

# StandAlone Windows Shield

The CREDANT Mobile Guardian (CMG) StandAlone Windows Shield installs with pre-configured policies and requires no Enterprise Server or console of any type. In fact, no server interactions are ever needed in order to install and operate this Shield, though this Shield can be easily migrated into an CMG Enterprise Edition environment at any time.

## Overview

The CMG StandAlone Windows Shield is a new protection option for enterprise customers who support an affiliate model where non-employee or contractor computers have access to sensitive corporate data. This Shield allows the organization's data to be protected on laptops and desktops that are in the corporate domain, in another domain or not part of any domain. It is also valuable for rapid deployment to protect corporate or affiliate systems, especially given that the StandAlone Windows Shield may later be migrated into fully managed CMG Enterprise Edition Windows Shield. Because the StandAlone Windows Shield requires no management infrastructure it also offers an option that scales well for Small to Medium Business where security is also important, but resources to manage solutions are limited.

There are two CMG StandAlone Windows Shield options. One distribution was designed to be installed only on computers with the Intel<sup>®</sup> Centrino<sup>®</sup> Pro and Intel<sup>®</sup> vPro<sup>™</sup> processor technologies with Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT). This Shield is available exclusively through Intel distributors. The non-hardware restricted StandAlone Windows Shield, which can also be installed on computers with Intel processors, is available through CREDANT and authorized partners.

## Key features:

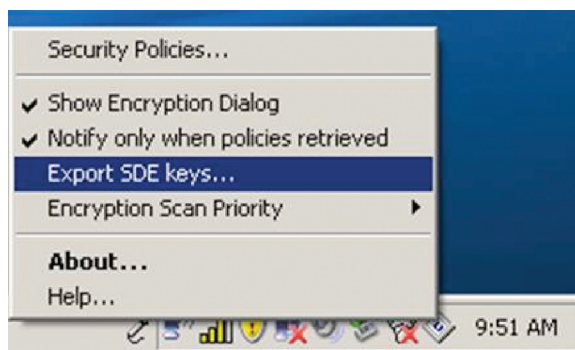
The CMG StandAlone Windows Shield provides a simple solution to protect sensitive data in any environment. Flexible and easy to implement, CMG StandAlone Windows Shield key features include:

- No management infrastructure enables quick deployment of data protection for laptops and desktops
- Easy migration to a fully managed CMG Enterprise Edition Windows Shield supports organizational growth
- Pre-defined security policies are locally enforced to secure and control sensitive corporate data no matter where it resides
- User-transparent encryption
- Can be deployed alone or in same environment with fully managed Windows Shields
- Broad OS support including Microsoft Windows 2000, XP Professional, XP Tablet PC Edition, and Microsoft Windows Vista (Enterprise Edition, Ultimate Edition & Business Edition)

## How It Works

The CMG StandAlone Windows Shield ensures security of sensitive data inside or outside of the corporate network for domain and non-domain computers. A variety of install options support environments with or without IT administrators. Command line installation is available for remote, silent deployment via software distribution packages or the computer owner can install this Shield via a simple, interactive, local interface. All policy settings are pre-configured to simplify installation and can't be changed unless the Shield is migrated into a CMG Enterprise Edition environment.

Once the installation completes the user is prompted to back up or archive their encryption keys, which are generated uniquely for each system during the installation. Key archival is crucial since it ensures that data is recoverable in case the encryption keys are damaged or otherwise become inaccessible to the computer. If the user does not archive their encryption keys immediately after installation, they are prompted to archive their encryption keys each time they log in. Key archiving can also be initiated at any time via the "Export SDE Keys" option available via the CMG Shield icon in the status area of the Windows taskbar, as shown in *Figure 1*.



*Figure 1: Initiating encryption key file back up*

During the key export process, keys are encrypted and stored securely in an executable file that must be saved in a location other than the local hard drive, such as a USB thumb drive or network drive. The default key archive file name includes the name of the computer that the encryption keys are associated with, to help ensure keys are recovered to the correct system if that ever becomes necessary. To ensure recoverability of data, encryption will begin only after encryption keys have been exported to recovery media. It is the user's responsibility to ensure that the exported key material is maintained in a safe location. If recovery is ever needed, the user simply runs the archived key executable which automatically places the encryption keys in the proper location on the computer.

Once encryption keys have been archived, the encryption process begins. All files on the computer are encrypted via CREDANT's System Data Encryption (SDE), with the exception of some system files required to boot the system. The user can continue to work on the computer throughout the encryption process. If the computer is shut down before all files are encrypted, CREDANT's Intelligent Encryption continues encrypting where it left off the next time the computer is started until encryption is complete. As users create, edit, or transfer files to their computer, the StandAlone Windows Shield automatically and transparently encrypts that data without requiring any action by the user. For more information on SDE, contact your CREDANT representative.

**How It Works (cont.)**

The StandAlone Windows Shield is a non-connected, unmanaged Shield so unlike the centrally managed CMG Enterprise Edition Windows Shield, the user can decrypt their data and uninstall the StandAlone Windows Shield at any time. Because the StandAlone Windows Shield is unmanaged, the following CMG features which require central management via a CMG Server infrastructure are not supported.

- External Media Shield (EMS) encryption of data stored on USB, CD and other media
- Centrally managed security policy updates
- Device inventory and audit reporting
- The StandAlone Shield integrates with the Microsoft Windows Graphical Identification and Authentication Library (GINA) or Credential Provider (Vista) and does not offer a GINA replacement Shield option

If these features are needed, the StandAlone Windows Shield may be activated against a CMG Enterprise Edition Server and converted into a managed Shield. This process is simple because and essentially requires that you provide the Shield with information on how to contact the CMG Server infrastructure over the network.

**Summary**

The CREDANT Mobile Guardian StandAlone Windows Shield supports today’s sophisticated mobile enterprise environments by offering a flexible and fast deployment option to protect domain and non-domain computers. System Data Encryption provides transparent and automatic encryption of all data on the protected computer. This disconnected, unmanaged Windows Shield can be implemented alone or in the same environment with other CMG Enterprise Edition Windows Shields. The StandAlone Windows Shield offers a simple migration option into an Enterprise Edition environment to enable support for central policy management, External Media Shield, and audit reporting.

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