



TECHNICAL WHITE PAPER

CREDANT Encryption Solutions Overview



CREDANT Encryption Solutions Overview

- Introduction 4
- CREDANT Solutions Overview 5
- Architecture 6
 - Overview 6
 - CREDANT Mobile Guardian (Software encryption) 6
 - CMG Enterprise Server 7
 - Enterprise Server 7
 - Enterprise Server Web Interface 7
 - Device Server 7
 - Web Services 7
 - Core Server 7
 - Key Server 8
 - Policy Proxy 8
 - CMG Shields 8
 - CREDANT FDE for Mac 8
 - CMG EE for Windows 9
 - CMG External Media Edition (EME) for Windows 9
 - CMG StandAlone Edition for Windows 9
 - CMG Dell Edition Windows Shield 9
 - CMG External Media Shield 9
 - CREDANT FDE for Windows, CREDANT FDE DriveManager
and CREDANT PolicyServer 10
 - CREDANT PolicyServer 10
 - CREDANT PolicyServer 10



CREDANT Encryption Solutions Overview

CREDANT PolicyServer MMC Snap-in	10
CREDANT PolicyServer Database Module	10
CREDANT Full-Disk Encryption Windows Clients	11
CREDANT FDE for Windows (Software Encryption)	11
CREDANT FDE DriveManager (Hardware Encryption) - Managed	11
CREDANT FDE DriveManager (Hardware Encryption) - Standalone	11
Functionality	12
Overview	12
Encryption and Management Options - High Level Summary	12
Technology Validations	13
Centralized Administration and Pre-Defined Policy Options	14
Small Office, Medical Office or Individual	14
Medium to Large Enterprise	15
Authentication	20
Integration and Interoperability with existing IT Infrastructure and Processes	22
Usability	23
Removable Media Protection	25
Audit and Compliance Reporting	27
CREDANT Benefits	29
Summary	30
Contact Us	31

CREDANT Encryption Solutions Overview

Introduction

The globalization of information has forever changed the security landscape. Today, information is exchanged in sub-milliseconds. Exports from entire countries are bought and sold online. Businesses merge into conglomerates or dismantle less profitable divisions. Healthcare providers access information on life-threatening illness. For better or worse, our new, more digitized world enables fast information access, a certain benefit for the patient awaiting care, or businesses whose growth relies on e-commerce. A certain nightmare of possibilities exists for consumers, whose personal information is increasingly exposed to criminals trading in fraud and identity theft. It's clear that now more than ever, the digitized world demands data encryption.

In the United States, Canada and Europe, federal regulatory standards increasingly supplement local reforms as the government pressures industries and businesses of all sizes to protect consumers' personal information. In many cases, the penalties for non-compliance can be crippling (as much as \$500,000 per instance in the case of Payment Card Industry-Data Security Standards regulations).

What's more, as social networking and Web-based applications proliferate and handheld devices increase in popularity and sophistication, information is shared more easily and with less reservation than ever. As accessibility increases, so does the risk of exposure. No company or industry is exempt from data tampering. And without proper measures, none can escape the risk of fines, loss of reputation, or possible bankruptcy.

Data encryption isn't just a best practice. It is an imperative for survival in today's global, digitized marketplace.

Yet every organization is unique. The right combination of data encryption solutions must be defined by the existing infrastructure, regulatory requirements and business practices.

CREDANT Encryption Solutions Overview

CREDANT SOLUTIONS OVERVIEW

Protecting sensitive information is critical and with CREDANT, organizations benefit from having unmatched flexibility in how they choose to protect this information. In the past, organizations had only two encryption choices: count on an end user to store a file in a special folder that ensures the file is encrypted, or encrypt the entire hard drive. Both of these software-based solutions had their strong points and challenges, but it became clear early on that it was best to avoid relying on an end user to ensure data security. Encrypting the hard drive, Full Disk Encryption (FDE), was generally considered the most secure solution.

Though encryption technology is built on well-established and standard algorithms, the solutions built around that technology have evolved to include a wide variety of software-and hardware-based encryption options. These choices have been driven primarily by ever increasing compliance requirements and by the fact that business environments are largely heterogeneous. One-size does not fit all. This wide range of solutions benefit organizations by making encryption accessible to every environment, but the plethora of choices sometimes makes it hard to decide which solution is best for you. Each solution provides a slightly different, yet important balance between maximizing security and maintaining usability.

As there is a wide range of options to secure critical corporate data, there is also a wide range of criteria to consider when deciding how to best protect your business. Power users or developers tend to be very sensitive to even the smallest impact on system performance. Less technically savvy end users will likely inundate the help desk with calls for assistance if they are saddled with a solution that forces them to change the way they work. Executives may carry more sensitive information than end users in other

departments and thus require different security policies. Traveling employees naturally incur more risk of data loss for a number of reasons than do employees working on a desktop that never leaves a secure office. Users traveling to countries like China, where there are strict restrictions on entering the country with encrypted laptops may need different policies depending on where they are. Though encryption may be managed by a security team that operates independent of IT, existing IT operations and processes must be taken into account. Resource constrained IT departments will likely challenge any new technology that makes it hard for them to do their job or that requires significant alterations to their existing process. It's also common to find groups within an organization who are independently responsible for the security of their team members, which can generate complex and often conflicting requirements within the same company. Finally, budgets must be considered. If there is existing technology the company already owns but isn't currently using, such as self-encrypting hard drives, a solution that helps them manage that encryption and also allows them to purchase additional software or hardware encryption as needed is desirable. These are just a few of the criteria that a company must navigate when choosing the right solution or solutions for their business.

CREDANT offers both hardware and software encryption with centrally managed or unmanaged options, depending on your needs. All managed solutions include extensive reporting to satisfy compliance needs and to ease deployment and day-to-day use. Products can be mixed and matched to find an overall solution that best fits your needs:

CREDANT Mobile Guardian provides software encryption and security for Windows or Mac OS X laptops and desktops, removable media, and PDAs and Smartphones. Windows systems are protected with CREDANT's Intelligent Encryption and FDE

CREDANT Encryption Solutions Overview

is used to protect Mac computers. External Media encryption is provided for both Windows and handhelds. Windows protection is available in both managed and unmanaged varieties.

CREDANT FDE for Windows provides full disk, software encryption for Windows laptops and desktops. All data on the local drive is encrypted at the sector level, including any blank space on the drive. This fully managed solution includes mandatory, pre-boot authentication and AES 256 encryption. CREDANT's unique network aware pre-boot authentication allows the end user to access the system via an existing domain login. Administrators avoid the high-overhead setup and maintenance of proprietary pre-boot user and administrator accounts.

CREDANT FDE DriveManager technology fortifies the Seagate Momentus self-encrypting 2.5" hard drives with remote management, strong authentication, and extensive auditing and reporting features, thus allowing companies to more easily implement Seagate hardware encryption. FDE DriveManager can be configured during installation to run as a managed or unmanaged client.

As business environments differ, so do the options CREDANT offers to secure critical data in those environments. All CREDANT solutions are designed to provide the most comprehensive security available for data stored on laptops, desktops, removable media and mobile devices. Each solution ensures mandatory authentication and provides industry standard encryption so you can select a product or a combination of products that best fit your needs without having to go to multiple vendors. CREDANT's broad range of solutions ensures your corporate data is secure while allowing your users to focus on doing their jobs and making your business successful.

ARCHITECTURE

OVERVIEW

CREDANT's solutions are built on a scalable, standards-based architecture that allows the flexibility needed to support any environment, regardless of size or complexity. Ports are configurable to eliminate conflicts with other products and to reduce the need for IT changes. While organizations may implement CREDANT solutions on their own, many make use of our professional services organization to help them plan and deploy their solution, thus taking advantage of our experience around best practices. Though CREDANT also protects handheld devices, this paper will focus on protection of laptops, desktops and removable media.

CREDANT MOBILE GUARDIAN (SOFTWARE ENCRYPTION)

CREDANT Mobile Guardian (CMG) Enterprise Edition includes all the components needed to configure, manage and report on the security of your sensitive corporate data (Figure 1). Through a single management interface, administrators can control and secure data on a broad range of devices, including Microsoft Windows and Apple Mac OS X desktops, tablets and laptops and their removable media.

CMG's modular architecture allows for very simple or large, scalable deployments, depending on your needs. The CMG Local Gatekeeper, Handheld Shields, Shield Wireless Installer (CMG Server component) and optional Over-the-Air (OTA) Sync Control enable protection of Smartphones and other handheld devices, as well as any SD cards or other removable media used in those devices. The following provides a more detailed description of the CMG components that protect your laptops, desktops and removable media.

CREDANT Encryption Solutions Overview

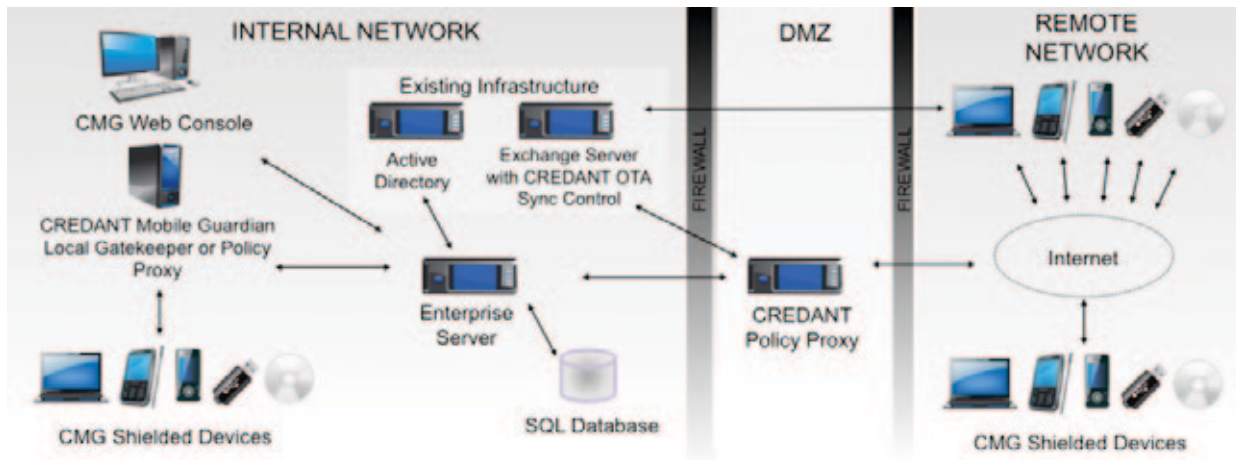


FIGURE 1: CREDANT Mobile Guardian Architecture

CMG ENTERPRISE SERVER

The CMG Enterprise Server consists of multiple components that can be installed on a single server or distributed across multiple servers, depending on the size of your environment and your deployment needs:

Enterprise Server

This is the command and control center for entire architecture and is required for all product functionality. A connection to the SQL Database is required at all times to record device inventory, retrieve reporting data and to escrow key material. This component communicates with Active Directory to authenticate, import, and verify domain users and groups that the CMG Server will be managing.

