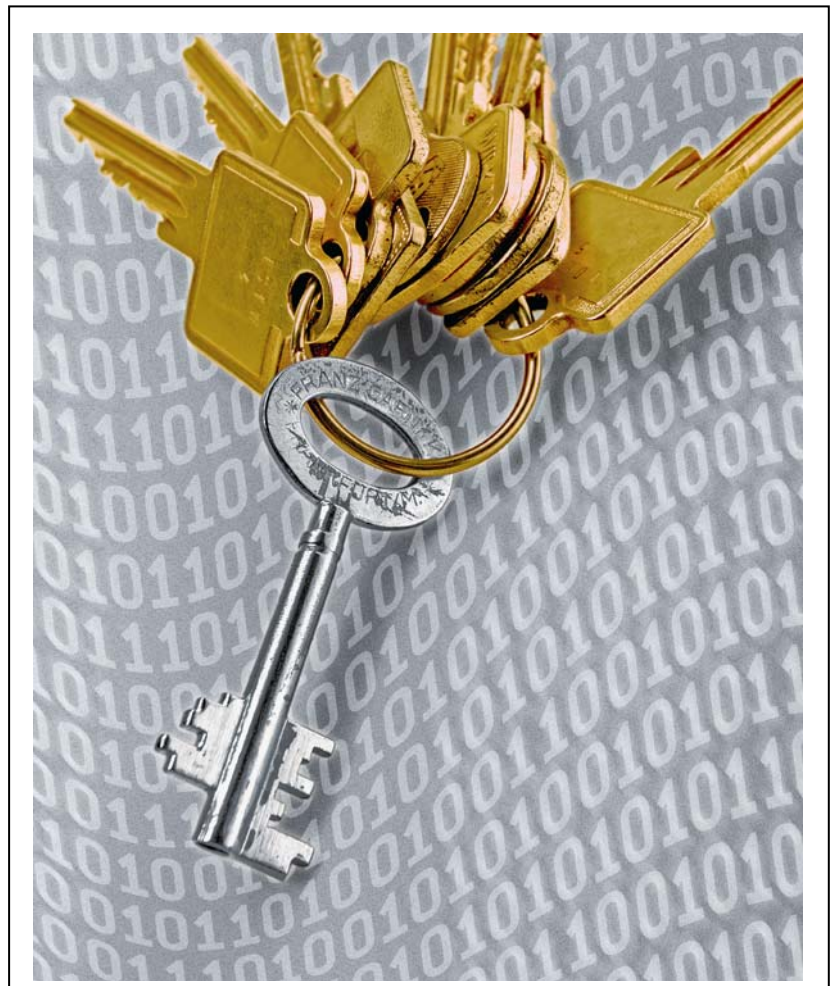




DriveLock 5.5

Full Disk Encryption



Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2008 CenterTools Software GmbH. All rights reserved.

CenterTools and DriveLock and others are either registered trademarks or trademarks of CenterTools GmbH or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

0	About This DriveLock Documentation	5
0.1	Content	5
0.2	Document Conventions	6
1	How DriveLock Full Disk Encryption Works.....	7
1.1	Hard Drive Encryption and Decryption	8
1.2	Pre-boot User Authentication	8
1.2.1	Misplaced or forgotten user authentication credentials.....	9
1.2.2	Unattended reboot followed by automatic pre-boot authentication.....	9
1.3	Windows User Authentication	9
1.3.1	Single sign-on.....	9
1.3.2	Manual Windows authentication.....	9
1.4	Recovery Files and Key Management.....	9
1.5	Disaster Recovery	10
2	System Requirements	11
2.1	Minimum Hardware Requirements.....	11
2.2	Supported Storage Hardware.....	11
2.3	Supported Operating Systems	11
2.4	Supported Networks	12
2.5	Software Compatibility.....	12
2.5.1	DOS drivers and TSRs.....	12
2.5.2	Windows and third-party boot managers.....	13
2.5.3	Windows Disk Management utility.....	13
2.5.4	Windows file compression.....	13
2.5.5	Windows System Restore utility	13
2.5.6	Windows Fast User Switching	13
3	Deploying DriveLock Full Disk Encryption.....	14

3.1	Before You Begin – Best Practices.....	14
3.2	Creating Encryption Keys	15
3.2.1	Using the Encryption Certificate Creation wizard.....	17
3.2.2	Exporting and importing encryption certificates	21
3.3	Installing the DriveLock Full Disk Encryption Package.....	22
3.4	Configuring Deployment Settings.....	26
4	Configuring Pre-Boot Authentication and Full Drive Encryption	30
4.1	Configuring Pre-Boot Authentication	30
4.1.1	Configuring authentication methods and logon settings.....	31
4.1.2	Configuring pre-boot authentication users.....	33
4.1.3	Configuring emergency logon parameters.....	34
4.2	Configuring Hard Disk Encryption.....	36
5	Recovery Procedures	42
5.1	Emergency Logon Recovery Procedures	43
5.2	Recovering Encrypted Disks	50
5.2.1	Creating the files required for decryption.....	50
5.2.2	Recovering (decrypting) disks	55
6	Uninstalling DriveLock Full Disk Encryption.....	57
6.1	Uninstalling DriveLock FDE Completely.....	57
6.2	Disabling Pre-Boot Authentication	58
6.3	Decrypting Hard Disks.....	60
7	User Logon and Appearance.....	63
7.1	Authenticating With Smartcard or Token and PIN	63
7.1.1	Pre-boot authentication	63
7.1.2	Windows authentication	64
7.2	Authenticating With User Name, Password, and Domain Name	65
7.2.1	Pre-boot authentication	65
7.2.2	Windows authentication	66

0 About This DriveLock Documentation

0.1 Content

This manual contains information about the DriveLock Full Disk Encryption (FDE). The first part is intended for administrators who need to configure encryption; the last chapter instructs users how to use full disk encryption.

- Chapter 1 presents an overview on how DriveLock FDE works.
- Chapter 2 describes the system requirements.
- Chapter 3 explains how to prepare and deploy DriveLock FDE.
- Chapter 4 describes how to configure pre-boot authentication and hard disk encryption.
- Recovering encrypted disks and user logons is described in Chapter 5
- Chapter 6 explains how to uninstall DriveLock FDE.
- Chapter 7 instructs users how to log on to a computer protected by DriveLock FDE.

Information about container-based removable media encryption can be found in the document “DriveLock Encryption Guide”.

Information about how to install DriveLock and how to deploy your configuration settings can be found in the document “DriveLock Planning – Installation – Deployment”.





Information about drive and device locking, whitelist rules, network profiles, application blocking, auditing and other features of DriveLock can be found in the document “DriveLock Administration Guide”.

For information about the Security Reporting Center, see the document “DriveLock Security Reporting Center Manual”.

More information about DriveLock (such as video tutorials, white papers and other documentation) can be found on the DriveLock Web site (www.drivelock.com).

0.2 Document Conventions

Throughout this document the following conventions and symbols are used to emphasis important issues that you should read carefully or menus, items or buttons you have to click on or select.

	<p>Caution: This symbol means that you should be careful to avoid unwanted results, such as potential damage to operating system functionality or loss of data</p>
	<p>Hint: Useful additional information that might help you save time.</p>
	<p>Information: Additional information about the current topic</p>
<p><i>italics</i></p>	<p>Italics represent fields, menu commands, and cross-references.</p>
	<p>A fixed-width typeface represents messages or commands typed at a command prompt.</p>
<p>Cancel</p>	<p>Bold type represents a button that you need to click.</p>
<p>ALT + R</p>	<p>A plus sign between two keyboard keys means that you must press those keys at the same time. For example, ALT+R means that you must hold down the ALT key while you press R.</p>
<p>ALT, R, U</p>	<p>A comma between two or more keys means that you must press them consecutively. For example 'ALT, R, U' means that you must first press the Alt key, then the R key, and finally the U key.</p>

1 How DriveLock Full Disk Encryption Works

In today's computing environment, hard disk drives have become mass repositories of proprietary information. The widely used Windows operating system provides adequate data privacy for stand-alone or networked computers in most operating environments. However, Windows does not sufficiently protect the data on a computer's hard disk against disclosure when the computer is lost or stolen. Unless additional data protection measures are taken, anyone with access to the hard drive can read all data on it.

To mitigate this data security risk, CenterTools has integrated a system security and data encryption solution into DriveLock. DriveLock Full Disk Encryption (FDE) provides the following functionality:

- **Hard Drive Encryption**
Strong data encryption of all sectors on the hard drive ensures that no unauthorized access to any data is possible.
- **Pre-boot User Authentication**
Used to authenticate users before the operating system starts. Upon successful authentication the pre-boot process retrieves a computer-specific key that is used to decrypt the disk sectors that store the operating system files and all other files on the encrypted drive as they are accessed. Users can authenticate using their Windows logon credentials or smartcards and tokens.
- **Single Sign-on or manual Windows authentication**
DriveLock FDE provides automatic Windows domain user authentication following successful pre-boot authentication so users don't need to authenticate twice. Manual Windows authentication is available as an alternative.
- **Emergency Pre-boot User and Token Logon Recovery**
Recovery of logon data for pre-boot logon of users who don't have access to their pre-boot credentials This includes users who forgot their passwords, don't have their smartcard or token with them, and the introduction of new users who have never logged onto the computer before.
- **Disaster Recovery Tools**
DriveLock FDE provides disaster recovery tools to decrypt an encrypted disk in case of disk failure.

1.1 Hard Drive Encryption and Decryption

All data encryption is transparent to the end user, the operating system and applications. DriveLock FDE can automatically encrypt and decrypt multiple hard disk partitions. When encrypted data is being read, DriveLock FDE decrypts it “on the fly”—it immediately becomes available to the user or applications. All data written to the disk is automatically encrypted. As a result, normal system operations remain unaffected.

1.2 Pre-boot User Authentication

To start an encrypted operating system partition, DriveLock FDE must get access to the disk *decryption key* before the operating system starts. This key is used to decrypt the disk sectors containing the operating system files and the rest of an encrypted hard drive.

DriveLock FDE prevents unauthorized access to the decryption keys by using *Pre-boot User Authentication*. The decryption key itself is encrypted using a unique key that is derived from the user credentials. After successful pre-boot authentication, the disk key is decrypted and used to provide access to the disk so that the operating system can be loaded. DriveLock FDE maintains its own *Pre-boot User Database* to authenticate user.

The Pre-boot User Database has the following characteristics:

- Maximum number of users or certificates — 2,000
- User name length — 1 to 20 characters
- Password length — up to 20 **case-sensitive** characters (no minimum)



Although the maximum number of users is 2,000, three of these slots are reserved for DriveLock FDE’s own use. The remaining slots are available to store user accounts and credentials. However, each user can potentially use *multiple* user slots, one for a password, one for a shared key, and one for each certificate.



When using the single sign-on functionality, Windows passwords can be no longer than 20 characters.

DriveLock FDE can authenticate users on stand-alone computers and computers belonging to a Windows domain who use passwords. Smartcards and tokens with a PIN can also be used to authenticate.

1.2.1 Misplaced or forgotten user authentication credentials

DriveLock FDE provides a mechanism for helpdesk personnel to let users log on who can't access their authentication credentials. This may include instances of users who have misplaced their smartcard or token or forgotten their Windows domain password.

DriveLock FDE provides automated procedures for handling these pre-boot authentication scenarios.

1.2.2 Unattended reboot followed by automatic pre-boot authentication

Various system administration functions not related to DriveLock FDE may at times require an unattended computer restart, followed by automatic pre-boot authentication. DriveLock FDE enables this functionality by using a special user account. A special command line utility is required to implement this functionality. Please contact the DriveLock support team for detailed information.

1.3 Windows User Authentication

1.3.1 Single sign-on

You can configure DriveLock FDE to *automatically* log users on to Windows following successful pre-boot authentication using their domain or local Windows accounts. This chaining of authentication processes is called *single sign-on*. Single sign-on simplifies the user experience as users only need to authenticate once.

1.3.2 Manual Windows authentication

As an alternative to the single sign-on mode, you can configure DriveLock FDE to present the standard Windows authentication screen each time the operating system starts, allowing the user to manually authenticate using a Windows account.

1.4 Recovery Files and Key Management

Prior to installing DriveLock FDE, you must create a recovery file set. These files are required to perform key recovery in case of a disaster and to perform emergency logon procedures. The recovery file set consists of the following files:

- **Master Security Certificate (MSC)** — The *PdMaster.cer* file contains a certificate with a public key that is used to encrypt a backup copy of the computer's disk encryption key. The *PdMaster.pfx* file contains the corresponding private key that is required to gain access to the disk decryption key that is used to decrypt a damaged hard disk. The *PdMaster.pfx* file is intended to be private. It should be securely stored and only accessible to individuals who are authorized to perform disaster recovery. *PdMaster.cer* contains the public key component of the Master Security Certificate (MSC). It does not contain confidential information and is used during each DriveLock FDE installation.
- **Recovery Support Certificate (RSC)** — The *PdRecovery.cer* file contains a certificate with a public key that is used to control access to the pre-boot authentication database. The *PdRecovery.pfx* file contains the corresponding private key that is used to authenticate such access when creating emergency logon credentials for users. The *PdRecovery.pfx* file is intended to be private. It should be securely stored and only accessible to individuals who can perform password recovery, such as helpdesk and support personnel). *PdRecovery.cer* contains the public key component of the Recovery Support Certificate (RSC). It does not contain confidential information and is used during each DriveLock FDE installation.
- **Recovery Envelope** — The *RecoveryEnvelope.env* file is created for on each client computer when you install DriveLock FDE. It contains recovery data that is specific to the computer and is required, in conjunction with the appropriate private key, for emergency logon procedures or disk decryption. If you save the recovery envelop to a file share instead of a local drive, the client computer name is included in the file name in the following format: *<computer name>.Recovery.env*.

1.5 Disaster Recovery

For standalone installations, disaster recovery preparation begins with periodic system data backups. DriveLock FDE creates recovery files that can be used to later decrypt a disk that is damaged or that cannot be accessed normally for other reasons. The recovery files must be stored off the client system to be available in case of system failure. This backup file set is used in conjunction with the Master Security Certificate (MSC) to perform Disk Key Recovery.

DriveLock FDE includes a command line recovery tool to perform disaster recovery tasks such as data decryption. This recovery tool is included in the DriveLock FDE installation and is generally used only by system administrators only.

2 System Requirements

2.1 Minimum Hardware Requirements

- 32-bit Intel-compatible CPU
- Sufficient memory to run the operating system, plus 30MB of available hard disk space
- CD ROM drive or access to an installation directory on a server
- Maximum hard disk size: 2TB

2.2 Supported Storage Hardware

DriveLock FDE can encrypt all fixed (non-removable) hard disk partitions that have been assigned a drive letter, including all IDE/EIDE, SATA and SCSI drives. There is no support for hidden partitions or software RAID arrays.

DriveLock FDE does not interfere with the normal operation of the storage subsystem, with the following exceptions:

- It is not possible to format any partition on the system drive after DriveLock FDE has been installed.
- DriveLock FDE does not support post-installation addition, removal or substitution of hard drives.
- During installation, DriveLock FDE examines all partitions present on the system. Repartitioning, resizing, converting or activating partitions after DriveLock FDE has been installed is not supported, including any manipulation of the Master Boot Record.

