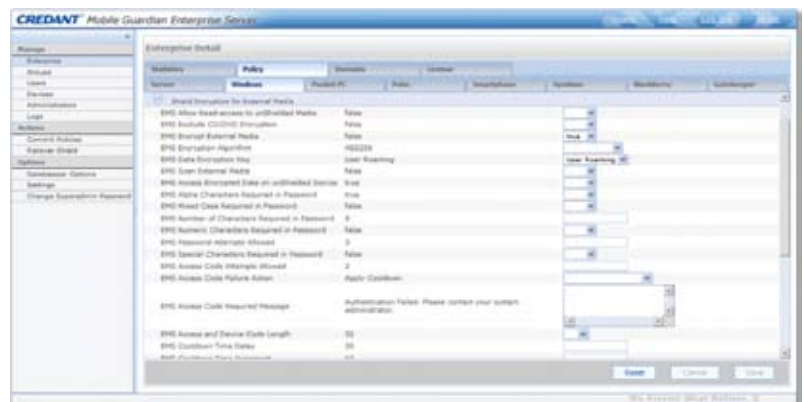


Figure 1. An Administrator can Establish and Control External Media Security Policies from the CMG Enterprise Edition Central Console

## User Scenarios: Security Policy Enforcement

With CMG EMS the administrator can set policy to share data securely with both protected (CMG Shielded) and unprotected (CMG UnShielded) systems, or allow users to share data only with other CMG Shielded systems. Policies can be defined for individual users, groups of users or all users. When external media is Shielded by EMS, an installer is also copied to the media. This allows you to take your encrypted external media to another computer that does not have EMS installed, and still be able to securely read and write encrypted data to the external media. When accessing encrypted data from an UnShielded computer, you have the option to install the EMS Service or access that data via the EMS Explorer, which requires no client installation on the computer. Access to encrypted external media on UnShielded systems can be disabled via policy. The following examples focus on Windows systems, however the use cases for handheld devices are the same in most instances.

## Shielding New External Media

When a user logs in to a CMG protected computer and inserts an UnShielded media device, the computer's CMG Shield for Windows recognizes the media device and checks administrative policy. Because this media device is not Shielded and EMS is enabled for that user, the user is prompted to define a password for the media device. Once the password is accepted, the user is notified that data on this media device will be encrypted, and the Windows Shield writes Shield executable, encryption key material, and policies to the media. If the *EMS Scan Media* policy is *True*, any existing data on the media will also be encrypted at this time. Encryption keys are automatically escrowed at the CMG Server to ensure easy recoverability of data. Any files copied to or edited on this media will be automatically encrypted from this point on, and the EMS password is now valid for that external media device until the user changes it.

If the user declines to Shield the media device and the *Allow Read-Access to unShielded Media* policy is *False*, they are given no access to the media device. If that policy is *True* and they decline to Shield the media device, they can access unencrypted files on the media device, but they are not able to edit those files and save them back to the media device, nor are they able to add new files from their protected computer.

## Accessing a Shielded Media Device from a Shielded Computer

With CMG EMS, data is easily shared between authorized users on any Shielded computer, even if it belongs to another user.

When a user logs into a CMG protected computer and inserts a Shielded media device, the computer's CMG Shield for Windows recognizes that the device is protected by CMG EMS and automatically provides access to data if the logged-in user is the user who initially Shielded this media device. If the media was Shielded by another user or the media is accessed from a computer other than the system that originally Shielded it, EMS prompts for the media device password before allowing access to protected data. If a user fails authentication they can access unencrypted files on the media device, but they do not have access to any encrypted data and are not able to add new files from their protected computer. With successful authentication to the media device, any files copied to or edited on this media will automatically be encrypted.

## Accessing a Shielded Media Device from an UnShielded Computer

In this scenario, data is easily shared between authorized users, even from an UnShielded computer, for secure portability of corporate data.

Unlike existing approaches to external media encryption, CMG EMS supports two modes of operation dependant upon the state of the Windows system. If CMG EMS on the external media device recognizes a laptop is not Shielded and the user has administrator privileges on that computer, CMG EMS prompts the user with two options to access encrypted data:

- 1) Install the EMS Service to access encrypted data (this option enables transparent access of protected media devices from that computer via Windows Explorer); or
- 2) View Encrypted files via the EMS Explorer (this option leaves no software on the computer, but provides slightly less transparent access via the EMS Explorer instead of Windows Explorer).