Enterprise Server Web Interface

This component provides a web-based administration console for all CMG administration, such as configuring policy, viewing or importing Active Directory (AD) users or groups and viewing status of your CMG Environment. It enables CMG administrative access from any supported Web Browser so there's no need for special management client software.

Device Server

This is required for all Shield activations and provides an XML-RPC API interface to the CMG Server. Activation is the initial process by which all Shields register with the CMG Server and acquire their encryption keys and policies. This component also handles all key material recovery codes and password recovery for handholds and External Media Shield (EMS) as well as all Admin Utility and Forensics Integration requests. Though most Server components should be installed in a secure data center, this component may be placed in the DMZ if needed.

Web Services

This component provides the interface for Local Gatekeeper and Policy Proxy communications with the CMG Server and also handles handheld Shield activation requests from Local Gatekeepers.

Core Server

This component is responsible for security policy and license management. It is required by the Enterprise Server and Enterprise Server Web Interface.

CREDANT Encryption Solutions Overview

Key Server

This handles Kerberos authentication requests for Forensics Integration and Admin Utilities. This component is required if using Admin Utilities and a minimum of one key server is required for each managed domain.

Policy Proxy

Policy Proxy provides a network-based communication path between the CMG Server and Shielded devices to deliver periodic policy updates and to receive inventory updates. At least one Policy Proxy is required for Windows and Mac Shields or for Shielded handhelds that communicate to the CMG infrastructure via the network (i.e. not via a Local Gatekeeper), however multiple Policy Proxies can be deployed throughout the environment as needed to optimize communication with geographically distributed devices. All information processed by the Policy Proxy is encrypted so this component can be installed in the corporate network or in the DMZ.

Unless otherwise noted above, the CMG Server components should be installed in a physically secured environment, behind a firewall within the corporate network. The CMG Server must have network connectivity to Active Directory, the SQL database, the CMG Policy Proxy and Local Gatekeepers, and any Shielded devices; however, continuous network connectivity is only required with the database. The CMG Server components can reside on one or more dedicated servers running Microsoft Windows Server 2003 or Microsoft Windows Server 2008. The Policy Proxy can also be installed on systems running Windows XP, Windows Vista and Windows 7. The CMG Server supports various editions of Microsoft SQL Server 2005 and 2008. For complete system requirements see the product documentation.

CMG SHIELDS

CREDANT Mobile Guardian Shield is the on-device component that enforces security policies whether

a mobile device is connected to the network or not. This ensures that all data remains protected on the device and its external media, even if they are lost or stolen. Shields also provide periodic updates to the CMG Server with inventory and compliance information so you can prove at any time that your devices and data are protected. The Shield comes in a number of varieties and supports numerous platforms to help organizations extend their trusted environment and protect sensitive corporate data. CMG Shields are tightly integrated with the device operating system to provide consistently enforced access control, encryption and authorization. In addition to the Shields described in detail below, CMG Shields can be installed on a variety of Windows Mobile (Pocket PC and Smartphone), Symbian and Palm devices to implement and enforce policy and to transfer inventory and compliance information to the CMG Server

CREDANT FDE for Mac

This Shield provides software-based FDE for Intel-powered laptops and desktops running Mac OS X v10.4 Tiger, v10.5 Leopard, and v10.6 Snow Leopard. It implements unique FDE technology that fully secures the Mac without requiring Pre-Boot Authentication, thereby avoiding the many operational constraints associated with traditional FDE-based solutions. Security policies for this fully managed Shield are defined and managed via the CMG Web Console and enforced across the Mac environment, even for non-domain systems and users with local administrator accounts. This Shield is designed from the ground up as a Mac solution, ensuring a familiar experience that will appeal to Mac users. It uses native Mac OS X authentication interfaces and provides out-of-the-box transparency to third-party applications, including Parallels Desktop and VMware Fusion virtualization software. Mac computers containing Boot Camp-installed Windows Environments are also supported.

CREDANT Encryption Solutions Overview

CMG EE for Windows

This Shield provides software-based, Intelligent Encryption for laptops and desktops running Microsoft Windows 7, Vista and XP (32- and 64-bit). It implements and enforces policy for sensitive data on local hard drives, including OS and Program Files, to fully secure the system. It is fully integrated with the existing Windows login mechanism so access to data is controlled by the user's domain password. Seamless, standards-based integration enables support for multi-factor authentication technologies like RSA SecurID, biometrics, and smartcards. Security policies for this fully managed Shield are defined and managed via the CMG Web Console, including External Media Shield (EMS) policies.

CMG External Media Edition (EME) for Windows

This Shield provides software-based, Intelligent Encryption for laptops and desktops running Microsoft Windows 7, Vista and XP (32- and 64-bit). It implements and enforces policy for sensitive data on any removable media inserted into the protected PC, but does not encrypt data on local hard drives. It is fully integrated with the existing Windows login mechanism so access to data is controlled by the user's domain password. Seamless, standards-based integration enables support for multi-factor authentication technologies like RSA SecurID, biometrics, and smartcards. EMS policies for this fully managed Shield are defined and managed via the CMG Web Console. This Shield was designed for systems that require no fixed disk protection or are using CREDANT's FDE to protect local hard drives, but also need external media encryption.

CMG StandAlone Edition for Windows

This Shield provides software-based, Intelligent Encryption for laptops and desktops running Microsoft Windows 7, Vista and XP (32- and 64-bit). It implements and enforces policy for sensitive data on local hard drives, including OS and Program Files, to fully

secure the system. It is fully integrated with the existing Windows login mechanism so access to data is controlled by the user's domain password. Seamless, standards-based integration enables support for multi-factor authentication technologies like RSA SecurID, biometrics, and smartcards. Security policies for this unmanaged Shield are pre-defined or configured during installation for quick, simple deployment. Because this is an unmanaged Shield reporting and EMS are not included. This Shield was designed to protect non-domain systems or those that are members of a domain not managed via the CMG Server.

CMG Dell Edition Windows Shield

This Shield provides software-based, Intelligent Encryption for laptops and desktops running Microsoft Windows 7, Vista and XP (32- and 64-bit). It implements and enforces policy for sensitive data on local hard drives, including OS and Program Files, to fully secure the system. It is fully integrated with the existing Windows login mechanism so access to data is controlled by the user's domain password. Seamless, standards-based integration enables support for multi-factor authentication technologies like RSA SecurID, biometrics, and smartcards. This Shield is factory-installed on a variety of Dell computers with pre-defined security policies so your new Dell systems can arrive already protected by CREDANT encryption. A CMG Dell Edition Server and managed Enterprise Edition for Windows Shield are also available via Dell. These products provide the same data protection and reporting available via CMG, but also include policy templates targeted to specific compliance and regulatory needs.

CMG External Media Shield

This Shield provides enforced access control and encryption for external media. 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

CREDANT Encryption Solutions Overview

cards. Through EMS, which is an included feature of the Windows and Handheld Shields, a modified version of the CMG Shield along with encrypted key material and policies are installed onto external media, allowing the security policies to travel with the data. Once installed on the media, the Shield enforces security policies and authentication on that media independent of its parent Windows or Handheld Shield. From that point on any data edited on or added to the media will be encrypted, even when the user is working on an UnShielded Windows computer or handheld device. There is no special media to buy and the encrypted data can be accessed via the same platforms supported by our Windows and Handheld Shields.

CREDANT FDE FOR WINDOWS, CREDANT FDE DRIVEMANAGER AND CREDANT POLICYSERVER

CREDANT FDE for Windows and CREDANT FDE DriveManager provide data protection, authentication, compliance, and centralized administration for Windows devices within your enterprise. Though both solutions provide exceptional FDE protection for your data, CREDANT FDE for Windows does so via software-based encryption while CREDANT FDE DriveManager protection is implemented via Seagate hardware-based encryption. Once either solution is installed, your Windows computers are protected with high-speed, whole device encryption. Both solutions are managed via the CREDANT PolicyServer, which provides a common interface and administrative console for all your CREDANT FDE protected Windows devices (Figure 2).

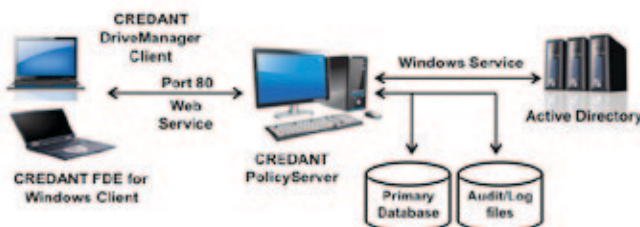


Figure 2. CREDANT FDE for Windows, FDE DriveManager and PolicyServer Architecture

CREDANT POLICYSERVER

CREDANT PolicyServer offers scalable, auditable, enterprise security so you can manage CREDANT's hardware-and software-based, FDE protection for Windows laptops and desktops from a single console. CREDANT PolicyServer includes the following, required components:

CREDANT PolicyServer

This is the primary management application that runs as a service and works with the MMC Snap-in to communicate with the CREDANT FDE for Windows and FDE DriveManager clients, the Microsoft Management Console (MMC) and the SQL Database.