2.3 Supported Operating Systems

This version of DriveLock FDE is supported on the following operating systems:

- Microsoft Windows XP Professional, Service Pack 2 (64-bit version is **not** supported)
- Microsoft Windows Vista Business, Service Pack 1
- Microsoft Windows Vista Enterprise, Service Pack 1
- Microsoft Windows Vista Ultimate, Service Pack 1
- Microsoft Windows Server 2003 R2, Service Pack 2

- Microsoft Windows Server 2003, Service Pack 2

DriveLock FDE supports the use of the FAT16, FAT32, and NTFS file systems.



MS-DOS can be used to start a computer to run DriveLock FDE disaster recovery tools. Computers running DriveLock FDE with a hard disk that is inaccessible or corrupt can be booted to MS-DOS from a floppy disk or a CD. Drives that require special DOS drivers, such as SCSI drives or TSRs are only accessible to the DriveLock FDE recovery tools if the required drivers are loaded. It is recommended to use the DriveLock Recovery Image (ISO) and an USB stick containing the Disk Recovery Keys. You can also start the computer using other bootable media, such as a CD containing the Windows PE operating system.

DriveLock FDE requires the following additional software on any computer where you are running the Management Console:

- .NET Framework 3.0

2.4 Supported Networks

DriveLock FDE is Active Directory-aware and fully supports Windows domains. It does not interfere with normal operation of any Windows network services, including Remote Desktop connections. Windows domain users and local Windows users can authenticate to computers that are secured by DriveLock FDE. All hard disk partitions encrypted with DriveLock FDE can be shared on a network at the discretion of the system administrator.

2.5 Software Compatibility

DriveLock FDE has been tested and does not interfere with normal operation of most Windows-compliant software, applications, services and utilities. Some care needs to be taken, however, when using the following.

2.5.1 DOS drivers and TSRs

When booted from a DOS floppy disk or CD, DriveLock FDE sees hard disks that are accessible using DOS drivers and TSRs only if the appropriate drivers are loaded.

2.5.2 Windows and third-party boot managers

At system startup, DriveLock FDE manipulates the Master Boot Record (MBR) and verifies its integrity. All software that needs to manipulate the MBR for its own purposes is incompatible with DriveLock FDE. This includes the standard Windows boot manager.

2.5.3 Windows Disk Management utility

No disk repartitioning, resizing, and mirroring configuration changes can be performed after DriveLock FDE has been installed. If any of the above operations are required, decrypt all disks and uninstall DriveLock FDE before proceeding.

2.5.4 Windows file compression

Windows file compression is fully supported, with one exception: The DriveLock FDE system files directory (`C:\Securdisk`) must not be compressed.



Do not install DriveLock FDE to a compressed system drive. This will result in compression of the `C:\Securdisk` directory, which will interfere with normal operations of DriveLock FDE.



The directory `C:\Securdisk` is a hidden system directory.

2.5.5 Windows System Restore utility

Windows system restore points created prior to the DriveLock FDE installation can no longer be used. The system can only be restored to any restore point created following the DriveLock FDE install.

2.5.6 Windows Fast User Switching

DriveLock FDE disables the standard Windows Welcome screen along with its fast user switching functionality.

3 Deploying DriveLock Full Disk Encryption

3.1 Before You Begin – Best Practices

Review the sections below and ensure that you have performed the appropriate procedures prior to installing DriveLock FDE.

Best practices for preparing to deploy DriveLock FDE include:

- Defragmenting the drives that will be encrypted by DriveLock FDE
- Repairing any existing disk errors
- Ensuring that the data storage on each computer is well organized and that no further rearranging of any partitions will be required later. Use Windows Disk Management as needed to configure all partitions and disk mirroring before installing DriveLock FDE.
- Running `CHKDSK /f` and the hard disk manufacturer's diagnostic utility to ensure file system health on all drives you intend to encrypt. Repair any bad sectors, as DriveLock FDE cannot encrypt such sectors.
- Backing up all important data prior to disk encryption.

The utilities provided by the hard disk manufacturer are typically the most robust tools for repairing disk errors.



It is recommended that you create a Recovery File Set, save it to removable media and place it in a safe location such as a safe. You should also include the Recovery Tools and Recovery Keys with the Recovery File Set. These files are required for the following procedures:

- Disaster Recovery Procedures
- Pre-boot Emergency Logon Procedures

3.2 Creating Encryption Keys

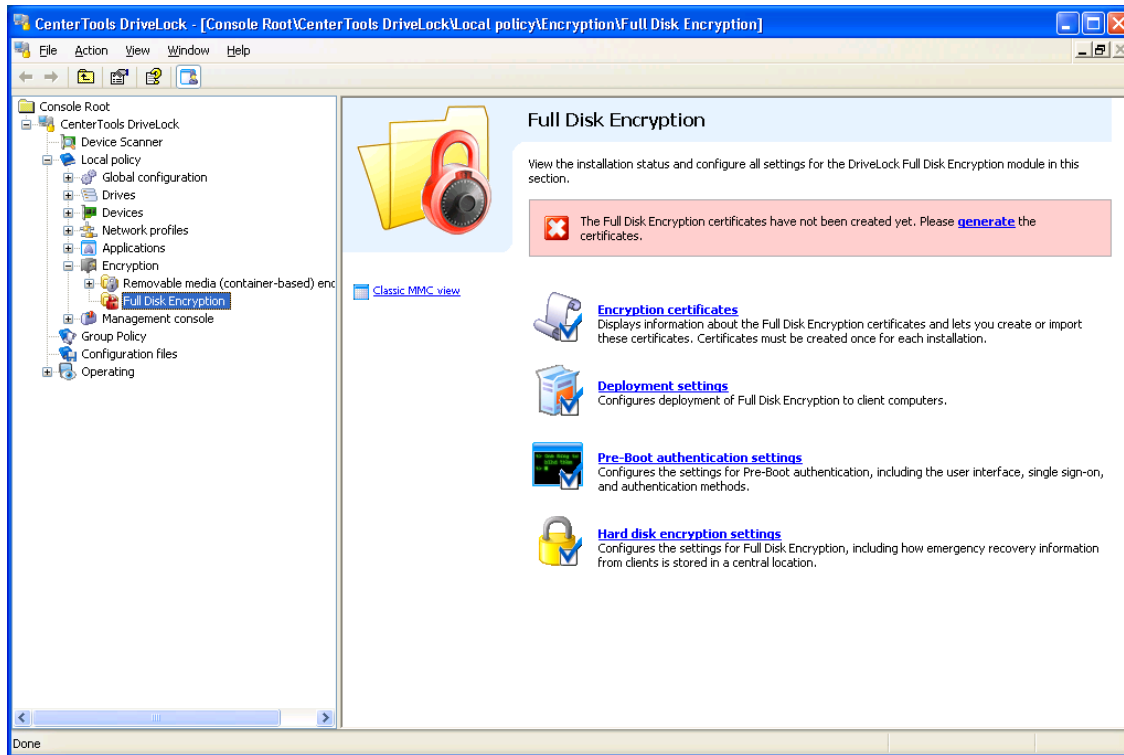
Before you can install DriveLock FDE, you must create encryption keys. These files are required to perform disaster key recovery and emergency logon procedures. The encryption keys are described in detail in the section “Recovery Procedures”.

- **Master Security Certificate (MSC)** — The *PdMaster.cer* and *PdMaster.pfx* files make up a public/private key pair. *PdMaster.pfx* is used to extract Disk Key Recovery information. The *PdMaster.pfx* file is intended to be private, and as such, it must be securely stored and only accessible to individuals who can perform disaster recovery. *PdMaster.cer* is the public key component of the Master Security Certificate (MSC), and is intended to be used on each installation.
- **Recovery Support Certificate (RSC)** — The *PdRecovery.cer* and *PdRecovery.pfx* make up a public/private key pair. *PdRecovery.pfx* is used for Emergency logon procedures. The *PdRecovery.pfx* file is intended to be private, and as such, it must be securely stored and only accessible to individuals who can perform password recovery (for example, Help Desk/Support personnel). *PdRecovery.cer* is the public key component of the Recovery Support Certificate (RSC) and is intended to be used on each installation.



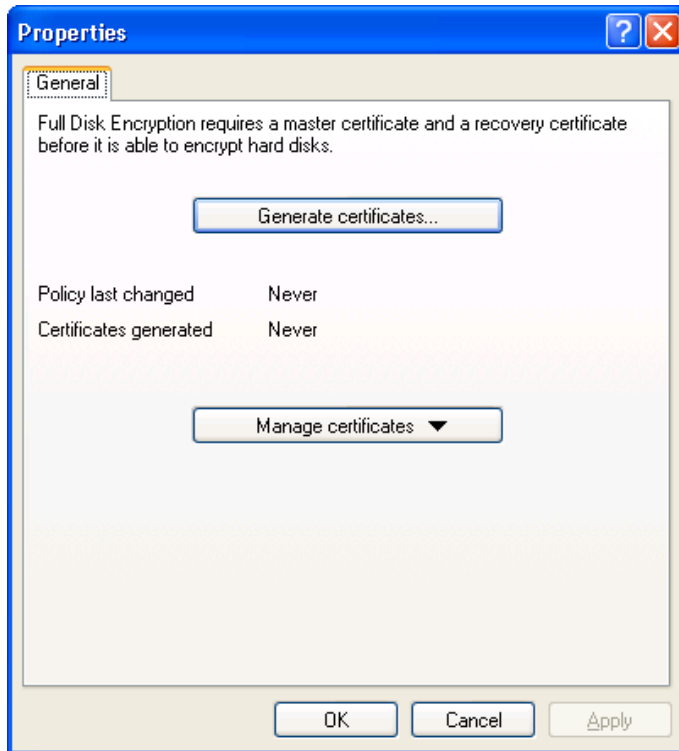
Without the encryption keys and the corresponding passwords you will not be able to recover any data or help users reset their passwords.

When you start DriveLock FDE for the first time the encryption certificates and keys have not been created yet.



Click **generate** to create new encryption certificates and keys.

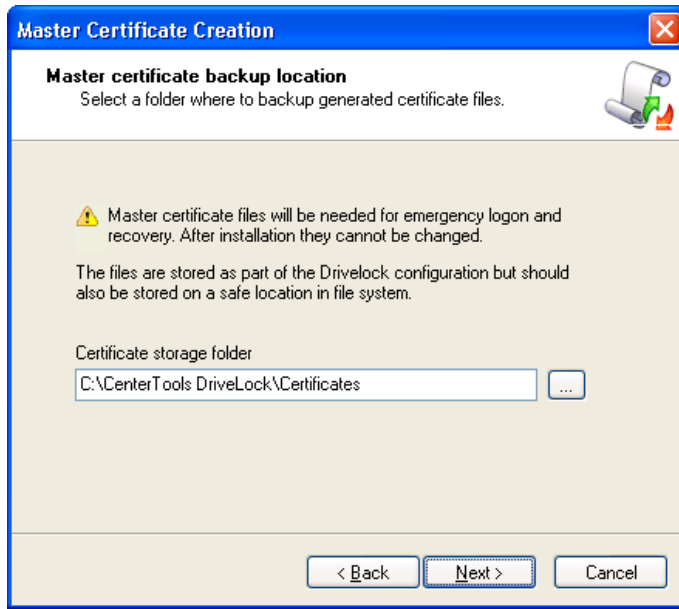
You can also start the wizard by clicking **Encryption certificates** and then, on the next screen, clicking **Create certificates**.



3.2.1 Using the Encryption Certificate Creation wizard



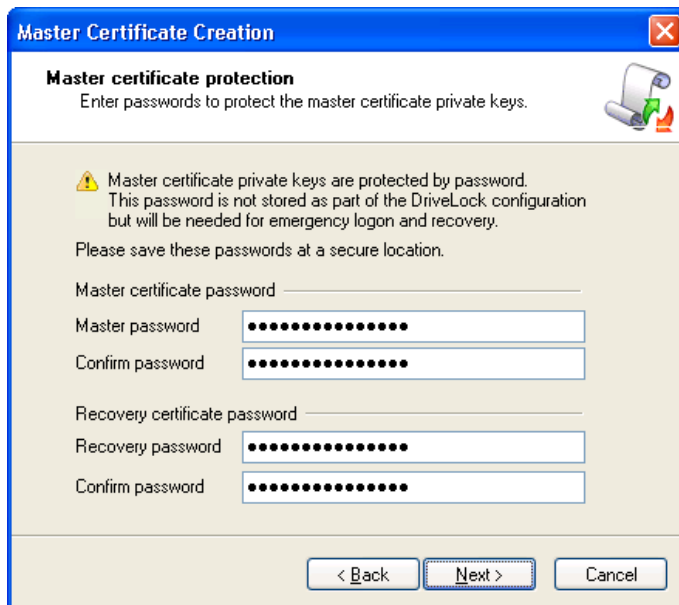
Click **Next**.



Specify the location to save the certificate files to and then click **Next**.



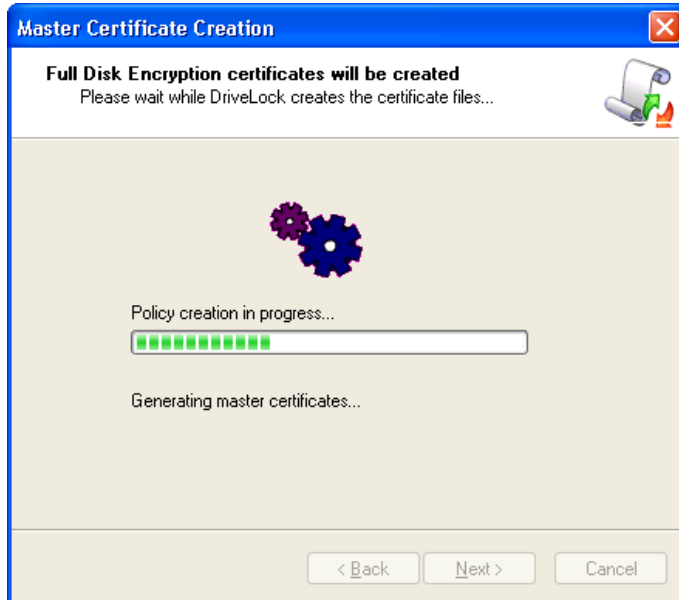
Store encryption certificate files in a safe location, as they are needed for user password and data recovery together with the Recovery Files Set.



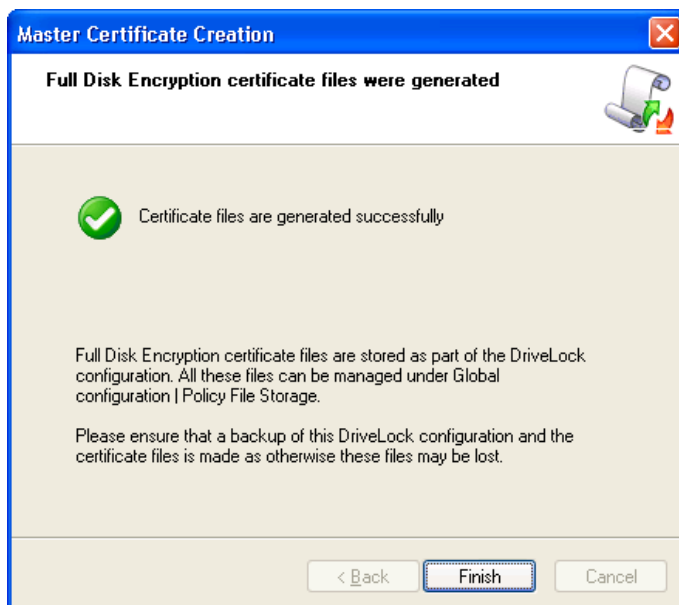
Type the passwords for both the master and recovery certificate and confirm each password by typing it again. Click **Next** to continue.



