



StandAlone Edition for Windows Shield

The CREDANT Mobile Guardian (CMG) StandAlone Edition for 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

CMG StandAlone Edition for Windows 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 Edition for Windows Shield may later be migrated into a fully managed CMG Enterprise Edition Windows Shield. Because the StandAlone Shield requires no management infrastructure it also offers an option that scales well for Small to Medium Business where security is important, but resources to manage solutions are limited.

Key features:

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

- No management infrastructure enables quick deployment of data protection for Microsoft Windows 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. XP Professional, XP Tablet PC Edition, and Microsoft Windows Vista (Enterprise Edition, Ultimate Edition & Business Edition)

How It Works

The CMG StandAlone Edition for Windows Shield ensures security of sensitive data inside or outside 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. With a few exceptions, 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.

There are a number of advanced configuration options available to ensure the StandAlone Edition for Windows Shield works in a variety of environments. CREDANT2go can be installed with the Shield, via the command line or via the interactive custom installation. CREDANT2go allows you to create a password-protected, compressed, encrypted, and self-extracting archive of one or more files. You can then email the encrypted archive, place it on a network drive, or transfer it to another Windows device. During installation you can also choose to encrypt only the system volume or all fixed volumes on the computer. Finally, customer also using CMG Enterprise Edition can configure their StandAlone Edition for Windows Shields to automatically escrow encryption keys to the CMG Server. Automatic key escrow can be configured via command line installation or via a registry setting after installation.

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. This step is not needed if automatic key escrow to a CMG Enterprise Edition Server has been configured for the StandAlone Shield. 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*.

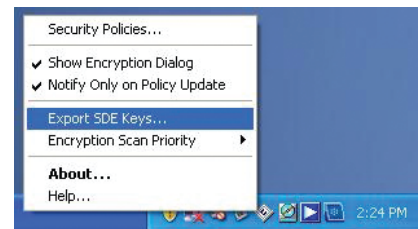


Figure 1: Initiating encryption key file back up

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 escrowed, either automatically to a CMG Server or manually. With manual key escrow, 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 or administrator 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 Edition for Windows Shield automatically and transparently encrypts that data without requiring any action by the user. For more information on SDE, contact your CREDANT representative.

The StandAlone Edition for 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 Shield at any time. Because the StandAlone 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 compliance reporting

If these features are needed, the StandAlone Edition for Windows Shield may be activated against a CMG Enterprise Edition Server and converted into a managed Shield. This upgrade from StandAlone Edition to Enterprise Edition is simple and enables easy migration of your Windows security from unmanaged to managed (upgrade costs may apply).

Summary

The CREDANT Mobile Guardian StandAlone Edition for 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 Edition for Windows Shield offers a simple migration path into an Enterprise Edition environment to enable support for central policy management, External Media Shield, and compliance reporting.