CREDANT PolicyServer MMC Snap-in

The MMC is a component of the operating systems that provides system administrators and advanced users with a flexible interface through which they configure and monitor the system. The PolicyServer MMC Snap-in is a COM component that provides an interface to the MMC.

CREDANT PolicyServer Database Module

This installs the primary and log database tables and schema for an existing SQL Server. The primary database retains the encryption keys, group, user and device information and is the staging table for logs. The Log Database provides a repository for transactions such as user logins and user, group and device management. The Log Database is used for long-term storage and is managed by the administrator, who has the capability to search the stored data for trends, such as security violations.

CREDANT PolicyServer uses Web Services as the basis for enterprise management of users and devices as well as for security policy. It can be configured to run inside or outside the corporate firewall and all servers to client communications paths are encrypted. The SOAP-based Web Services are used to communicate policies, client encryption information, log files, and

CREDANT Encryption Solutions Overview

authentication information between the CREDANT FDE for Windows and FDE DriveManager clients and the CREDANT PolicyServer. The CREDANT PolicyServer components can reside on systems running Microsoft Windows Server 2003. Microsoft SQL Server 2000 and 2005, with the latest service packs, are supported. The SQL database may exist on the same machine as the CREDANT PolicyServer, on a separate system or as an instance in an existing database cluster. For complete system requirements see the product documentation.

CREDANT FULL-DISK ENCRYPTION WINDOWS CLIENTS

CREDANT FDE for Windows and CREDANT FDE DriveManager are the on-device components that enforce security policies whether a Windows computer is connected to the network or not. This ensures that all data remains protected on the Windows laptop or desktop, even if it is lost or stolen. The Windows FDE clients come in three varieties and support numerous platforms to help organizations extend their trusted environment and protect sensitive corporate data. The CMG External Media Edition Shield, described earlier in this paper, can be added to any of the clients described below to protect removable media used with the Windows computer.

CREDANT FDE for Windows (Software Encryption)

This client provides software-based, FDE for laptops and desktops running Microsoft Windows 7, Vista, and XP (32- and 64-bit). Security policies for this fully managed client are defined and managed via the CREDANT PolicyServer. The client is designed to provide comprehensive and simple security by encrypting every sector on the physical drive, including unused space. The CREDANT client then verifies the user has the appropriate credentials, via pre-boot authentication, before granting access to the device and its data. Broad authentication options provide users with a variety of identification methods, including fixed, PIN, smartcard, domain password Single Sign-On (SSO), etc. These

choices, which can be enabled or disabled by the administrator, offer flexibility to support the security requirements of any enterprise.

CREDANT FDE DriveManager (Hardware Encryption) - Managed

CREDANT FDE DriveManager software is designed to work with the Seagate Momentus self-encrypting 2.5" hard drives. Both 5400 and 7200 RPM drives are supported in laptops and desktops running Microsoft Windows 7, Vista, and XP (32- and 64-bit). Seagate DriveTrust technology implements a cryptographic service provider in hardware, including encryption, hashing, secure storage, decryption, digital signature and random number generating functions. The entire hard drive is encrypted instantaneously when the first user logs into the system, thus offering exceptional security and performance. Security policies for this fully managed client are defined and managed via the CREDANT PolicyServer. Before granting access to the system and protected data, the CREDANT client verifies the user has the appropriate credentials, via pre-boot authentication. Broad authentication options provide users with a variety of identification methods, including fixed, PIN, smartcard, domain password Single Sign-On (SSO), etc. These choices, which can be enabled or disabled by the administrator, offer flexibility to support the security requirements of any enterprise.

CREDANT FDE DriveManager (Hardware Encryption) - Standalone

This client provides the same features as the previous client and offers the same security benefits, but it is not centrally managed. Whether the client is managed or standalone is determined during installation. This is an ideal solution for small businesses, medical offices and individuals.

CREDANT Encryption Solutions Overview

FUNCTIONALITY

OVERVIEW

CREDANT believes that security solutions should be flexible enough to integrate seamlessly into a variety of environments, thus minimizing the impact on security administrators, IT, the help desk and end users. Encryption is a standard technology used to protect your intellectual property and reputation and to help you satisfy industry compliance regulations. It should enable your business, not get in the way. Once you are assured that the base encryption technology is implemented correctly and securely, which is generally proven via technology validating institutes like the National Institute of Standards and Technology (NIST), you can focus on the management and reporting built around each encryption solution to decide which is best for you. Often, needs vary, even within a single company so the best solution may actually be a combination of products. CREDANT's philosophy is to

offer you a diverse group of products and features so you can select the options that are right for you, rather than trying to force you to accept a single solution that may not exactly satisfy your needs.

This section will describe the wide range of features offered for the solutions we've presented so far (Figure 3). We can't cover every feature available in this one paper so we'll focus on those that organizations have told us are most important to them. If we've missed something that's important to you, please contact us so we can show you how one or more of our solutions can solve your security and compliance problems.

ENCRYPTION AND MANAGEMENT OPTIONS - HIGH LEVEL SUMMARY

CREDANT offers numerous protection options for your Windows, Mac OS X, removable media and handheld devices to ensure there's a solution for ev-

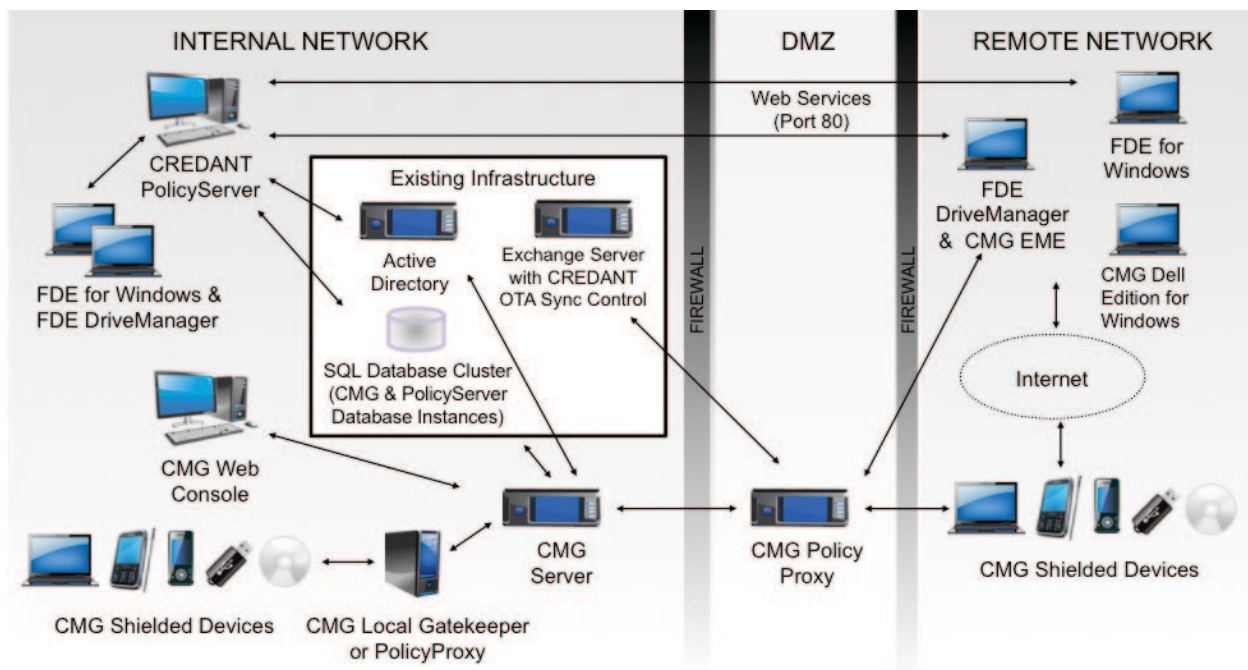


Figure 3: CREDANT Solutions can be deployed together as shown, or just install the pieces you need

CREDANT Encryption Solutions Overview

CLIENT NAME	MANAGEMENT	ENCRYPTION TYPE	ENCRYPTION PROCESS	ENCRYPTION ALGORITHM
CREDANT FDE for Mac	Managed via CMG Server	Full Disk Encryption	Software Encryption	AES 256 or 128 (policy defined by administrator)
CMG Enterprise Edition for Windows	Managed via CMG Server	Intelligent Encryption	Software Encryption	AES 256 or 128, Rijndael 256 or 128, 3DES or Blowfish (policy defined by administrator)
CMG External Media Edition for Windows	Managed via CMG Server	Intelligent Encryption	Software Encryption	AES 256 or 128, Rijndael 256 or 128, 3DES or Blowfish (policy defined by administrator)
CMG StandAlone Edition for Windows	Unmanaged	Intelligent Encryption	Software Encryption	AES 256
CMG Dell Edition Windows (Standalone)	Unmanaged	Intelligent Encryption	Software Encryption	AES 256
CMG Dell Edition Windows (Enterprise Edition)	Managed via CMG Dell Edition Server	Intelligent Encryption	Software Encryption	AES 256 or 128, Rijndael 256 or 128, 3DES or Blowfish (policy defined by administrator)
CMG External Media Shield	Managed via CMG Server (through parent Windows Shield)	Intelligent Encryption	Software Encryption	AES 256 or 128, Rijndael 256 or 128, 3DES or Blowfish (policy defined by administrator)
CREDANT FDE for Windows	Managed via PolicyServer	Full Disk Encryption	Software Encryption	AES 256
CREDANT FDE DriveManager	Managed via PolicyServer or Unmanaged (install option)	Full Disk Encryption	Seagate Hardware Encryption	AES 128

everyone from the small office or individual to very large enterprise companies. To help clarify this information before you read more about the features and benefits of each, the table above lists all the CREDANT clients for laptops, desktops and removable media with some high level information about each. More details on all these clients are provided throughout this paper.