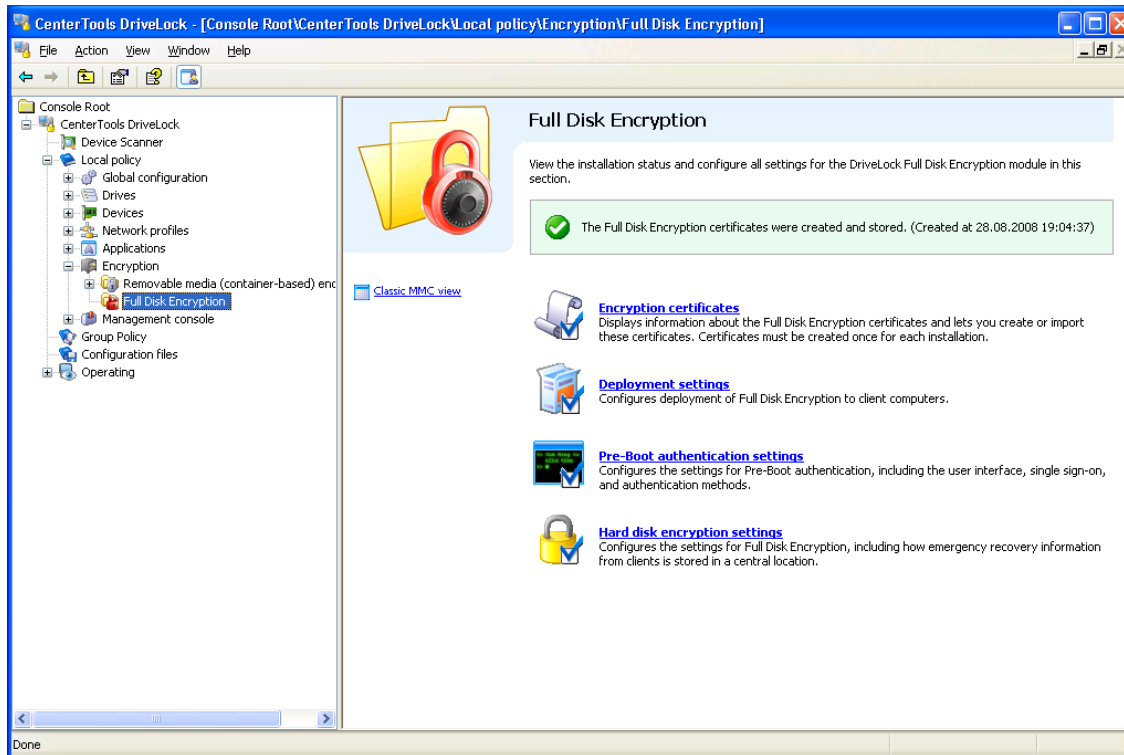
Make sure to record these passwords and store them in a secure location, such as a safe.



The wizard notifies you when it has finished creating the certificates. Please do not interfere with the policy creation process.



Click **Finish**.



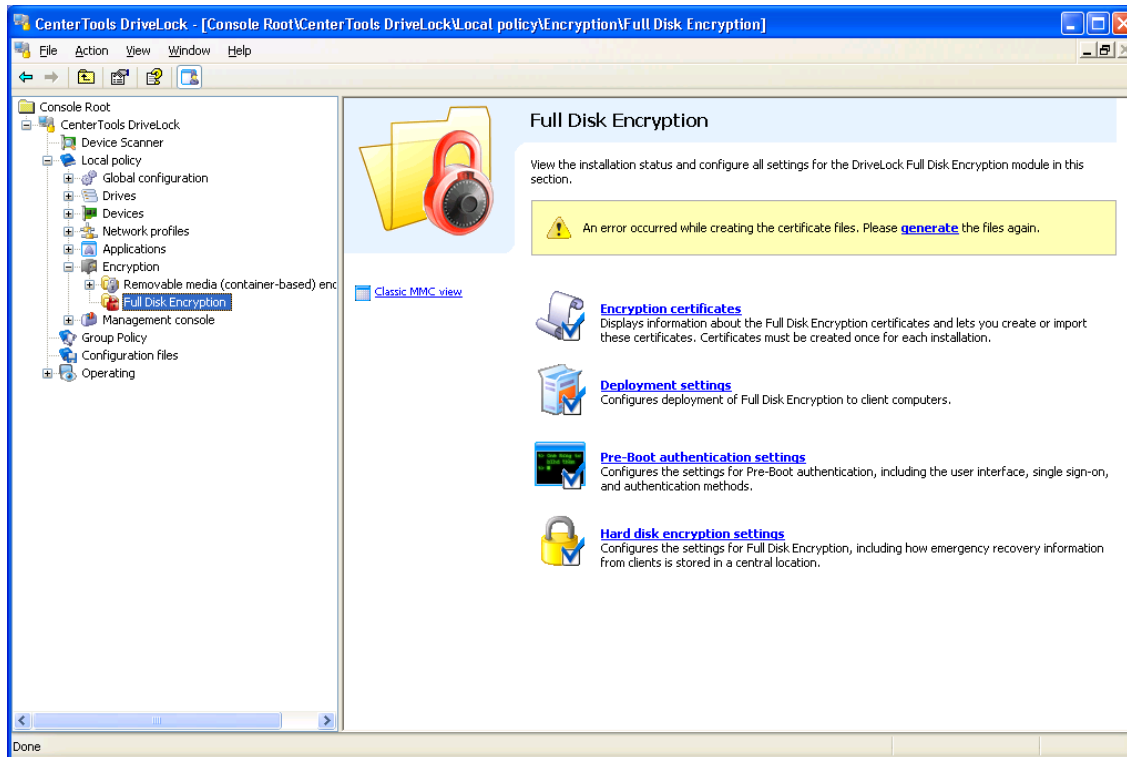
Once the encryption certificates have been created the DriveLock Management Console displays the creation time and date.

The certificates are also stored in user's private certificate area and the public keys are stored within the DriveLock Policy file storage



Once the certificates have been created and DriveLock FDE has been installed on client computers, do not create a new set of certificates.

If you cancelled the certificate creation wizard or if the certificate creation failed, DriveLock displays an error message and you must start the certificate creation process again.

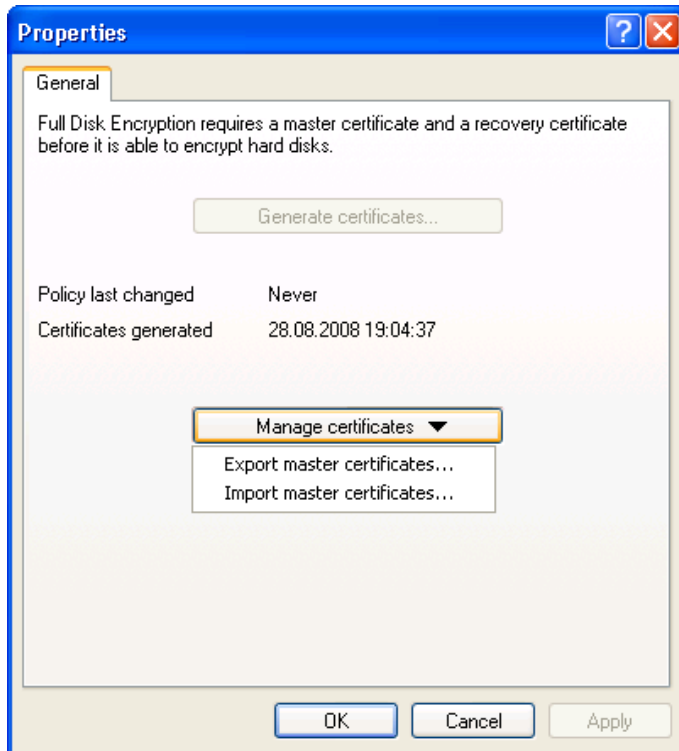


Creation of smartcard-based private keys is not supported in this version of DriveLock.

3.2.2 Exporting and importing encryption certificates

After you have created the encryption certificates you can export the public keys from the DriveLock Policy File storage.

In the DriveLock Management Console, click **Master certificates**.



To export the two certificate files, click **Manage certificates** and then on the drop-down menu click *Export master certificates*. Select a directory to save the files to.

You can also import certificates (public keys) that have been previously created into the DriveLock Policy File storage. To import the two certificate files, click **Manage certificates** and then on the drop-down menu click *Import master certificates*. Select the directory containing the certificate files.

3.3 Installing the DriveLock Full Disk Encryption Package

The DriveLock Full Disk Encryption module will be installed and managed by the DriveLock Agent. To perform this task, the Agent needs to read the installation file "*pdinstall.bin*". The Agent can access this file from the following local or network locations:

- *Security Reporting Center server* – The Agent retrieves the file from the Security Reporting Center.
- *Web server URL* – The Agent downloads the file from the specified server by using HTTP.
- *File server (UNC path)* – The Agent downloads the file from the specified shared folder.
- *Local installation on client* – The file is located on the Agent's local disk.

On the computer where you will make the installation file available, run “*DriveLock Full Disk Encryption.msi*” to install the DriveLock FDE installation file.



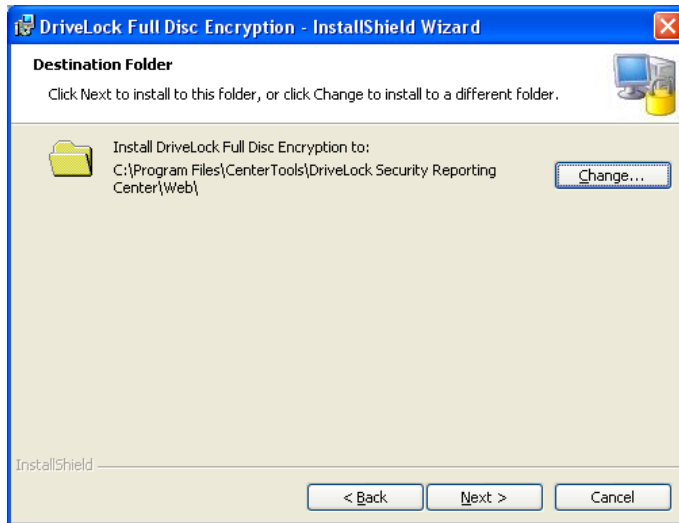
You can download the file “*DriveLock Full Disk Encryption.msi*” from the DriveLock Web site. It is also included in the DriveLock ISO disk image that is available at this site.



Click **Next**.



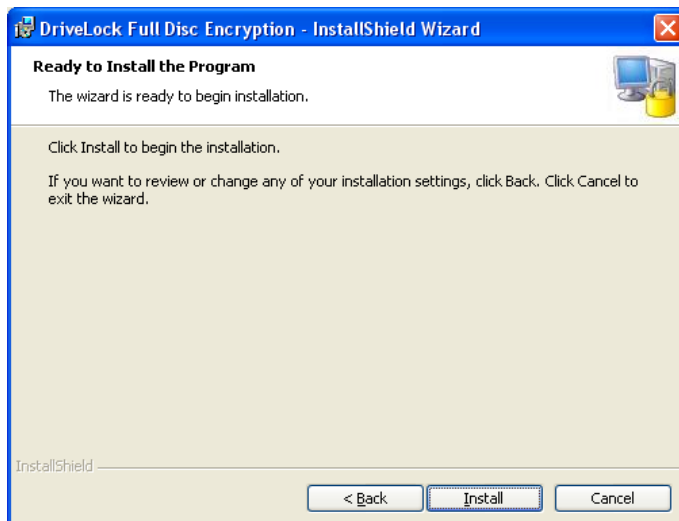
Accept the license agreement and click **Next**.



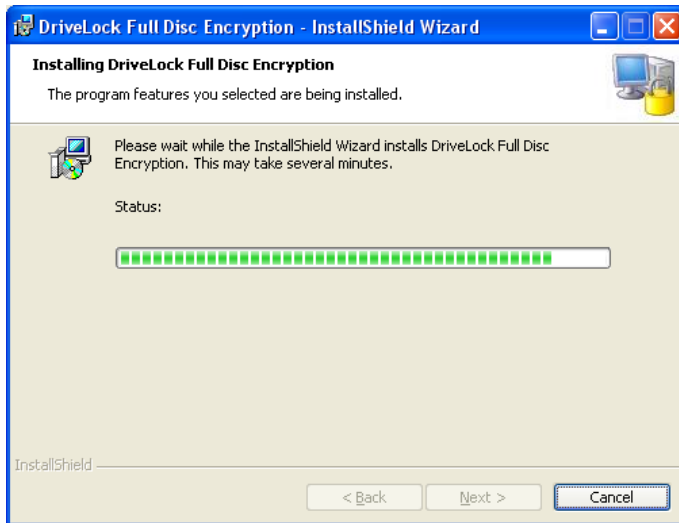
Select the folder to install the file to.



If you install the file on the Security Reporting Center, the folder must be *"C:\Program Files\CenterTools\DriveLock Security Reporting Center\web"* (or the corresponding location if you did not install the SRC in the default location).



Click **Install** to start the installation.



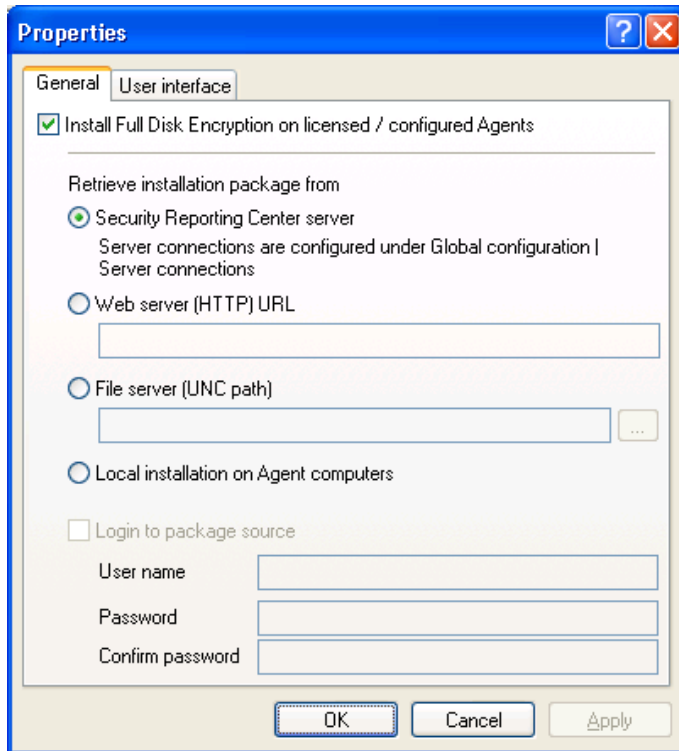
Click **Finish** to complete the installation.



You can also use Windows Group Policy or other deployment tools to deploy the DriveLock FDE installation package.