If the logged in user does not have administrator privileges on the UnShielded computer, they are only presented with the option to view encrypted files via the EMS Explorer. Once an option is selected, the user then is prompted for his or her media device password (Figure 2 shows Option 2 login). Once authenticated they can access encrypted data. Any files copied to or edited on this media device will automatically be encrypted.

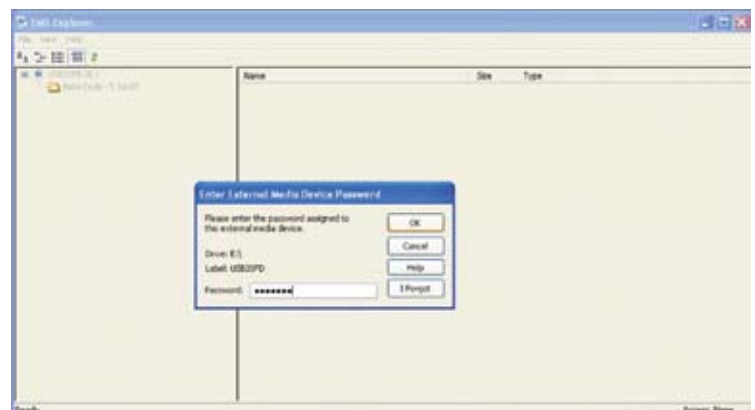


Figure 2. Log-in Prompt to View Encrypted Files Using EMS Explorer Option

## Authentication Options

CMG EMS passwords are not the same as the password used to log on to the user's Windows computer or Windows Mobile device. Rather, CMG EMS requires the user to set a password for every new piece of external media. Administrators can define, enable, disable, and enforce detailed policies around password strength through the CMG EE console. EMS also provides disconnected help desk assisted recovery and fail-safe actions, such as cool down periods between authentication attempts or automated deletion of encryption key material to protect encrypted data if the device is lost or stolen. If the media device is found, this key material can be recovered to the media device via the computer that originally Shielded the media and the CMG Server.

Examples of EMS authentication policies available to administrators include:

**EMS Alpha Characters Required in Password**

**EMS Numeric Characters Required in Password**

**EMS Number of Characters Required in Password**

(1-40) Minimum number of characters required in the password.

**EMS Password Attempts Allowed**

(1-10) Number of times the user can attempt to enter the correct password.

**EMS Access Code Failure Action**

**Apply Cooldown, Cooldown Time Delay and Cooldown Time Increment** <all text before this should be bold> work together to define increasing time delays between attempts to enter the correct help desk assisted recovery code, thus resisting brute force attacks in case the media is lost or stolen. Help desk assisted recovery is required only if the user fails authentication or indicates that they've forgotten their password.

**Wipe Encryption Keys** forces automatic destruction of the encryption key material on the removable media, making the encrypted data inaccessible until the media owner connects the media to the originally Shielding computer or handheld and manually authenticates. The Shielded media requires no connectivity to the CMG environment or the corporate network to implement key material destruction as a response to multiple failed authentication attempts.

**EMS Access Code Failed Message**

(String—5-500 chars, such as "You are not authorized to use this device. Please contact your system administrator.")

Administrator configurable message that displays following unsuccessful authentication.

## Summary

CREDANT Mobile Guardian Enterprise Edition supports today's sophisticated mobile enterprise environments by extending its unique policy-based encryption and centralized administration for computers and handhelds to external storage devices via the new CMG External Media Shield, or CMG EMS. When a portable storage device is inserted into a CMG-protected desktop, laptop, Smartphone or PDA for the first time, CMG detects the device and requires the user to set a password for future access to protected data on that media. Once the password is set, CMG automatically provisions the CMG EMS client, secured encryption key material, and policies to the media device. From this point forward the device is password protected and all data added to or edited on that media is automatically encrypted per policy. Administrative policies can be established for individual users or groups of users and require that all data be encrypted. Policies can also be set to allow encrypted and non-encrypted data to coexist. Enterprise Edition customers who do not need full protection for some systems can purchase a smaller footprint External Media Edition for Windows Shield. This Windows Shield only enforces EMS policies and is useful when fixed disk encryption is not required.

CREDANT Technologies	15303 Dallas Parkway, Suite 1420, Addison, Texas 75001 USA	866-CREDANT (273-3268) or 972-458-5400	www.credant.com	info@credant.com
----------------------	--	---	-----------------	------------------