TECHNOLOGY VALIDATIONS

CREDANT believes that third party validations are a great way to show that our core technology is sound and thus all our products have attained those validations that are most relevant to the technology.

CREDANT has achieved Federal Information Processing Standard (FIPS) 140-2 Level 1 validation for the CREDANT Cryptographic Kernel (CCK). This CCK is

CREDANT Encryption Solutions Overview

used across all CREDANT Mobile Guardian supported platforms. The CREDANT implementation of the AES, 3DES, SHA-1, HMAC-SHA-1, and RNG algorithms are all FIPS approved. The certificate is available online at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp584.pdf>. We are currently in the process of updating this to FIPS 140-2 Level 2. CREDANT Mobile Guardian has also been granted Common Criteria EAL 3 validation and the UK Government quality CESG Claims Tested Mark (CCTM), (formerly the CSIA Claims Tested Mark) which is awarded by CESG, the National Technical Authority.

CREDANT FDE for Windows has attained FIPS 140-2 Level 1 and Level 2 and is National Institute of Standards and Technology (NIST) certified and approved. Common Criteria EAL 4+ validation for this product is currently in final review.

CREDANT DriveManager and Seagate have attained FIPS 140-2 Level 1 and Level 2. Validation has also been granted by the National Institute of Standards and Technology (NIST) (in review by NIST) and this product is NSA approved (NSTISSP-11 Certifications).

CENTRALIZED ADMINISTRATION AND PRE-DEFINED POLICY OPTIONS

Meeting the diverse security needs of different organizations is an area where CREDANT excels. Individuals or small companies need a simple, pre-configured solution that doesn't require a security team to administer while larger, more complex organizations require flexible policy options with central administration and compliance reporting. CREDANT has solutions for all these needs and provides an easy upgrade path as companies grow and their needs change.

SMALL OFFICE, MEDICAL OFFICE OR INDIVIDUAL

While smaller organizations need the same world-class security as a large enterprise company, they generally prefer a simple, "set and forget" solution and don't need the flexibility offered by centralized

management and reporting. For this type of organization, CREDANT offers a variety of solutions that allow you to take advantage of our security expertise via pre-configured policy. The best options for this environment include CMG StandAlone Edition for Windows, CMG Dell Edition Windows, CREDANT FDE for Windows and CREDANT FDE DriveManager. These options scale well for Small to Medium Business where security is important, but resources to manage solutions are limited.

A variety of install options support environments with or without IT administrators for all these solutions. 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. The Dell Edition Shield can also be ordered pre-installed with your new Dell PC purchase. With a few exceptions, all policy settings are pre-configured to simplify installation and can't be changed unless the solutions are later migrated into a CREDANT managed environment.

CREDANT FDE for Windows (software encryption) and CREDANT FDE DriveManager (hardware encryption) can both be managed via CREDANT PolicyServer. FDE DriveManager can also be installed in a stand-alone, or unmanaged, mode. Even in their managed configuration, the simplicity of full disk encryption makes these great options for individuals, small businesses or medical offices where security resources are scarce or aren't available at all. After some basic system preparation, such as defragmenting the hard drive, FDE automatically and transparently encrypts every sector on the hard drive. There is no advanced security knowledge needed to implement these solutions and minimal configuration is required. There are no complex policies to navigate and no decisions have to be made about what data to encrypt.

To install FDE DriveManager in unmanaged mode, simply double click the installation executable on the

CREDANT Encryption Solutions Overview

system to be protected, enter a username and password for the end user who will be working on this system and shut down the computer when the installation completes to allow the software to lock the system. The username should match whatever the user currently uses to login either locally or via the domain. The initial installation password is changed when the user logs in for the first time after DriveManager is installed to ensure only they know the password. This allows an administrator to install the software, if desired, without knowing the end user's password. From that point on the user is prompted to log into the system as soon as it boots instead of just when Windows starts. This ensures that only authorized users can access the encrypted drive. Encryption keys are generated uniquely for each system during the installation to lock that drive to a specific PC. Because this client encrypts data via hardware, the entire drive is encrypted instantaneously as soon as the end user logs in the first time after DriveManager is installed. As users create, edit, or transfer files to their computer, the Seagate hard drive automatically and transparently encrypts that data without requiring any action by the user. See the next section for details about managing the Windows FDE solutions via CREDANT PolicyServer.

The CMG StandAlone Edition for Windows and CMG Dell Edition Windows Shields install with pre-configured encryption policies and require no Enterprise Server or console of any type. These Shields ensure the security of sensitive data inside or outside the corporate network for domain and non-domain computers. The Dell Edition Shield can be ordered pre-installed, directly from Dell with your new Dell computers for an even easier to deploy solution.

There are a number of advanced configuration installation 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. Encryption keys are generated uniquely for each system during the installation to lock that drive to a specific PC. Organizations also using CMG Enterprise Edition can configure their StandAlone Edition for Windows Shields to automatically escrow those encryption keys to the CMG Server. For environments without a CREDANT Server, the Shield prompts the user to escrow their encryption keys to a location independent of the protected system before data is encrypted.

Once encryption keys have been escrowed, the software-based 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 CREDANT Shield automatically and transparently encrypts that data without requiring any action by the user.

MEDIUM TO LARGE ENTERPRISE

Because they are part of CREDANT's overall solution, the small office options described in the previous section are also great for enterprise organizations that support an affiliate model where non-employee or contractor computers have access to sensitive corporate data. These unmanaged solutions allow the organization's data to be protected on laptops and

CREDANT Encryption Solutions Overview

desktops that are in the corporate domain, in another domain or not part of any domain. They are also valuable for rapid deployment to protect corporate or affiliate systems, especially given that they can later be migrated to be part of our fully managed solutions.

Windows computers, Mac OS X systems, handhelds and removable media protected by CREDANT's centrally managed client software offer exceptional scalability and flexibility to address the needs of any medium to large enterprise. Management and reporting for these solutions are provided via the CMG Server and CREDANT PolicyServer. Both management solutions offer scalable, auditable, cross-platform enterprise security for all your mobile data.

CREDANT PolicyServer

The CREDANT PolicyServer is a powerful, MMC-based application that allows an administrator to enable or disable CREDANT products, define security policy parameters, and manage users, groups, and devices (Figure 4). Via PolicyServer, an administrator can modify authentication and recovery policies, configure pre-boot authentication and manage users or groups. Enterprise-level policies provide a baseline that serves as the template for all new groups and therefore should be fairly lenient. Group-level policies can be defined to further enhance security by fine-tuning policies for select devices, groups or individuals.

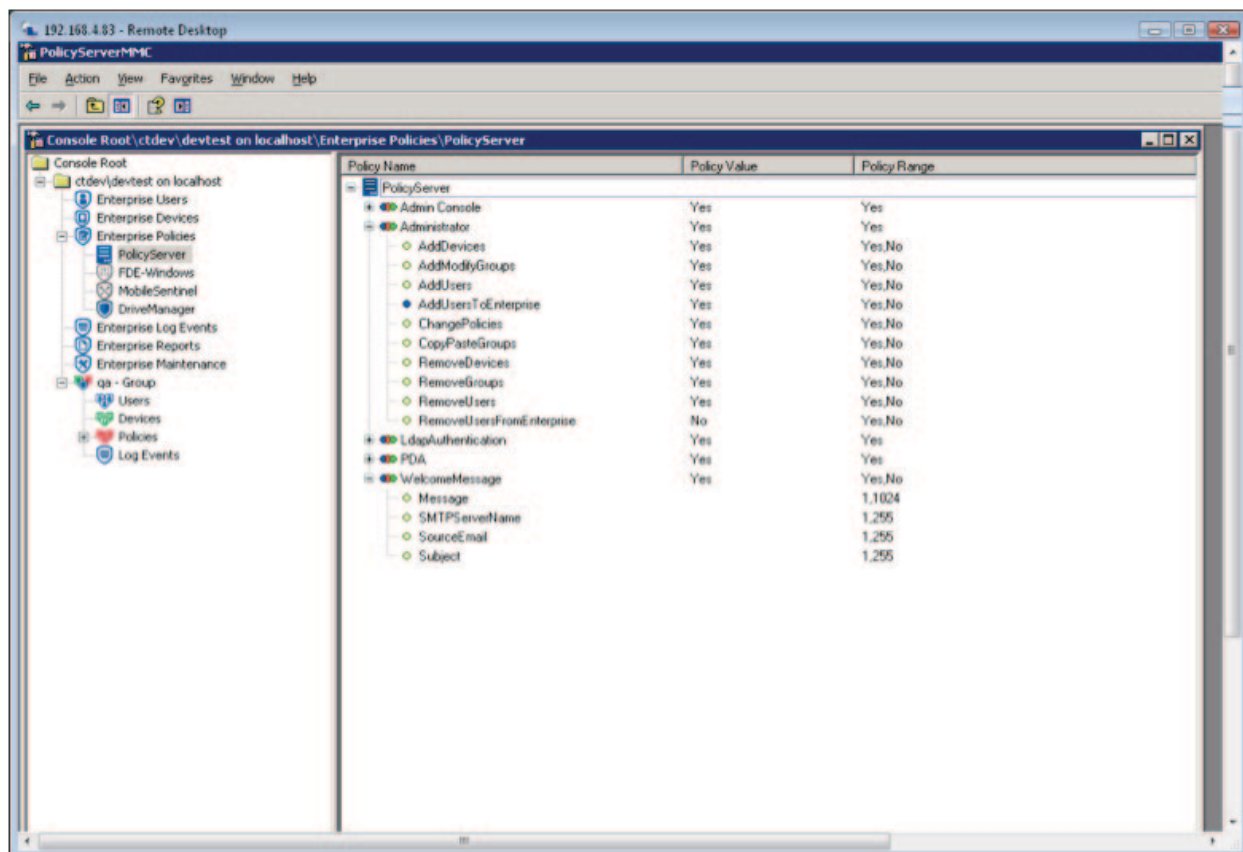


Figure 4: CREDANT PolicyServer Interface

CREDANT Encryption Solutions Overview

Because the PolicyServer manages the Windows FDE products, there is no need to configure data encryption, but policies can be configured to control a number of options. Some important policies that can be configured include:

AllowedCharacter Types

Specify whether passwords can contain alpha, numeric, special or a combination of characters. This is one of many policies to control password strength, forced resets, and other pre-boot authentication options.