3.4 Configuring Deployment Settings

After you created the Recovery Key Set you can configure DriveLock FDE deployment settings. To configure these settings, in the right pane of the DriveLock Management Console, click **Deployment settings**.



To install DriveLock FDE on client computers, select the “*Install Full Disk Encryption on licensed / configured Agents*” checkbox.



Once you have activated deployment by selecting “*Install Full Disk Encryption on licensed / configured Agents*”, as soon as the DriveLock Agent detects that the policy has changed, it retrieves the installation package and installs DriveLock FDE on the client computer.

You can select to have the Agent retrieve the file “*pdinstall.bin*” from the following locations:

- **Security Reporting Center server** – The Agent retrieves the file from the Security Reporting Center.
- **Web server (HTTP) URL** – The Agent downloads the file from the server location you specify by using HTTP (for example, *http://server/pdinstall.bin*)

- **File server (UNC path)** – The Agent downloads the file from the shared folder you specify (for example, \\server\networkshare).
- **Local installation on Agent computers** – The file is located on a local disk. You must specify the location by editing the registry.

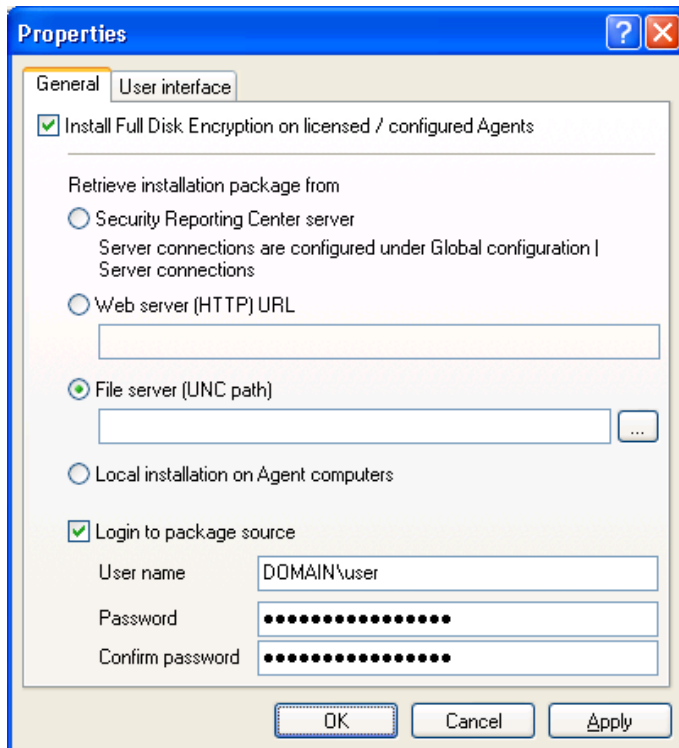


Ensure that you have installed the file *pdinstall.bin* in the selected location before you enable DriveLock FDE installation. For more information about the installation process, refer to the section “Installing the DriveLock Full Disk Encryption Package”.



You must configure a SRC server connection and specify a user name (domain\user) and password to enable the Agent to connect to the SRC server, as the Agent is usually configured to run as “Local System”. Otherwise the Agent will not be able to download the file “pdinstall.bin” and installation of DriveLock FDE will fail. Refer to the document “*DriveLock Administration Guide*” on how to configure an SRC server connection.

You must specify logon credentials that the Agent will use to access a Web server or a file share.



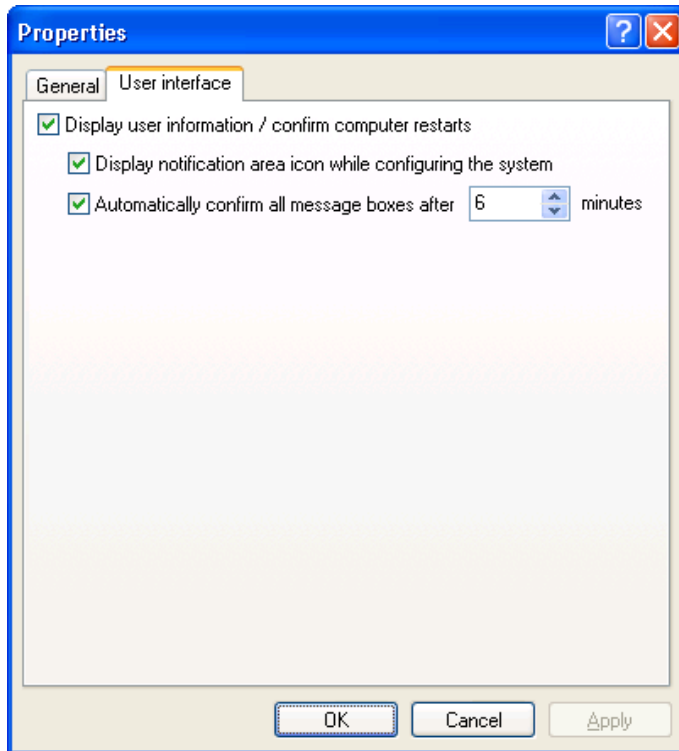
The screenshot shows a Windows-style dialog box titled "Properties" with two tabs: "General" and "User interface". The "General" tab is active. It contains the following elements:

- A checked checkbox: "Install Full Disk Encryption on licensed / configured Agents".
- A section titled "Retrieve installation package from" with three radio button options:
 - Security Reporting Center server
Server connections are configured under Global configuration | Server connections
 - Web server (HTTP) URL
[Empty text box]
 - File server (UNC path)
[Empty text box] [Browse button]
 - Local installation on Agent computers
- A checked checkbox: "Login to package source".
- Below the checkbox, three text input fields:
 - User name: "DOMAIN\user"
 - Password: [Masked with dots]
 - Confirm password: [Masked with dots]
- At the bottom, three buttons: "OK", "Cancel", and "Apply".



Type the user name in the format `<domain>\<user>` when using a domain account to log on to the central location.

Select the tab *User interface* to configure additional settings.



To not display information messages on the client computer while DriveLock FDE is installed, deselect the “*Display notification area icon while configuring the system*” checkbox. You can also select whether information messages are confirmed automatically after being displayed for a specified number of minutes.

When the Agent gets its new configuration settings and prepares for installing DriveLock FDE, the Agent displays the following message to the currently logged on user:



Click **OK** or **Apply** to save the settings, or click **Cancel** to discard any changes you made.

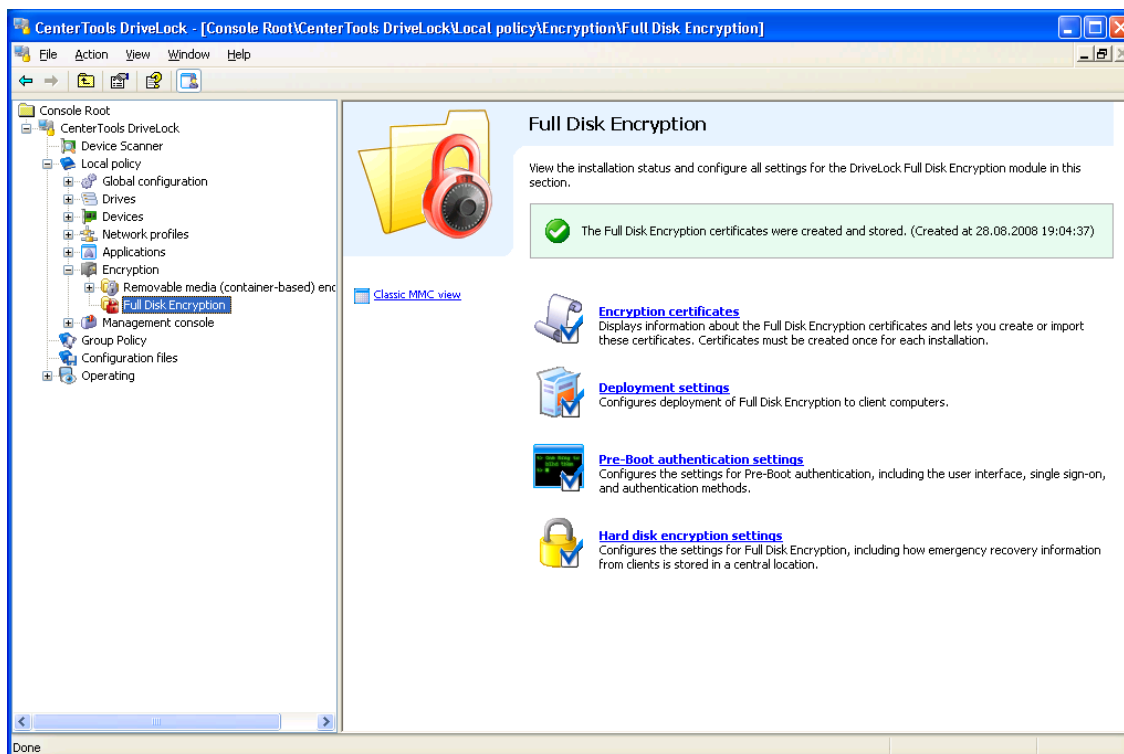
4 Configuring Pre-Boot Authentication and Full Drive Encryption

Once you have deployed DriveLock FDE to client computers you can configure settings for drive encryption and pre-boot authentication parameters.



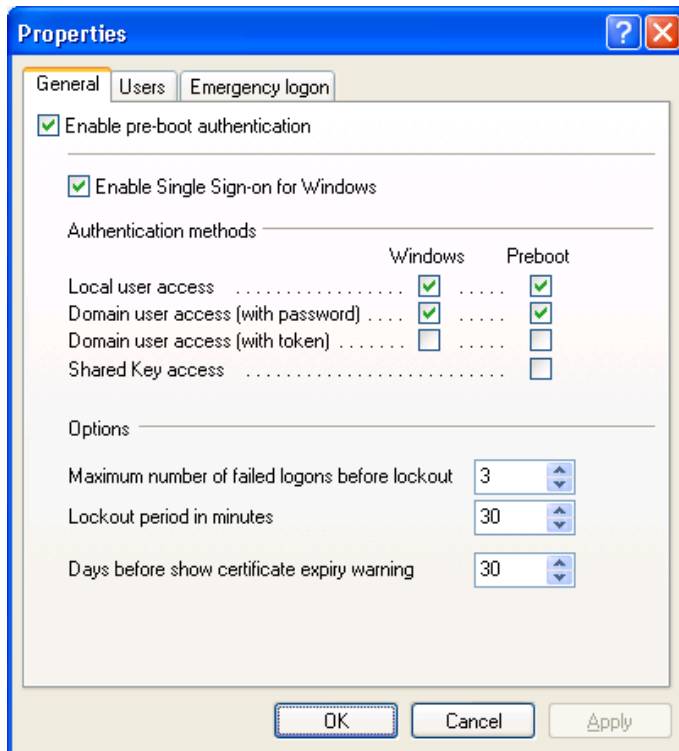
You can activate and configure pre-boot authentication before you begin to encrypt hard drives on client computers. This can help divide the deployment process in larger environments or help users get familiar with the new logon procedure.

4.1 Configuring Pre-Boot Authentication



Click **Pre-boot authentication settings** to open the configuration dialog box.

4.1.1 Configuring authentication methods and logon settings



To enable pre-boot authentication on client computers, select the “*Enable pre-boot authentication*” checkbox.



As soon as the DriveLock Agent detects the new configuration settings, pre-boot authentication is activated and takes effect the next time the computer is restarted. Ensure that all other required parameters in this dialog box have been configured and that users are aware of the change. DriveLock displays the following message to the user when pre-boot authentication is first activated:



To disable DriveLock FDE without uninstalling it, clear the *“Enable pre-boot authentication”* checkbox. Without pre-boot authentication, all features of DriveLock FDE, including disk encryption, are disabled. If you clear this checkbox you can make still changes to other settings in this dialog box, but changes do not take effect until DriveLock FDE is re-enabled by selecting the *“Enable pre-boot authentication”* checkbox again.



Deactivating pre-boot authentication removes all users from the client computer’s pre-boot user database. Windows domain users will be added again automatically at Windows logon once pre-boot authentication is reactivated, provided that you configured DriveLock to automatically add Windows users. Local Windows users, however, will not be automatically added again and will not be able to perform pre-boot authentication. To allow local Windows users to log on, you must add these users manually after you reactivate pre-boot authentication.

To gain access to a computer protected by DriveLock FDE, authentication at both pre-boot and Windows authentication are mandatory.

You can require users to use one or multiple authentication methods for pre-boot authentication and Windows logon, based on the settings you configure. These authentication methods are described in detail below.

To make an authentication method available to users, select the *Windows* checkbox, the *Pre-boot* checkbox, or both, to match the security requirements of your organization. You must select at least one check box each for Windows and pre-boot authentication.



Do not configure DriveLock FDE to allow only tokens and smart cards for Windows logon unless your network is configured for certificate-based logon. If users don't have tokens or if required drivers are not installed and the computer is locked, it can't be unlocked using a password. If DriveLock FDE is configured to only allow token logon, ensure that valid tokens have been distributed to users and that they can be used for pre-boot authentication, Windows logon and unlocking.

Local user access – Enabled by default. This method lets users authenticate by typing a local Windows user name and password and selecting the computer name.

Domain user access (with password) – This method lets users authenticate by typing a Windows domain user name, password and selecting the domain name.

Domain user access (with token) – This method lets Windows domain users authenticate by using a smartcard or token with a PIN.

Shared Key access – This method lets users perform pre-boot authentication by using a shared key token (non-PKI). If this option is selected, at least one Windows authentication method must also be selected.

In single sign-on mode, a user only needs to log on once to authenticate both to the pre-boot authentication and to Windows. This option is only available when at least one authentication method is enabled for both pre-boot authentication and Windows .

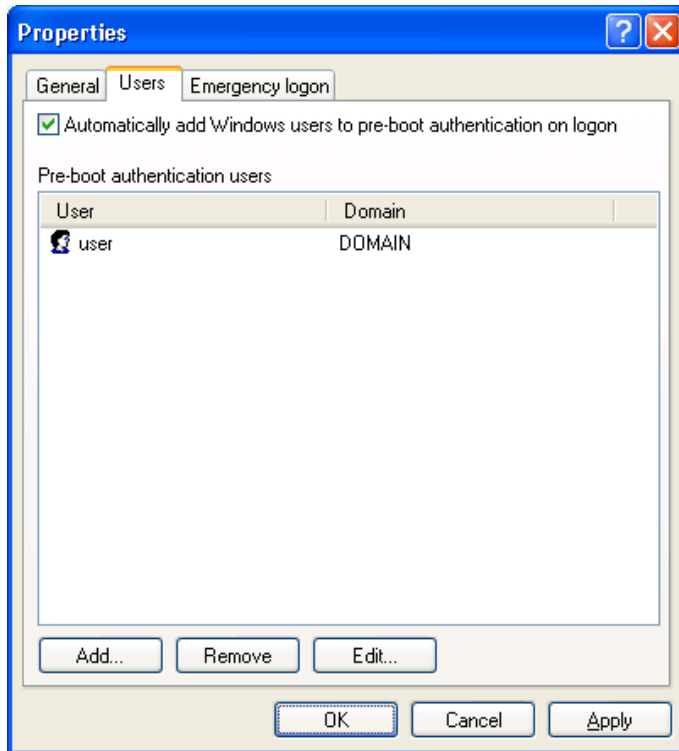
Select the "*Enable Single Sign-on for Windows*" checkbox to enable single-sign on mode.

DriveLock FDE can lock out a user after a configurable number of failed logons for a number of minutes to protect the authentication database against automated brute-force attacks. Adjust the values to match your organization's security policy.

If you use certificates for authentication you also can configure how many days before the expiration of a certificate DriveLock FDE notifies the user of the upcoming expiration.

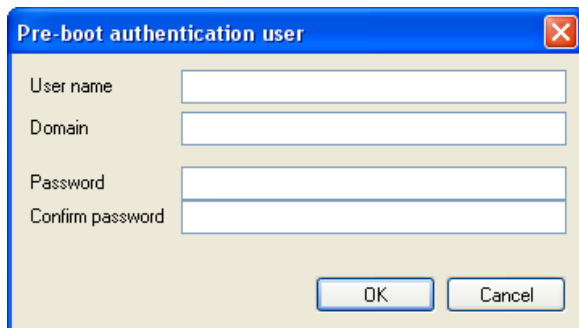
4.1.2 Configuring pre-boot authentication users

DriveLock FDE can hold up to 2000 users in its pre-boot authentication database. You can manually add users to this database. A pre-boot authentication user does not need to correspond to a specific Windows user account. If required, you can configure separate credentials that are used for pre-boot authentication only.



By default DriveLock FDE adds any user who has successfully logged on to Windows to the pre-boot authentication database. Deselect the “*Automatically add Windows user to pre-boot authentication on logon*” checkbox if you don’t want Windows users to be automatically added.

Use the **Add**, **Remove** or **Edit** buttons to change or remove existing users or to add new users to the database.

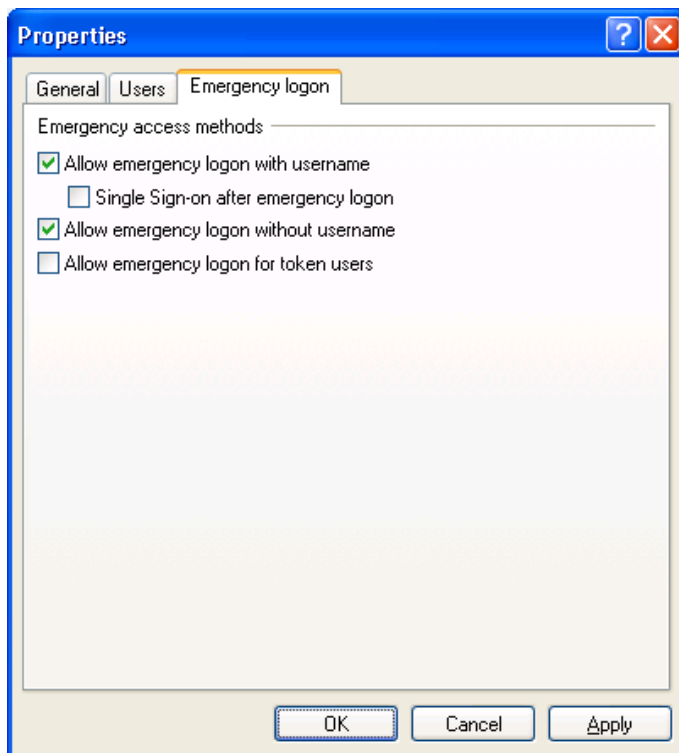


After you have entered the information and confirmed the password, click **OK** to save the user.

4.1.3 Configuring emergency logon parameters

Emergency logon parameters specify which logon procedures are available for users when they are not able to log on by using normal procedures. For example, this includes users who forgot their password. For

more information about how to perform these procedures, refer to the section “Emergency logon recovery procedures”.



Emergency logon settings are available when authentication is enabled at the pre-boot level and the *Local user access* or *Domain user access* check boxes are selected.

Allow emergency logon with user name – When enabled, this option lets a user initiate the *emergency logon with user name procedure*. This procedure is used when a user has forgotten the pre-boot authentication password. It also applies to local Windows or domain accounts that have been added to DriveLock FDE but not been assigned an initial password. Emergency logon with user name enables one-time-only pre-boot access to the system.



This feature requires that a user was authenticated by pre-boot authentication on the computer at least once or that the user was added to the pre-boot authentication database by an administrator. A user who is not in the pre-boot authentication database must initiate the *emergency logon without username procedure*.

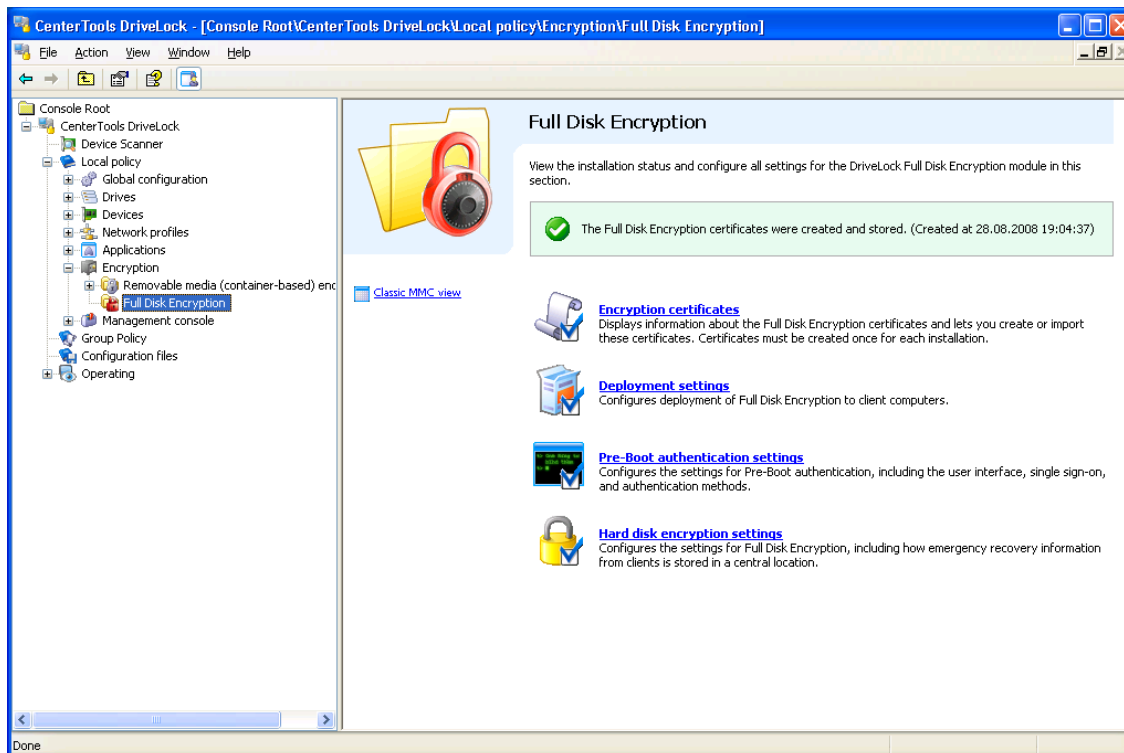
Single Sign-on after emergency logon – When enabled, this option allows the user to automatically authenticate to Windows immediately after the successful completion of the *emergency logon with username procedure*.

Allow emergency logon without username – When enabled, local Windows or domain users may initiate the *emergency logon without username procedure*. This allows for one-time-only pre-boot access to the system for users who don't have a pre-boot user account. This procedure also adds the user to the pre-boot authentication database. Once the user log on to Windows, the Windows password is automatically synchronized with the pre-boot authentication database to enable authentication using this password in the future.

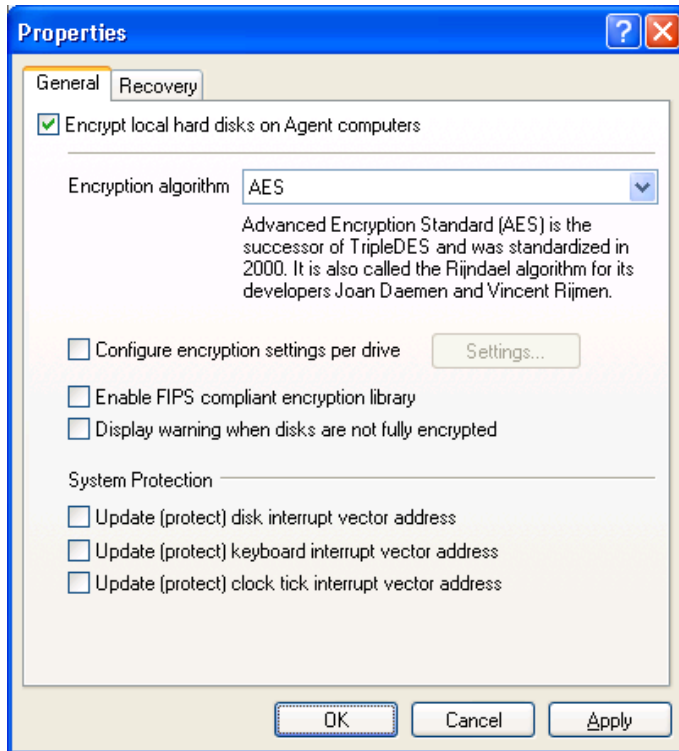
Allow emergency logon for token users – This option is available only if at least one of the following pre-boot authentication method options is selected: *Domain user access (with token)* or *Shared Key access*. If this option is enabled, smartcard and token users who have misplaced a token or forgotten the PIN are permitted to initiate the *emergency logon for token users procedure*. This procedure allows for a one-time-only pre-boot access to the computer without having to use a token.

4.2 Configuring Hard Disk Encryption

This chapter contains information on how to configure DriveLock FDE, how it stores emergency recovery information centrally and how Agents save this data.



Click **Hard disk encryption settings** to open the Properties dialog box.



To globally enable hard disk encryption, select the “*Encrypt local hard disks on Agent computers*” checkbox.



When you enable hard disk encryption, as soon as the DriveLock Agent receives the updated configuration settings, it starts to encrypt the local hard disk and applies the settings you specified. Ensure that all settings are configured correctly before you enable hard disk encryption.



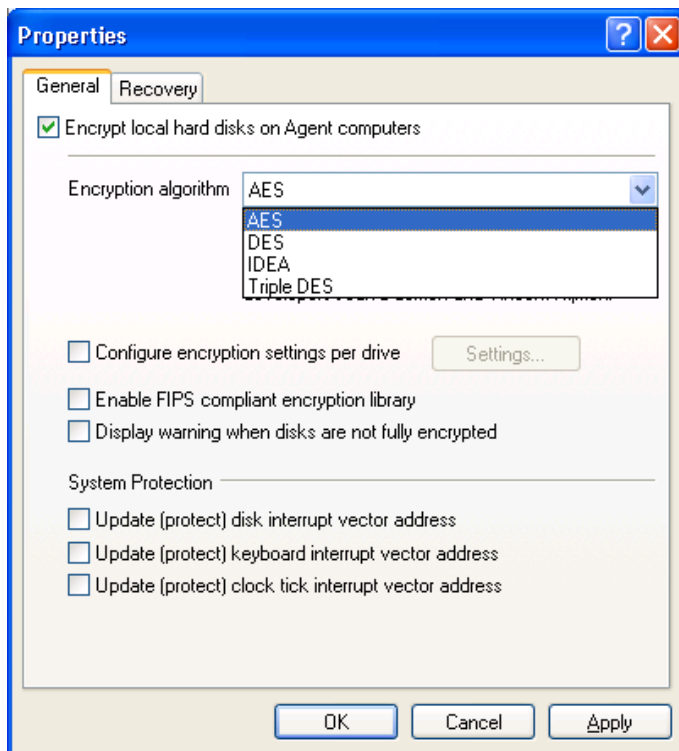
Depending on the size of your hard disk, encrypting or decrypting may take several hours. You can continue to use the computer during this time, but performance will be slightly degraded. You can shut down or re-boot the computer while encryption takes place. The encryption process will resume once the computer is running again.

You can select from several encryption algorithms. DriveLock can use the following algorithms:

- **AES** - The Advanced Encryption Standard (AES) is a symmetric encryption mechanism that was chosen by the National Institute of Standards (NIST) in October 2000 as the successor to DES and 3DES. It is also called the *Rijndael* algorithm for its developers Joan Daemen and Vincent Rijmen.
- **IDEA** - The International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James Massey of ETH Zurich and was first described in 1991. The algorithm was intended as

a replacement for the Data Encryption Standard. IDEA is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a round) and an output transformation (the half-round). The processes for encryption and decryption are similar.

- **DES** - The Data Encryption Standard (DES) is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny which motivated the modern understanding of block ciphers and their cryptanalysis. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small. This algorithm should only be used in environments with low security requirements.
- **Triple DES** - Triple DES (3DES) is a symmetric encryption method based on the older DES (Data Encryption Standard) but works with twice the key length (112 bit) of its predecessor. Data is encrypted using three successive DES operations. Because of the key length, 3DES is regarded as a relatively safe method for encrypting most data, unlike DES, which is more susceptible to brute-force attacks.



Select an encryption algorithm by using the drop-down menu.

By default DriveLock FDE encrypts all local hard disks. To configure encryption separately for each local hard disk, select the “*Configure encryption settings per drive*” checkbox and then click **Settings**.

If your organization’s policy requires compliance with Federal Information Processing Standard (FIPS) standard 140-2, select the “*Enable FIPS compliant encryption library*” checkbox. If this option is not selected, DriveLock instead uses a secure, CC EAL-2 approved, non-FIPS library that provides better performance for encryption and decryption operations.

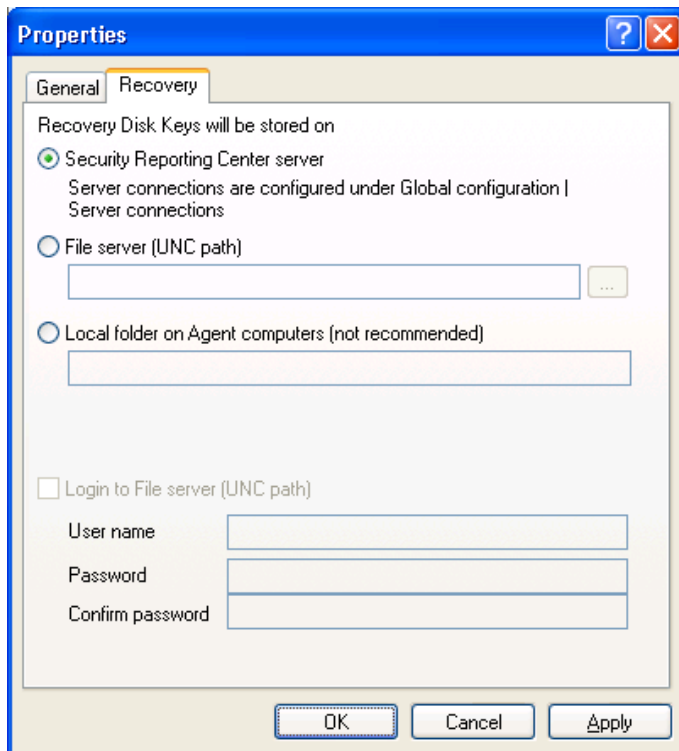
To display a warning message to all users at Windows logon that informs them when disks are not completely encrypted, select the “*Display warning when disks are not fully encrypted*” checkbox.