Allowed Authentication Methods

Specify the authentication methods that can be used. Options include Fixed, Smartcard, Domain Single Sign-On, and PIN, which are described further in the Authentication section of this paper.

LockDeviceTime Delay

Forces the device to lock for a specified number of minutes if the user fails pre-boot authentication the number of times allowed per policy.

LocalLogin Multiple Choice

Specify the action to be taken when the device locks due to failed authentication. Actions are Erase (all contents on the device will be wiped), Remote Authentication (require the user to perform a remote authentication) or Time Delay (lock the device for a time specified via policy).

AccountLockout Period and AccountLockout Action

These policies work together to specify the action to be taken, if the protected device has not communicated with the PolicyServer in X days. Actions are Erase

(all contents on the device will be wiped), Remote Authentication (require the user to perform a remote authentication) or Ignore (do not take any action).

DeadManSwitch

Specify a sequence of characters that, when entered, will destroy the device.

CMG Server

The CMG Server provides a central, web-based interface for security policy definition and management, real-time device inventory, and continuous reporting of security status for policy compliance (Figure 5). This management server can be accessed via standard web browsers, including Internet Explorer and Firefox, and provides a variety of benefits including:

- › A single, secure administration interface to manage security across disparate mobile devices
- › Default security policies that can be easily adjusted to align data security to the type of user, device and location
- › Automated and transparent archiving of encryption keys to enable Day Zero data recovery
- › Inventory management and reporting
- › Self-service and administrator assisted device recovery in case of authentication failure
- › Enterprise database integration for a scalable and reliable solution

CREDANT Encryption Solutions Overview

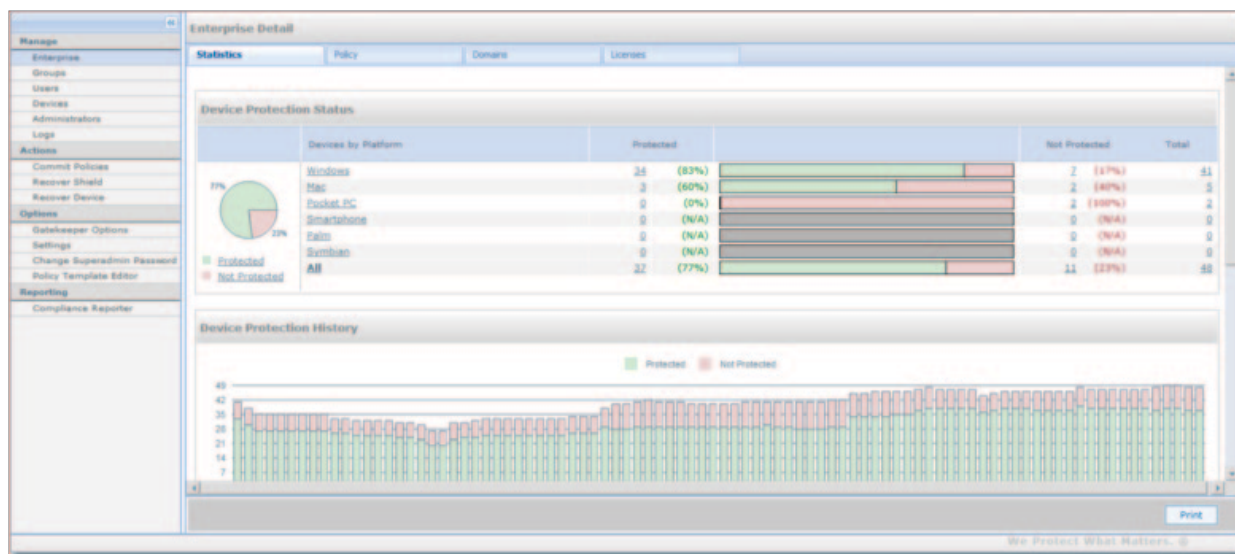


Figure 5: The CMG Server home page provides current and historical device protection summaries

The CMG Server web UI enables configuration of CREDANT's Intelligent Encryption. This patent-pending encryption technology requires more configuration than FDE, but provides fine grained control while closing the security gaps created by file/folder based solutions since all sensitive data is encrypted automatically, with no user interaction.

Encryption rules can be as simple as defining encryption for entire drives or partitions, including program and OS files, or as detailed as your environment dictates (Figure 6). CREDANT's Intelligent Encryption applies a "defense in depth" approach, consisting of the following encryption layers, each implement via different encryption keys to ensure data privacy, even within your organization:

Common encryption automatically encrypts any type of data written to any fixed disk, regardless of file type or where that data resides. Data encrypted via the Common Encryption Key can be accessed by any managed user with a valid login to the system. This,

combined with User Level Encryption and SDE, provides an excellent option for medical offices or other environments where systems are shared by multiple users, but certain data should not be accessed by all users.

User encryption automatically enforces encryption of user specific data ensuring that local administrators and other users with machine access cannot access another users' sensitive data. For example, if the CFO's data is encrypted via the User Level Encryption key, an outsourced IT worker can log into the system for maintenance, but will not have access to confidential CFO data. A unique encryption key is created for every managed user on the system to ensure data privacy, even for shared systems.

File type encryption automatically encrypts all new and previously created files of a specified type (or multiple types) regardless of how they are created or where they are stored on the hard drive. This process ensures protection of legacy data, and temporary and

CREDANT Encryption Solutions Overview

swap files that may not be covered by other encryption policies.

Application data encryption automatically enforces encryption of any data written by specified applications, to protect against user error or malicious renaming of a file type that could leave data exposed. This patent pending approach requires no modification to the application and is transparent to both the application and the user.

External Media encryption provides automatic and portable encryption of all media to ensure the security of sensitive data as it flows beyond the protected corporate computer boundary. EMS is described in depth in another section of this paper.

System Data Encryption (SDE) provides a simple, global catch-all group of policies that encrypt any data not already encrypted by other CMG policies, thus making it easy for customers to prove that all sensitive data on the hard disk is encrypted. The default SDE policy encrypts all data not yet encrypted by other policies, including OS and Program Files, with the exception of some system files required to boot the system. This ensures user transparency without impacting existing IT operational processes. Encryption keys are derived from unique operating system and hardware information, allowing the keys to be automatically regenerated to unlock SDE-encrypted data every time the system boots. This process ensures access to data is tied to the operating system and hardware to thwart off-line attacks and to lock the hard drive to a particular system.

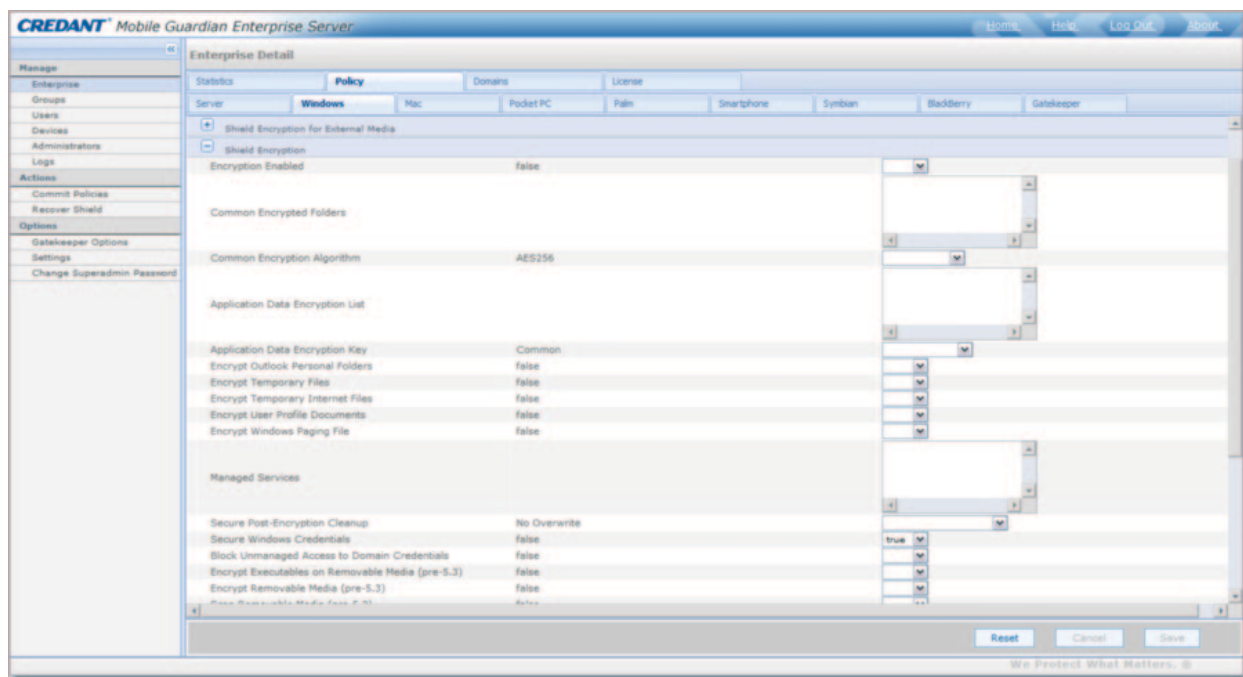


Figure 6: CMG Server configuration of Intelligent Encryption Policies

CREDANT Encryption Solutions Overview

AUTHENTICATION

Mandatory authentication is a critical component of any security system, as the authentication process establishes a user's unique identity. All CREDANT encryption solutions require and enforce authentication, though the methodology differs somewhat by client and OS. CMG Shield for Windows integrates with the existing domain login process so the same credentials that allow access to the OS determine what encrypted data may be accessed by a user. The Shield for Mac prompts for domain authentication only once as each unique Mac OS X user authenticates. This process associates domain users with their non-domain Mac systems and local user accounts, enabling enhanced compliance reporting without requiring changes to the Mac OS X configuration. The CMG EMS client implements and enforces local authentication for protected media, since there is no native authentication, domain or local, on removable media. The CREDANT FDE for Windows and FDE DriveManager clients encrypt all OS, program and user data with a single key, at the sector level, so authentication must occur before the OS starts. For these clients, Linux-based pre-boot authentication is implemented to ensure only authorized users can access the encrypted hard drive.