DriveLock FDE maintains a record of some BIOS interrupt vector addresses. This allows DriveLock FDE to detect attacks that depend on changing the interrupt vector address. When DriveLock FDE detects a discrepancy between the BIOS interrupt vector address and the copy it stored previously, it displays an error message. Select the corresponding check boxes to automatically update the stored copy of the interrupt vector addresses after the user has been notified.



When an interrupt vector address changes for legitimate reasons, for example after updating the BIOS, the warning message is still displayed. The *System Protection* group provides a mechanism to accept a legitimate change by updating DriveLock FDE’s copy of the disk, keyboard, and clock tick interrupt vector addresses.

To configure where the client’s recovery disk keys will be stored, click the *Recovery* tab.



The recovery disk keys consist of two files:

- *Recovery.env* – This is the envelope file for emergency logon recovery
- *DiskKeyBackup.zip* – This ZIP file contains the recovery files for disk decryption procedures



The envelope file is created and sent to the location you configured immediately after the Agent has finished installing DriveLock FDE on a client computer. The ZIP file containing the encryption recovery files is created and copied only after all drives have been completely encrypted.

The recovery files should be stored in the Security Reporting Center or on a central file share. It is not recommended to store these files on the local computer because of security and recovery considerations.



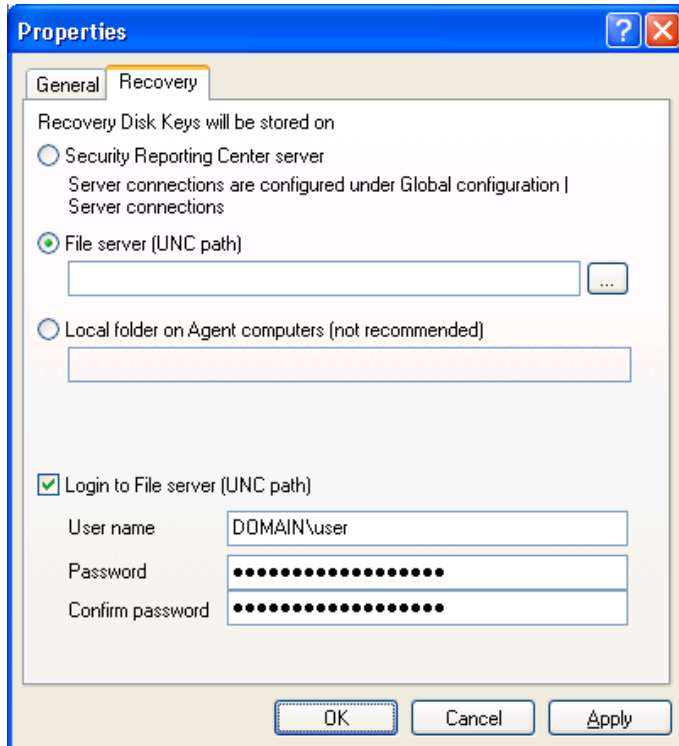
If you store the files on a central file share, the following file names are used:

- *<computer>.envelope.env*
- *<computer>.backup.zip*



You must configure a SRC server connection and specify a user name (domain\user) and password to enable the Agent to connect to the SRC server, as the Agent is usually configured to run as “Local System”. Otherwise the Agent will not be able to upload the files. Refer to the document “*DriveLock Administration Guide*” on how to configure an SRC server connection.

If the file server requires credentials for logon, specify them on the Recovery tab.



You need to type domain user names in the format `<domain>\<user>`.



Verify that you have stored these recovery files for all your client computers, as they are required to perform any of the recovery procedures described later in this manual. Use the Security Reporting Center to get a list of all events created after the Agent has successfully transferred these files to the central location.

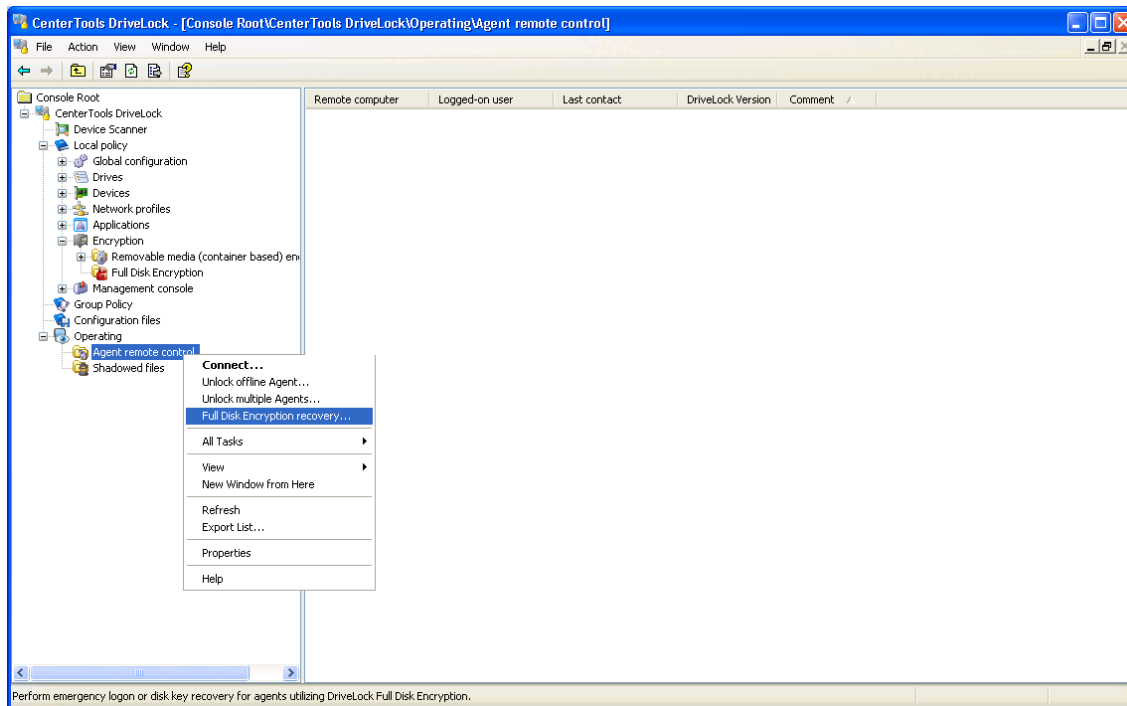
5 Recovery Procedures

DriveLock FDE contains tools for two types of recovery scenarios:

- Emergency logon recovery procedures
- Recovering encrypted disks

The emergency logon recovery procedures are used when a user can't log on to the pre-boot authentication database, for example, because of a forgotten password or PIN. Disk recovery is used when a local disk drive becomes inaccessible, for example, when data sectors of the drive have become corrupt or you cannot log on to Windows anymore.

To start the recovery wizard, open the DriveLock Management Console, select *Operating* → *Agent remote control*, right-click **Agent remote control** and then click *Full Disk Encryption recovery*.



5.1 Emergency Logon Recovery Procedures



If you disabled pre-boot authentication in the System Policy settings, the information in this section does not apply. In this case, the user sees the standard Windows domain authentication dialog box and normal Windows logon procedures apply.

There are three emergency logon procedures:

- Emergency logon with username
- Emergency logon without username
- Emergency logon for token users

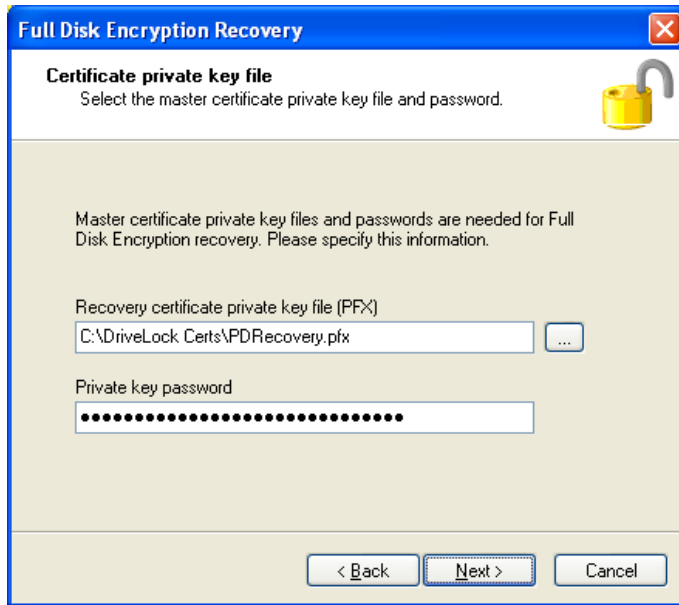
You can configure which of these procedures are available to users during pre-boot authentication. Refer to the section “Configuring emergency logon parameters” for details on how to configure these settings.



Select *Emergency logon* for the recovery type.

If you configured DriveLock FDE to send the client’s recovery disk keys to the Security Reporting Center, select *Security Reporting Center Server (SRC)*. To specify a file as the location of the required recovery disk keys, select *Recovery files (copied from the agent computer)*.

Click **Next** to continue.



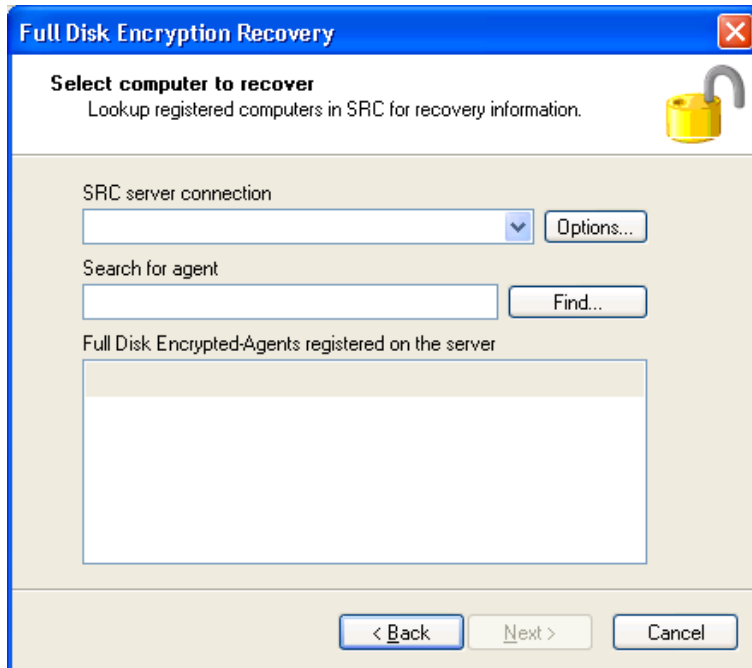
To perform emergency logon procedures you need to access the private key of the recovery certificate. Specify the path where the file *PDRecovery.pfx* file is located and type the password that is used to protect the private key.



If you lost access to the private key, recovery is not longer possible.

Click **Next** to continue.

If you selected the option to retrieve recovery information from the Security Reporting Center, the following dialog box appears.

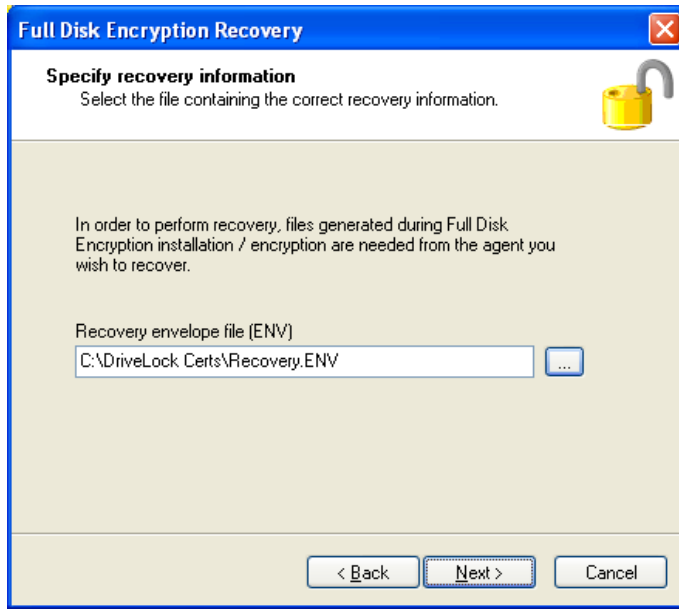


Select the SRC server from the drop-down menu. If the SRC Server requires logon credentials, click **Options** and specify these credentials.

To search for Agents registered with the selected SRC server, type the computer name and then click the **Find** button. If you enter only part of the name, DriveLock FDE displays all registered computers that contain this text as part of their names. To view a list of all registered computers, click the **Find** button without first typing a computer name.

Select the appropriate computer from the list and then click **Next** to continue.

If you selected to retrieve recovery information from a file, the following dialog box appears:

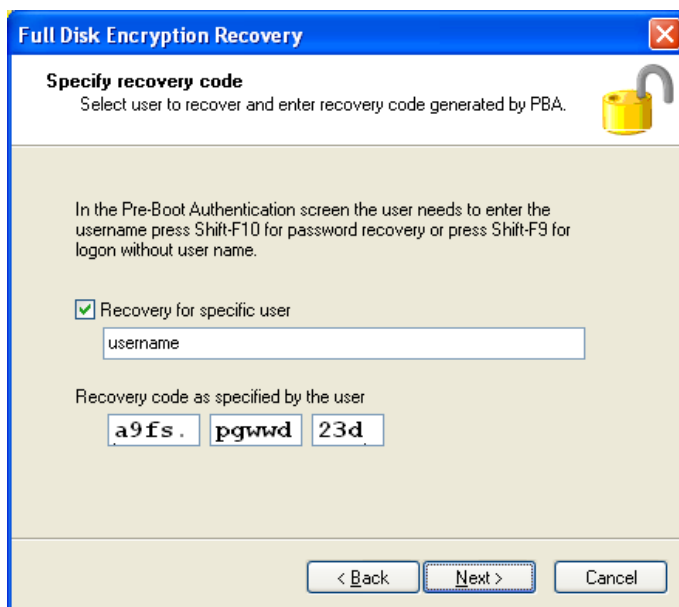


Type the path for the location of the recovery file or click the “...” button to open the file selection dialog box.

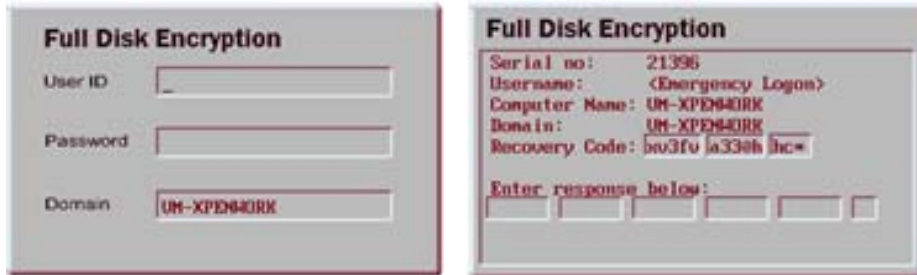


Each client computer has its own envelope file, which must be used for emergency recovery logon procedures. If you have configured DriveLock FDE to upload this file automatically to a central file share, the file name is prefixed with the name of the client computer (for example: *DE2319WX.Envelope.env*).

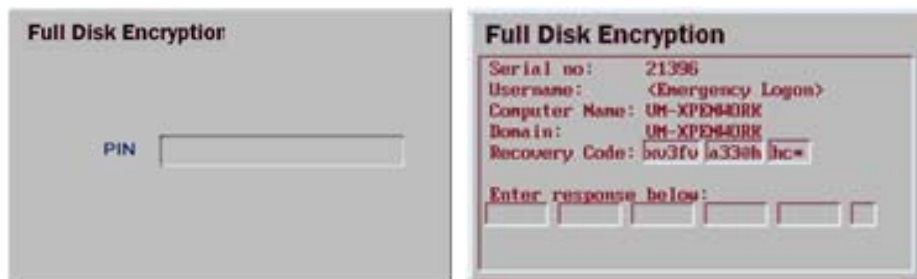
Click **Next** to continue.



If the user has logged on to pre-boot authentication before, at the pre-boot authentication screen, the user must type the user name, select the domain, place the cursor in the password field, and then press SHIFT-F10. This starts the *emergency logon with username procedure*:

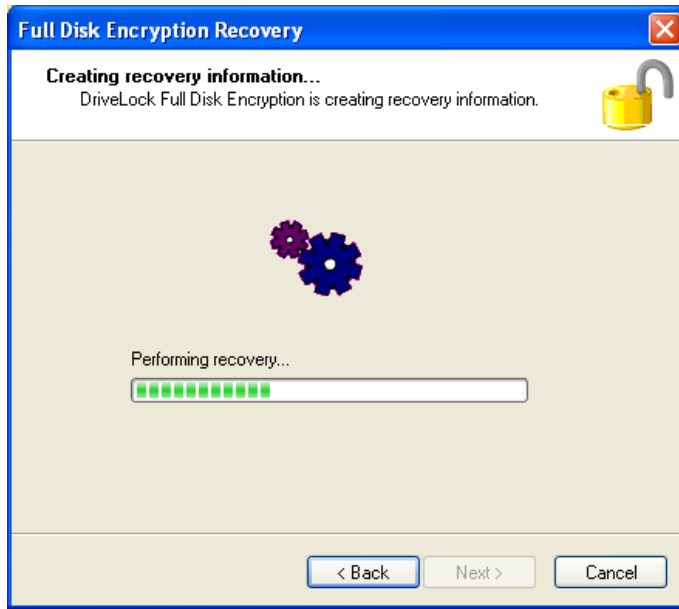


If the user has never logged on to the pre-boot authentication at any time or PIN authentication is used, at the pre-boot authentication screen, the user must place the cursor in the “User ID” or “PIN” field and then press SHIFT-F9. This starts the *emergency logon without username procedure* or *emergency logon for token user procedure* :

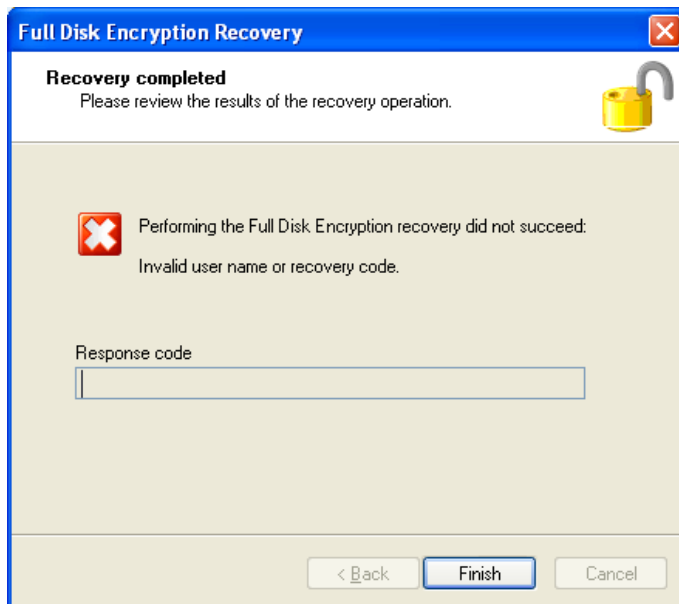


In the DriveLock Management Console, type the user name (if user has pressed SHIFT-F10) and the recovery code provided by the user.

Click **Next** to generate a response code for the user.

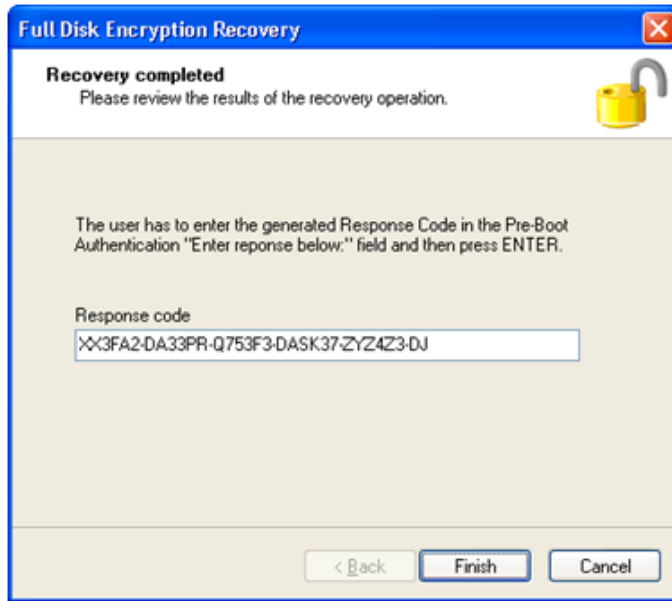


If an error occurs during the generation of the response code, DriveLock displays the following message:

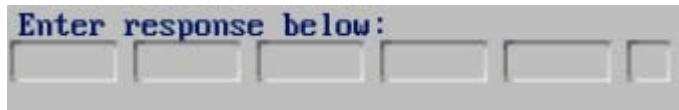


Click **Finish** and then start the recovery procedure again.

If recovery was successful, DriveLock displays a response code.



The user must type this response code at the pre-boot recovery screen:



Once the user types the response code, pre-boot authentication continues and Windows starts normally. Depending on how you configured DriveLock FDE, the user will be logged on to Windows *automatically* or can log on *manually*.

5.2 Recovering Encrypted Disks

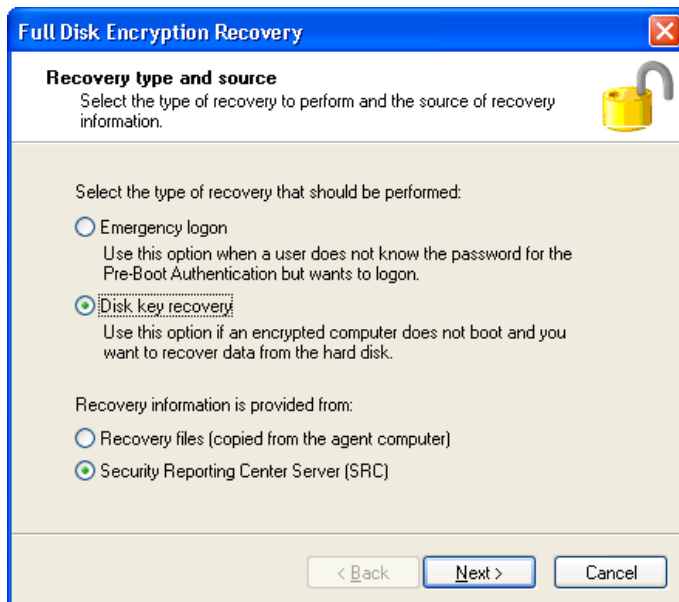
Disk recovery becomes necessary when local disk drives can no longer be accessed. This can occur, for example, when data sectors of the drive have become corrupt.

To recover (decrypt) an encrypted disk you must perform the following steps:

1. Create the recovery files
2. Copy all the files that are required for decryption to bootable media, such as a floppy disk, removable USB drive or CD.
3. Start the computer using the bootable media.
4. Use the files on the recovery media to decrypt the inaccessible hard disk.

These steps are described in more detail below.

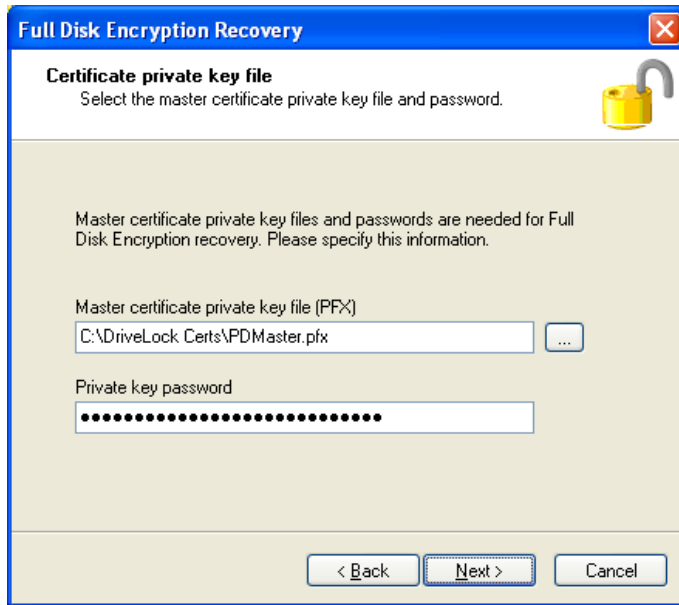
5.2.1 Creating the files required for decryption



Select *Disk key recovery* as the recovery type.

If you configured DriveLock FDE to send the client's recovery disk keys to the Security Reporting Center, select *Security Reporting Center Server (SRC)*. To specify a file as the location of the required recovery disk keys, select *Recovery files (copied from the agent computer)*.

Click **Next** to continue.



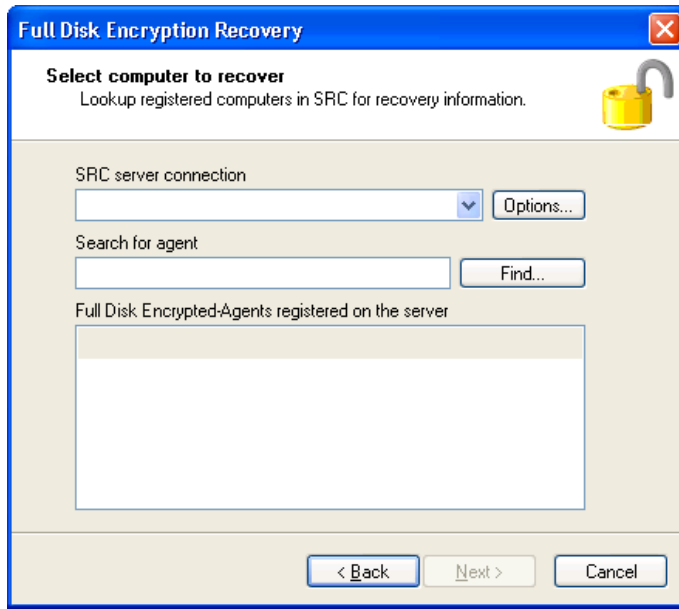
For disk recovery procedures you need to access the private key of the recovery certificate. Specify the path where the file *PDMaster.pfx* file is located and type the password that is used to protect the private key.



If you lost access to the private key, recovery is not longer possible.

Click **Next** to continue.

If you selected the option to retrieve recovery information from the Security Reporting Center, the following dialog box appears.

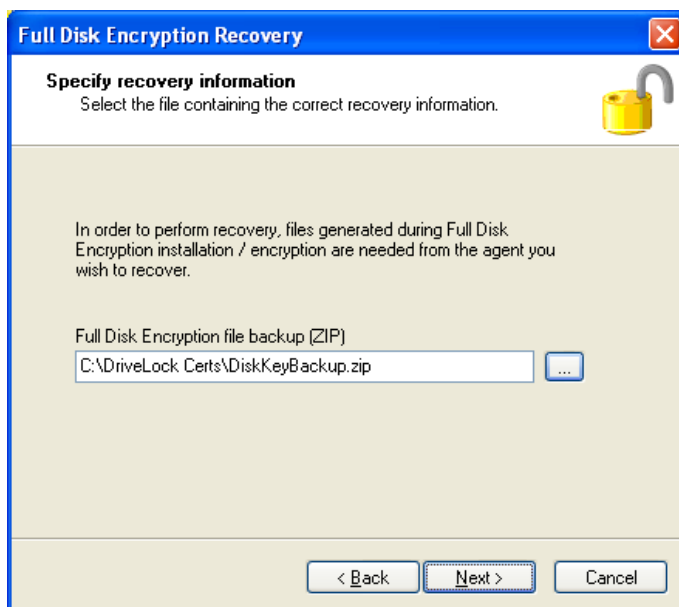


Select the SRC server from the drop-down menu. Click **Options** if the SRC Server requires logon credentials.

To search for Agents registered with the selected SRC server, type the computer name and then click the **Find** button. If you enter only part of the name, DriveLock FDE displays all registered computers that contain this text as part of their names.

Select the computer from the list and then click **Next** to continue.

If you selected to retrieve recovery information from a file, the following dialog box appears:



Type the path for the location of the recovery file or click the “...” button to open the file selection dialog box.

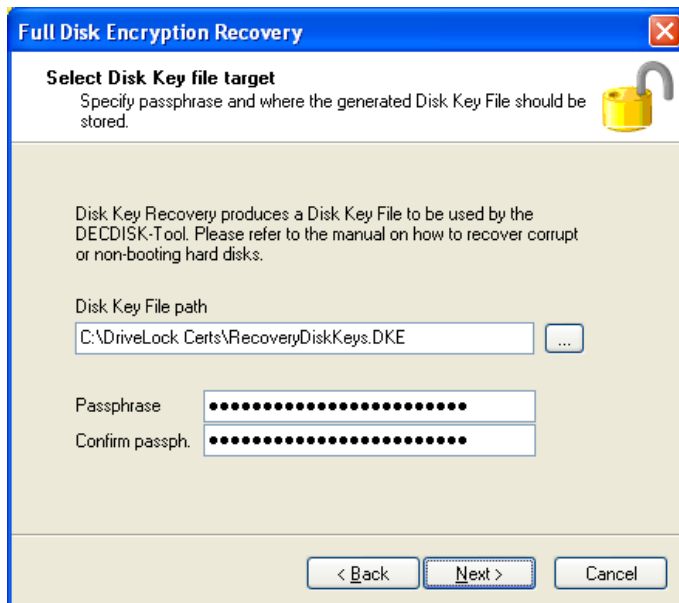


Each client computer has its own disk recovery file, which must be used for emergency recovery logon procedures. If you have configured DriveLock FDE to upload this file automatically to a central file share, the file name is prefixed with the name of the client computer (for example: *DE2319WX.Backup.zip*).



The EFS recovery files are automatically generated by the DriveLock Agent after all hard disks have been completely encrypted.