All CREDANT solutions offer seamless, standards-based integration with authentication technologies, like RSA SecurID, smartcards, Common Access Cards (CAC), Dell contactless card readers and biometrics so organizations can continue using their multi-factor authentication method of choice regardless of which encryption solutions they select. CREDANT solutions also integrate with enterprise directories like Active Directory (AD). The CMG Server integration with Active Directory provides a central, web-based interface for security policy definition and management against existing AD groups and users. Read-only integration with enterprise LDAP directories enables enterprise, domain, group, or individual user level security poli-

cies. CREDANT PolicyServer's directory integration enables domain single sign-on so administrators do not have to manage separate pre-boot authentication passwords.

CREANT FDE for Windows and FDE DriveManager authentication services are performed when a device is powered on. When a valid user enters their credentials, the user is then granted access to the PC, its resources, and all data stored on the PC. No access is granted if a user is determined to be invalid. CREDANT's role in authentication for the Seagate Momentus self encrypting drives may not be as obvious as it is for our software-based FDE solution, though it's equally important. Without CREDANT, when encryption is implemented in hardware by the Seagate SED, the door is always locked, but the key is left in the lock for anyone to open. When CREDANT DriveManager is installed on these drives, it removes the key from the lock; only providing it to users once they have authenticated to CREDANT FDE DriveManager.

CREANT FDE for Windows and FDE DriveManager authentication options are configured and enabled or disabled via PolicyServer. All options below are followed by the existing OS login, except the Active Directory (AD) Domain Password option, which combines the pre-boot and OS logins.

- › **Smartcard (CAC/PIV)** - A smartcard often looks like a credit card in size and shape, but inside it contains a memory chip (microprocessor) that has the ability to store large amounts of data. The microprocessor is able to carry out certain functions to interact intelligently with a smart card reader, such as multi-factor authentication. CREDANT supports a broad range of smartcards, including RSA SecurID and CAC.
- › **AD Domain Password** - This single sign-on (SSO) option allows the user to authenticate to the CREDANT client and the OS in a single

CREDANT Encryption Solutions Overview

step, with their existing domain credentials. This significantly reduces the learning curve for end users and simplifies administration by enforcing the current Active Directory login policies. A voluntary domain password change can be made through the CREDANT FDE for Windows application during the authentication sequence or from within Windows. Numerous methods are implemented by the CREDANT client to make sure any password changes are synchronized between the domain controller, Windows and the CREDANT pre-boot authentication.

- › **Fixed Password** - A Fixed Password is generally entered on a keyboard and is composed of letters, numbers, and special characters. Fixed passwords are the most common and traditional method of user identification. The fixed password is chosen by the user and can be almost anything. However, administrators may place restrictions on fixed passwords to ensure they are not easily compromised. This method can be used alone or as the basis for our domain SSO authentication.
- › **PIN** - This Personal Identification Number (PIN) is similar to fixed password, but only numeric characters are used.

If the user fails to successfully authenticate, he is prompted to re-enter the credentials. Consecutive unsuccessful authentications trigger responses, as determined by the system administrator, which include:

- › **Temporary account lockout or Hard account lockout** - The user account is locked and no authentication attempts can be made until the lockout time is passed. The user can contact the system administrator for assistance or use Self Help to unlock the PC.
- › **Erase** - To prevent the data from being compromised, the system administrator may configure

the PC to automatically remove all data after a specified number of unsuccessful login attempts are made on a device.

To help users avoid these responses in case of forgotten login credentials, the administrator can also enable self-service password resets and remote password reset. The first self-service reset option allows the user to provide answers to questions defined via policy. If the user requires a password reset, he must select and correctly answer one or more questions as defined by policy. Users are also given the option to change their answers to any of the questions each time they log into the system. For the second self-help option the user must have email access via another device. A challenge response is emailed to the user. Once received, the user selects Reset Help, enters the challenge response in the "Response" field, clicks Continue and is then presented with the Change Password function. If desired, the administrator can require both self-help options be completed before allowing a password reset. There is also a remote help desk option that allows the help desk to provide a soft or hard token password reset for users who can't complete the self-help reset for some reason.

CREDANT Mobile Guardian integrates with the existing domain or local login so with the exception of EMS, there is very little to manage around authentication. Once the CMG Server is configured to manage a domain or domains, users and user groups can be imported, either manually or automatically as users log into protected devices for the first time. Once the CMG Server is aware of AD groups or users, it is automatically updated of any changes to membership via the domain controller. This information is reflected in the CMG Server so there's no need to manually update groups to match the directory. This greatly simplifies policy administration and authentication. In addition to devices allowing access to data based

CREDANT Encryption Solutions Overview

on the current logged in user, CMG Administrators authenticate to the CMG Server with their domain credentials. Many organizations create a CMG Administrator group in AD for each CMG Administrator role (Help Desk Administrator, System Administrator, Security Administrator, Log Administrator, Account Administrator, Forensic Administrator, Report Administrator, Report Owner Report User, or Super Administrator) and then by simply moving users in or out of those AD groups, administrator access to the CMG Server is granted or removed.

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 web 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 their Shielded computer or, if the user is no longer with the company, the CMG Admin can recover the encryption keys. Examples of EMS authentication policies available to administrators are provided later in this paper.

INTEGRATION AND INTEROPERABILITY WITH EXISTING IT INFRASTRUCTURE AND PROCESSES-

CREDANT solutions were designed to work in today's complex and diverse enterprise environments. Security solutions are not always managed by the same teams who manage networks or systems so it's just as important to reduce the burden that security places on IT as it is to minimize end user impact.

As described in the previous section, all CREDANT solutions integrate seamlessly with directory infrastructure like Active Directory. This allows administrators to leverage the directory infrastructure already in place, which significantly reduces the challenge of implementing security that fits your business. For example, the CMG Server provides a simple interface for designating which domains the Server and clients should integrate with (Figure 7). This seamless integration with Active Directory provides the ability to apply policy by AD users or groups and to support the CMG Shield integration with the Windows login. AD integration also enables domain SSO for clients managed via CREDANT PolicyServer.

CREDANT Encryption Solutions Overview

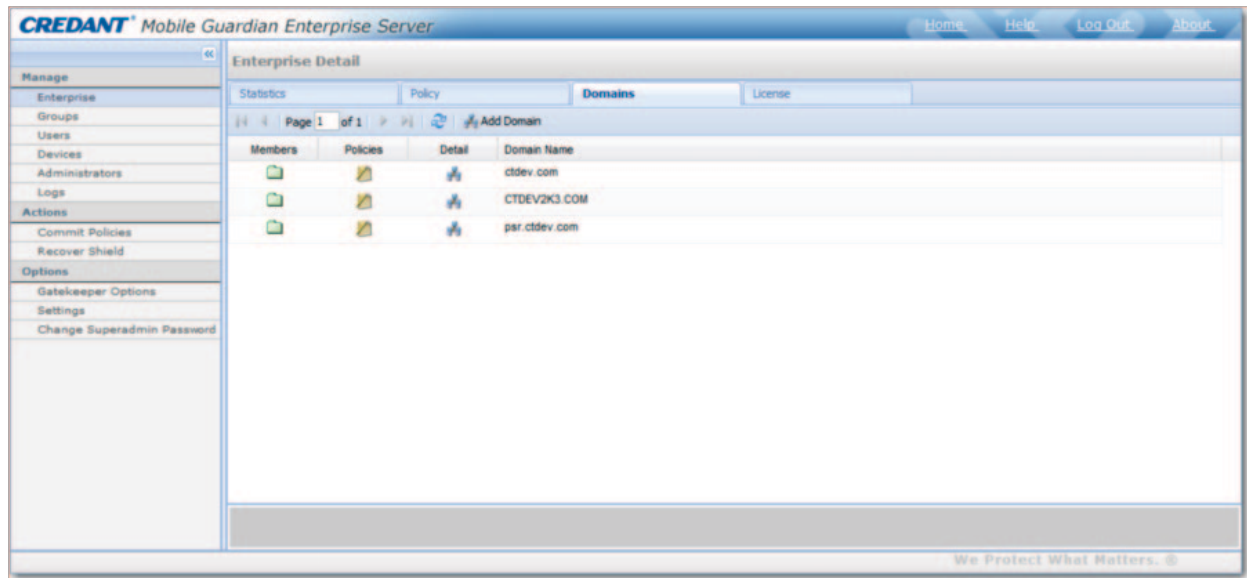


Figure 7: Interface for adding managed domains to CMG

The CMG Server also supports tight integration with Forensics applications like Guidance EnCase and AccessData Forensic Toolkit (FTK). Forensics software is used by many CREDANT customers to investigate security incidents, internal HR investigations, and to back up litigation requiring electronically stored evidence. Forensics software applications search, collect, and analyze digital information in a forensically sound way so it's important to allow them to access encrypted data without changing that data and thus make it inadmissible in court. At the same time, encryption keys must be made available to the Forensics application without risking the security of those keys and the data they protect. Data decryption is on the fly so there's no need to decrypt the hard drive during an investigation. Both off-line and on-line investigation workflows are supported.

Software deployment is an area that IT typically manages via a variety of tools, like Microsoft System Management Software (SMS). It is important to allow IT to use the tools they are familiar with so CRED-

ANT clients utilize MSI and other standard installation technology. This allows the use of existing software deployment tools to distribute and script silent installation of all clients without the need to purchase or learn a new software deployment tool. In addition to full support for software distribution tools, CREDANT's solutions allow the use of Patch Management tools, often with no changes. In the rare case where small adjustments are needed, CREDANT provides simple to use tools that enable your existing process, while ensuring that data remains encrypted and protected.

USABILITY

In many cases, the usability of an encryption solution is evaluated by how well hidden it is from the end user. This means that data must be encrypted automatically and without impacting end user productivity. End users should be able to use their systems as they always have and the security of data should not require that files be saved in a specific location to ensure they are encrypted. All CREDANT solutions,

CREDANT Encryption Solutions Overview

whether they are implemented via Intelligent Encryption, Full Disk Encryption, software encryption or hardware encryption satisfy these requirements.

While many organizations still prefer to hide encryption from their users, there's an emerging trend to reduce that transparency in ways that give the end user some sense of control without negatively impacting data security. Many companies want features that allow them to use encryption as a teaching tool. In some cases, employees are more likely to embrace security technology if they feel they have some control and thus they are part of the solution. In addition to the self-service password recovery offered by both CREDANT PolicyServer and CREDANT Mobile Guardian, CMG offers usability policies that define when to enforce updated policies, Encryption sweep behavior, and what information and options should be shown to the user (e.g. via a CMG Shield tool tray icon). There are also policies to configure one or more delays before forcing a reboot or logoff, when needed to implement new policy. This ensures that a policy update can occur at any time without disturbing end users. These policy options are all controlled by the CMG Administrator. The following are some examples of CMG Windows features that can be enabled or disabled so administrators can find the right level of transparency for their end users (Figure 8):

Allow Encryption Processing Only when screen is locked - Allows the CMG administrator to force encryption sweeps to:

- › Occur only when the client computer is locked (True)
- › Occur at any time (False)
- › Allow the user to control whether sweeps can occur at any time or only when the screen is locked (User Optional). The "Allow encryption processing only when screen is locked" Shield icon menu option will be presented to the user if this policy option is selected

Hide Policy Viewer - Allows the CMG Administrator to hide/enable the Shield policy viewer option that's normally available via the CMG tool tray icon context menu (Figure 9). Administrators can also hide the entire CREDANT tool tray icon if desired.

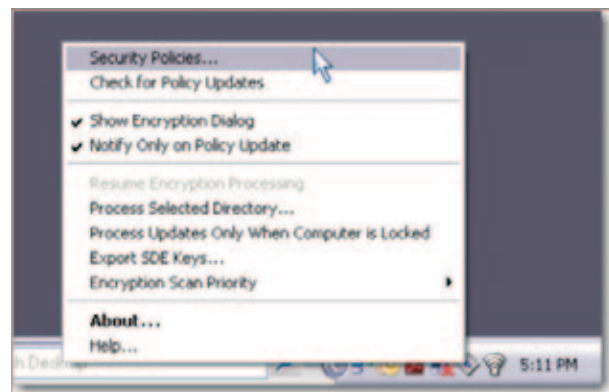


Figure 8: CMG Tool Tray icon with end user controls

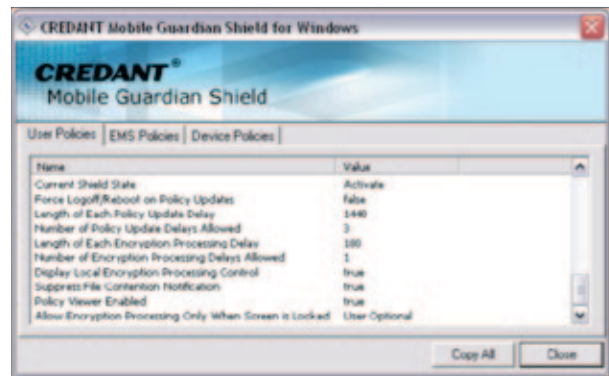


Figure 9: CMG Shield Policy Viewer

CREDANT Encryption Solutions Overview

REMOVABLE MEDIA PROTECTION

CREDANT External Media Shield (EMS) ensures security and privacy of sensitive data as it flows beyond the protected computer, guaranteeing exceptional data mobility while protecting data, even if media is lost or stolen. When the administrator enables EMS for an enterprise, individual user or group of users, the EMS client is placed on removable media inserted into the 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. Password strength is enforced per administrator-defined policies. EMS encryption applies to all media devices connected via USB, FireWire, Compact Flash bus, Secure Digital bus and other external ports, even if Windows designates the device as a fixed disk.

In addition to the EMS client, encryption keys and policies, an installer is also copied to the media to enable a clientless access to the media or a one-time client install so users can securely read and edit encrypted data, even from a computer not protected by CREDANT. This access to encrypted external media from "UnShielded" (unprotected by CMG) computers can be disabled by the administrator via policy if desired. Unlike other approaches to external media encryption, EMS supports two modes of data access, depending on the state of the Windows system. When protected media is inserted into another CREDANT protected computer, the user is prompted to enter their media password. Once authenticated, they work with the media as usual and data is automatically and transparently encrypted as it is written to the media. If EMS protected media is inserted into an unprotected computer and the user has administrator privileges, 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 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).

Key examples of EMS encryption policies available to administrators via the CREDANT Mobile Guardian Console 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 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, but the user won't be able to work with encrypted data via any unShielded computer. This is useful if you want to keep users from moving corporate data to home or public kiosk computers.

EMS Access to UnShielded Media

Allows the administrator to control what an end user is allowed to do if they choose "No" when prompted to Shield unprotected media:

CREDANT Encryption Solutions Overview

Block - Prevents any read or write access to Un-Shielded media

Read-Only - Users can read or move data from Un-Shielded media to the protected laptop or desktop, but can't move data from the protected computer to the unprotected media. This option 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.

Full Access - Users can decide which media to encrypt and are allowed full read/write access, even to media they choose not to Shield.

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 Alpha Characters Required in Password and EMS Numeric Characters Required in Password

These two policies help control and enforce password complexity. Administrators can set EMS password policy to match their domain password policy to ease end user adoption or they can set EMS policy slightly different from the domain password policy if they want to ensure that users don't set the same password for media that they use for domain access.

EMS Number of Characters Required in Password

With this policy, the administrator can define from 1-40 as the minimum number of characters required in the EMS password.

EMS Password Attempts Allowed

The number of times a user can attempt to enter the correct EMS password for a piece of media before having to call the help desk for a recovery code, with valid values from 1-10 attempts.

EMS Access Code Failed Message

A String of 5-500 characters is used to create a message to the end user when they fail authentication and are placed in recovery mode. This administrator configurable message should direct the user to contact their help desk for a recovery code following failed authentication. Administrator assisted recovery restores access to the encrypted media in case of forgotten authentication credentials, even when the end user is disconnected from the corporate network.

EMS Access Code Failure Action

This defines what happens if the end user or an attacker enters invalid recovery codes after failing authentication the number of times allowed.

Apply Cooldown, Cooldown Time Delay and Cooldown Time Increment

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 a Shielded 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 so it is an excellent way to prevent unauthorized access to corporate data.

CREDANT Encryption Solutions Overview

AUDIT AND COMPLIANCE REPORTING

An important aspect of any security system is the ability to evaluate the system's status through the use of current and historical information in both detailed and graphical formats. CREDANT provides extensive compliance reporting options via the CMG Server, CREDANT PolicyServer and CREDANT Compliance Reporter. Our enterprise database records system activities and makes them available to these products for a broad range of configurable reporting options. CREDANT tracks changes made to policies, successful/failed login attempts, list of removable media used in protected systems, which media was Shielded and which was not, device inventory, encryption failures

and much more information about your CREDANT protected devices and data. Information is maintained in the CREDANT database to be displayed in audit logs or in reports. Reports can be scheduled or created on-demand in a variety of formats, including CSV for import into other tools. Exact details vary for the different reporting options.

Pre-defined reports can be reviewed to provide an accurate assessment of your environment (Figures 10 and 11) or report templates can be customized and saved (Figure 12) to ensure you have the exact information you need in the format you are most comfortable with.

CREDANT [®] Mobile Guardian Enterprise Server								
Device Detail for: SnowyMacPro.G87233FLUQ2								
<table border="1"> <thead> <tr> <th>Properties</th> <th>Policy</th> <th>Shield</th> <th>Shield users</th> <th>All</th> </tr> </thead> </table>				Properties	Policy	Shield	Shield users	All
Properties	Policy	Shield	Shield users	All				
Properties								
Item	value							
Battery remaining	<Not available>							
Memory (MB) available/total	115 / 5120							
OS / Version	Mac OS X 10.6.3 / 10.6.3 (10D573)							
Processor	2.66 GHz Dual-Core Intel Xeon							
Serial number	G87233FLUQ2							
Shield state	Shielded							
Unique ID	SnowyMacPro.G87233FLUQ2							
Effective policies	[site]							
Shielded								
Item	value							
Category	MAC							
Policy Proxy group	CHGRENOTE							
Last Gatekeeper Sync	<Not available>							
Recovery ID	SCPG38DD							
Version (core/edition)	6.7.1.23627 / 6.7.1.23627							
Shielded users								
User	Last successful login	Last unsuccessful login						
Paul.Wasmund2 (wasmund2@stdev.com)	<Not available>	<Not available>						
Paul.Wasmund (wasmund1@stdev.com)	04/21/2010 12:13:54 CDT	<Not available>						

Figure 10: CMG Server Detail Report on Shielded Mac OS X System

CREDANT Encryption Solutions Overview

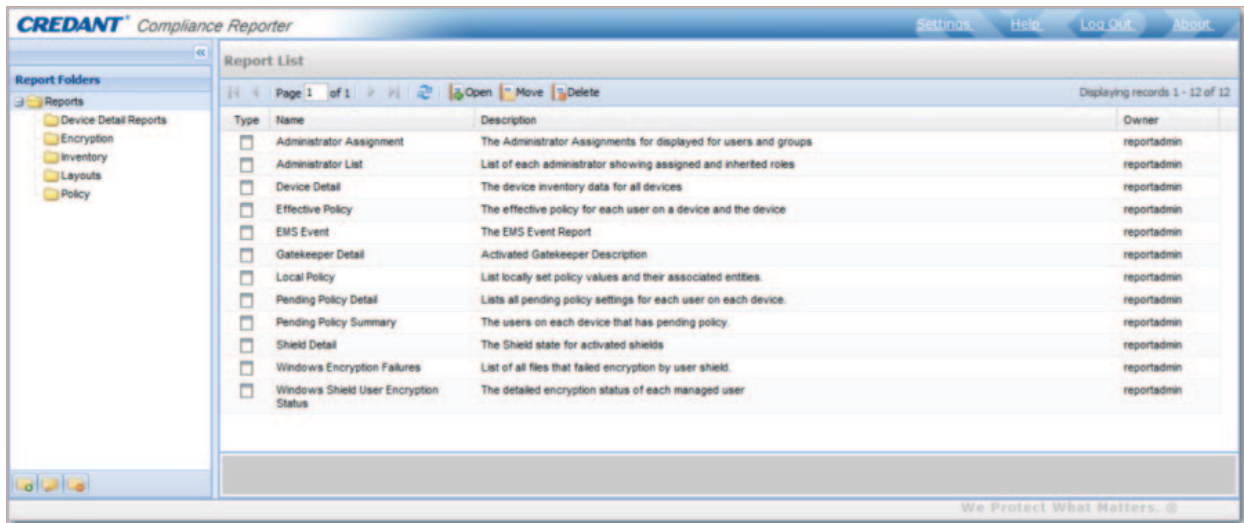


Figure 11: CREDANT Compliance Reporter Pre-Defined Reports

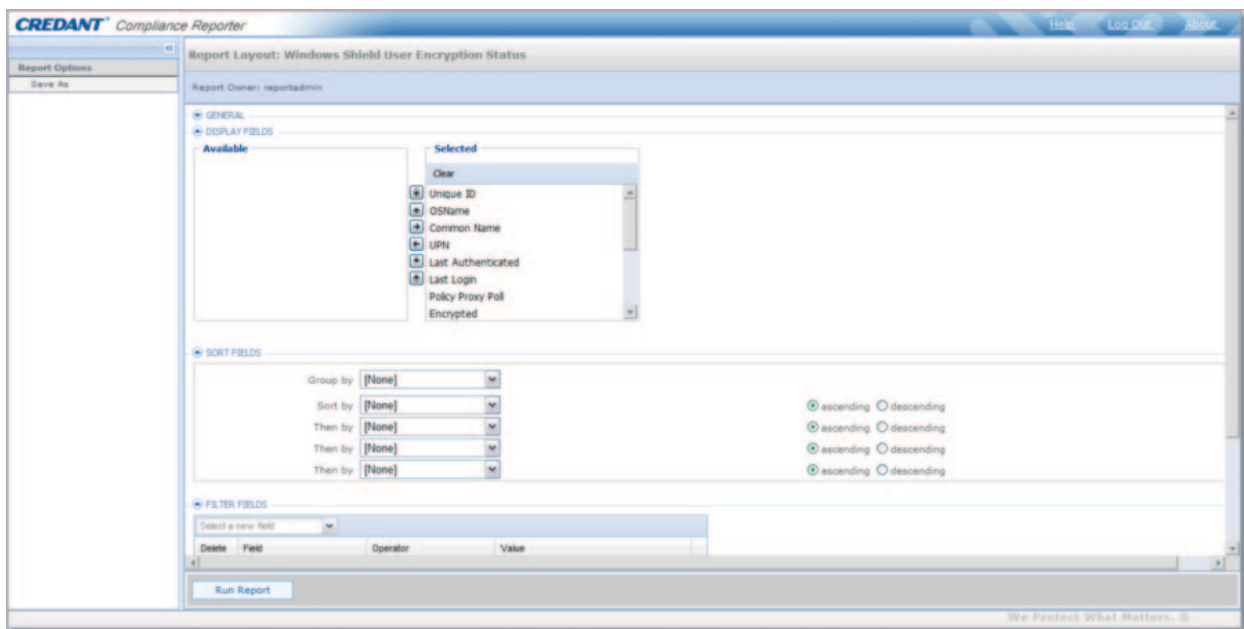


Figure 12: Creating a Customized Report Template from an Existing Report

CREDANT Encryption Solutions Overview

Due to ever increasing regulatory compliance requirements for data protection, encrypting data is not enough. In order to meet many of the mandates, you must encrypt the data and have the reporting and auditing capabilities to prove that the sensitive data is protected as required, especially if a device is lost or stolen. CREDANT provides the management and reporting capabilities to meet regulatory requirements and to cover everything you need to manage your CREDANT protection, including:

- › CREDANT Client Versions details to help track which versions of CREDANT software your clients are running. This is especially helpful as you upgrade clients and for environments with a variety of CREDANT protection options.
- › Device inventory provides details on OS, battery life, Shielded users and other hardware and software details about your protected computers and media.
- › Effective Policy reports help you verify exactly which policies are active on your protected devices. This is a great way to verify that systems have received policy updates and to track down systems that may not have the most recent policies in use.
- › The Encryption status of protected devices is available in a variety of formats so you can be sure of when encryption occurred.
- › Devices that are not Fully Encrypted can be reported on, including details about encryption failures for specific files.
- › Devices that have not communicated with the CREDANT management servers in "x" days can be identified via reports so you can take action to address any communications problems that may prevent the devices from receiving updated policies.

- › Reports are available for all devices and the last user to have logged into them. Reports are also available by user that show how many and what types of protected devices they are using.

In addition to an unending variety of reports, event logs track administrator access and policy change details by administrator, device access attempts, system errors and many other details. Administrators can filter logs via specific search criteria and then display the information in the CMG Server or CREDANT PolicyServer.

CREDANT BENEFITS

CREDANT solutions all provide automatic and transparent data security without requiring user interaction. Security can be completely transparent to end users, while CREDANT also provide options that allow companies to use security technology to educate their users without putting data at risk. Some benefits are specific to a particular solution, including:

- › Instantaneous encryption with zero performance impact (CREDANT FDE DriveManager)
- › Encryption of all data on the hard drive with no need to define granular encryption policy (CREDANT FDE for Mac, CREDANT FDE for Windows, CREDANT FDE DriveManager)
- › Layered encryption with different encryption keys by user and type of data to provide data privacy, and to ensure that users can only access their data, even when they share computers (CMG Enterprise Edition for Windows, CMG Stand-Alone Edition for Windows and CMG Dell Edition Windows)

CREDANT Encryption Solutions Overview

- › Seagate DriveTrust technology and CREDANT System Data Encryption lock encrypted data to the hardware to prevent unauthorized data access if the drive is removed and installed in another system.
- › Integration with CREDANT Compliance Reporter and the ability to import AD user and group membership and to keep that information synchronized automatically as changes are made in AD (CMG Server)
- › Web-based Management (CMG Server)
- › Ability to configure automatic deletion of data and to force a system to lock for Windows computers that haven't contacted the management system in a specified number of days (CREDANT Policy-Server)
- › Tight integration with MMC for a powerful management solution (CREDANT PolicyServer)
- › Superior flexibility and interoperability with the Windows login and transparency for the user
- › Protection of all sensitive data on internal drives regardless of where it is stored and with no user action required
- › Data on an encrypted drive is only accessible when the encryption key is enabled through a valid password. If the encryption key is changed or eliminated, all protected data is instantly rendered inaccessible. Technicians can then safely repurpose or dispose of the drive, without compromising sensitive information.
- › Centralized policy management with device-level precision
- › Centralized key escrow and recovery
- › Highly scalable and easy to deploy

While some benefits are specific to a solution, most benefits are common to all CREDANT products, including:

- › Default security policies that can be easily adjusted to align mobile data security to the type of user, device and location
- › Extensive inventory management and reporting
- › Self-service and administrator assisted device recovery in case of authentication failure
- › Enterprise database integration for a scalable and reliable solution
- › Industry standard encryption to protect critical data anywhere on the disk or on removable media to help your organization ensure compliance with government legislation

SUMMARY

CREDANT's broad solutions offer an equally wide range of features to help you better manage your data protection and to ensure there's a solution that fits everyone from small office to large, complex enterprise environment. Solutions include hardware and software encryption and both managed and unmanaged options. Regardless of the solution, CREDANT provides balanced protection to maximize security while maintaining usability. Through the CREDANT management interface, security administrators can monitor the real time state of mobile device discovery and policy compliance. Default global policies, based on security best practices, help enterprises begin securing their mobile data quickly. CREDANT's flexible solutions easily fit into existing IT procedures without sacrificing security. Finally, CREDANT's extensive and flexible audit logs and reporting options ensure that you can prove compliance to ever increasing and often confusing regulatory laws.

CREDANT Encryption Solutions Overview

CONTACT US

Please contact us for more information about how we can help meet your mobile data security needs.

CREDANT Technologies
15303 Dallas Parkway, Suite 1420
Addison, Texas 75001

1-866-CREDANT (273-3268) or 972-458-5400
www.CREDANT.com
info@CREDANT.com