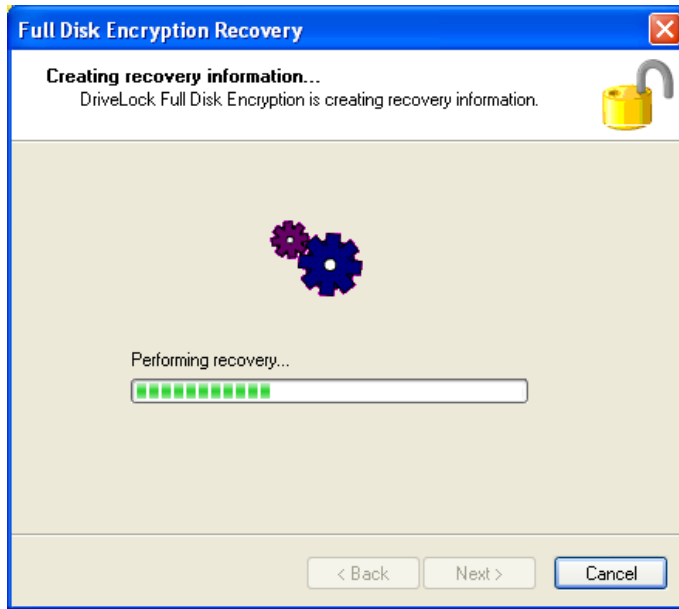
Click **Next** to continue.



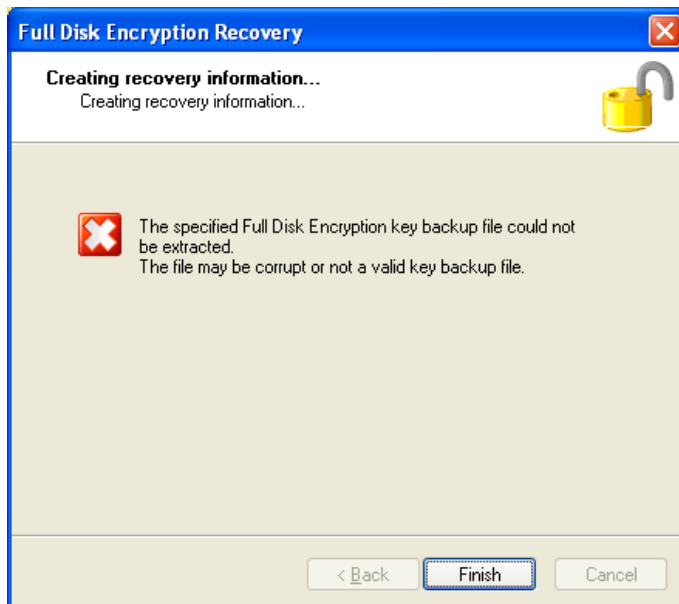
To allow for recovery, DriveLock FDE must generate a Disk Key File. To specify a file name and path, click the “...” button, or type the path and file name, including the file extension (*.dke*).

Type a password or passphrase to secure access to this file and confirm this password by typing it again. The password must at least contain 6 characters.

Click **Next** to generate the Disk Key File.

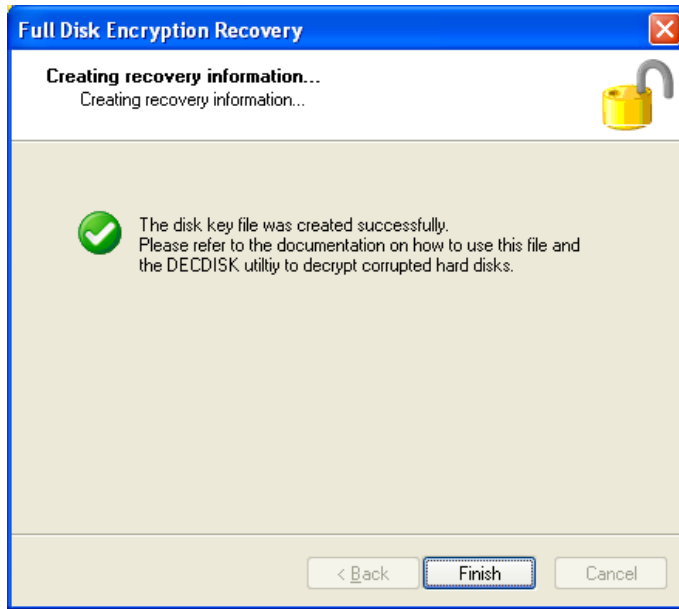


If you have selected an incorrect recovery file, the following dialog box appears:



Click **Finish** and then restart the recovery procedure.

After the Disk Key File has been created, DriveLock displays the following message:



Click **Finish** to close the wizard.

Copy the Disk Key File you created and the command line utility *decdisk.exe* to a bootable floppy disk, USB drive or CD to be used for recovering disks.



The *decdisk.exe* command line utility is located in the DriveLock program folder (Default: *C:\Program Files\CenterTools\DriveLock*). You can also use the ISO-Image provided to create a bootable CD containing all the tools required.

5.2.2 Recovering (decrypting) disks

Before you begin, verify that you have bootable media that contains DOS or an equivalent operating system. Ensure that the media contains the *decdisk.exe* utility and the encrypted *.dke file and that you know the passphrase you specified.

1. Start the computer by booting from the disk you created .
2. To decrypt the disk, from the command line, run the *decdisk.exe* program with the */dk* option and specify the Disk Key File, for example: `decdisk /dk diskkey.dke`.
3. When prompted, type the passphrase that protects the Disk Key File.
4. When prompted, select the area of the disk to be decrypted.
5. After decrypting the disk, type `fdisk /mbr` to remove the DriveLock pre-boot authentication and restart the PC.



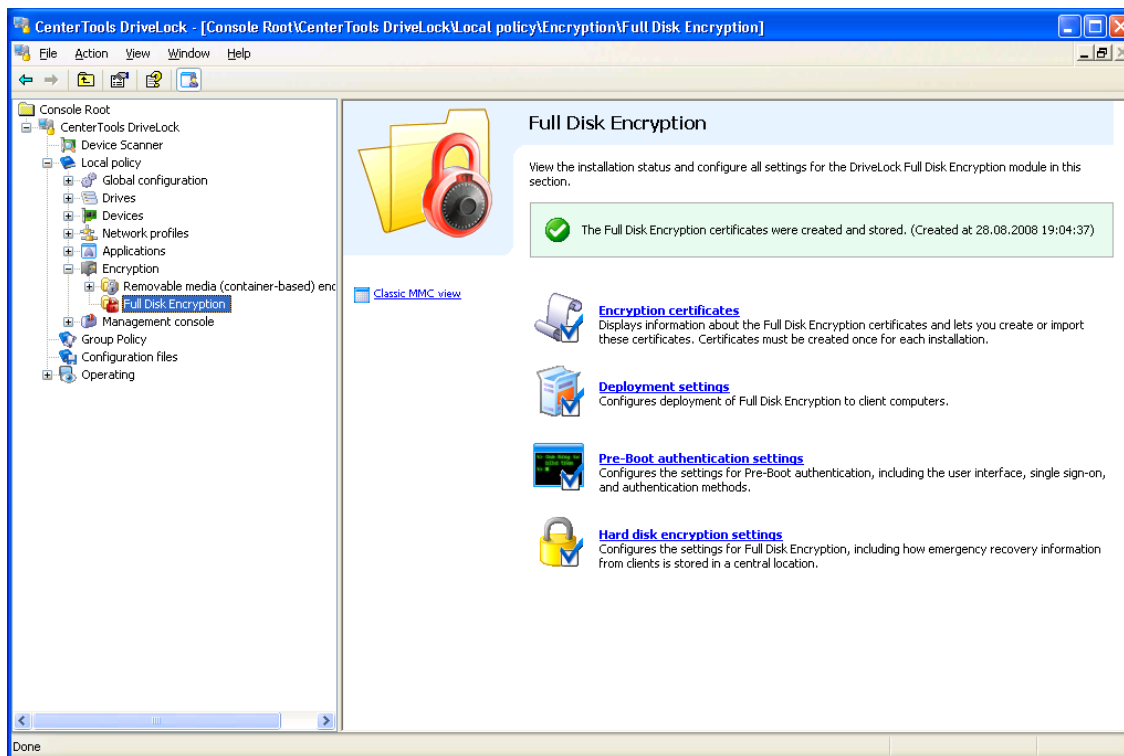
Running `fdisk /mbr` may not be sufficient to restore the boot environment on a computer running Windows Vista.

6. After the computer restarts, uninstall DriveLock FDE (see chapter “Uninstalling DriveLock FDE Completely”).
7. Delete the Disk Key File and passphrase, as they are now obsolete.

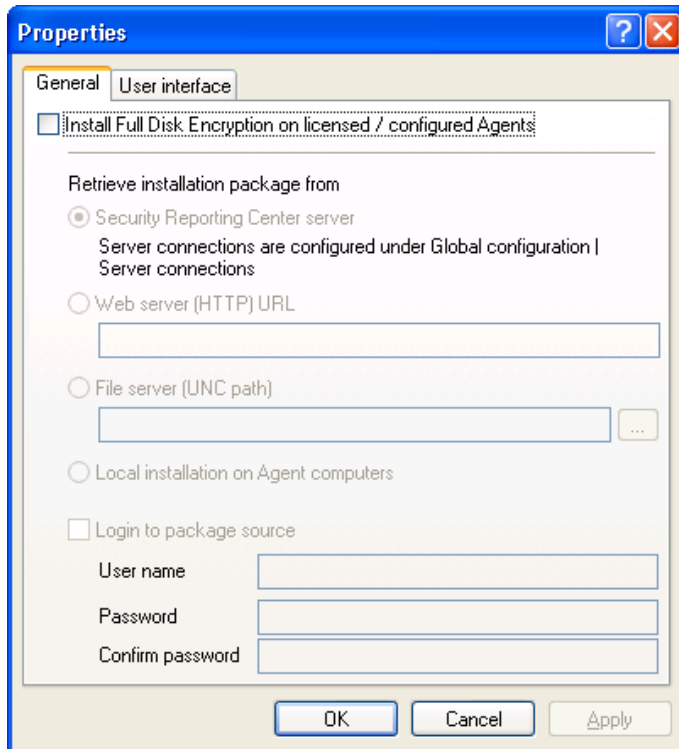
6 Uninstalling DriveLock Full Disk Encryption

You can configure DriveLock FDE to decrypt previously encrypted hard disks on client computers, to remove pre-boot authentication and to completely uninstall DriveLock Full Disk Encryption.

6.1 Uninstalling DriveLock FDE Completely



To completely remove DriveLock FDE from client computers click **Deployment settings**.



Clear the “*Install Full Disk Encryption on licensed / configured Agents*” checkbox and then click **OK** to close the dialog box.

When the Agent receives the new configuration settings, it performs the following steps:

1. Decrypting all encrypted hard disks
2. Removing pre-boot authentication from the system
3. Uninstalling DriveLock FDE



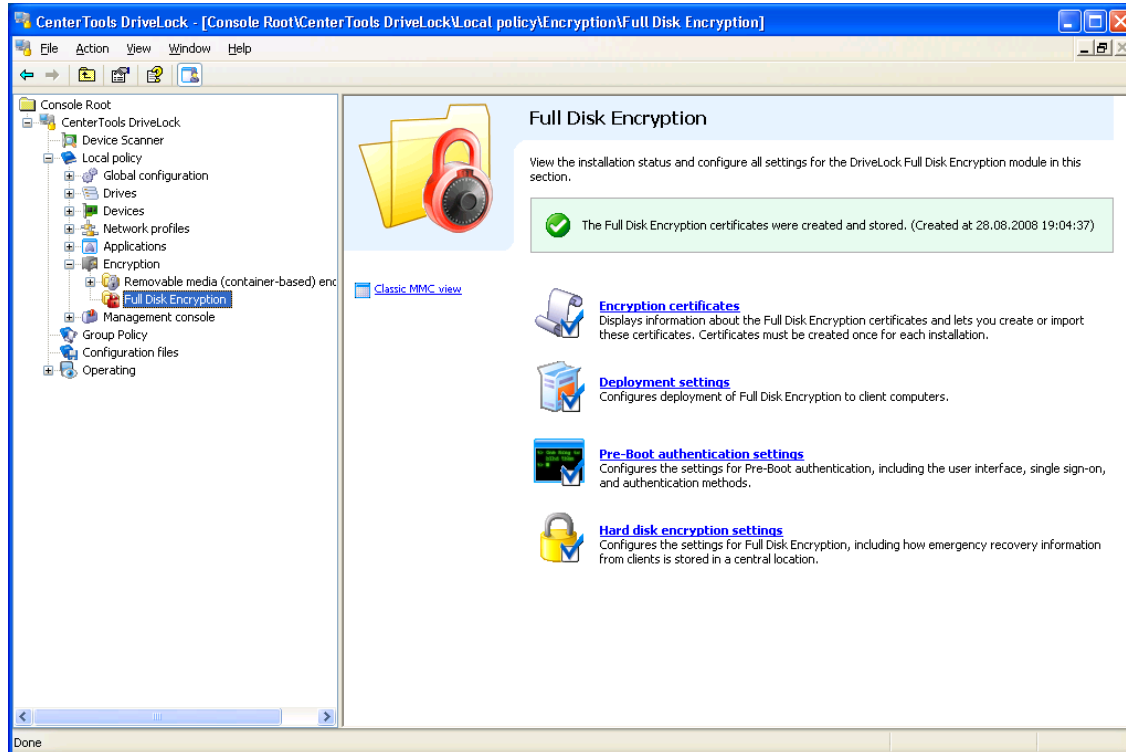
If you installed the DriveLock FDE installation package *pdinstall.bin* locally on the client and it is no longer required, you must delete it manually.

6.2 Disabling Pre-Boot Authentication

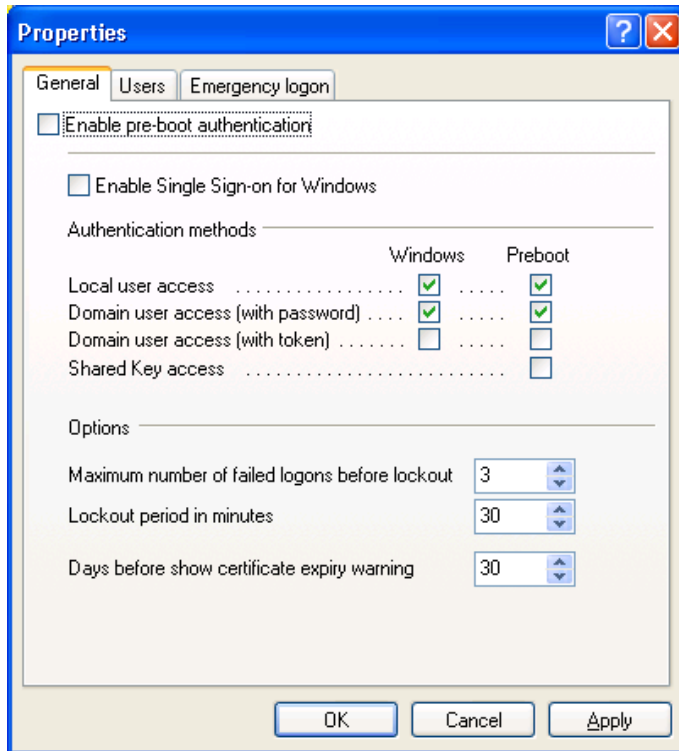
You can configure DriveLock FDE to disable pre-boot authentication.



Disabling pre-boot authentication also initiates the decrypting of any encrypted hard disks.



To disable pre-boot authentication on client computers, click **Pre-boot authentication settings**.



Clear the “*Enable pre-boot authentication*” checkbox and then click **OK** to close the window.

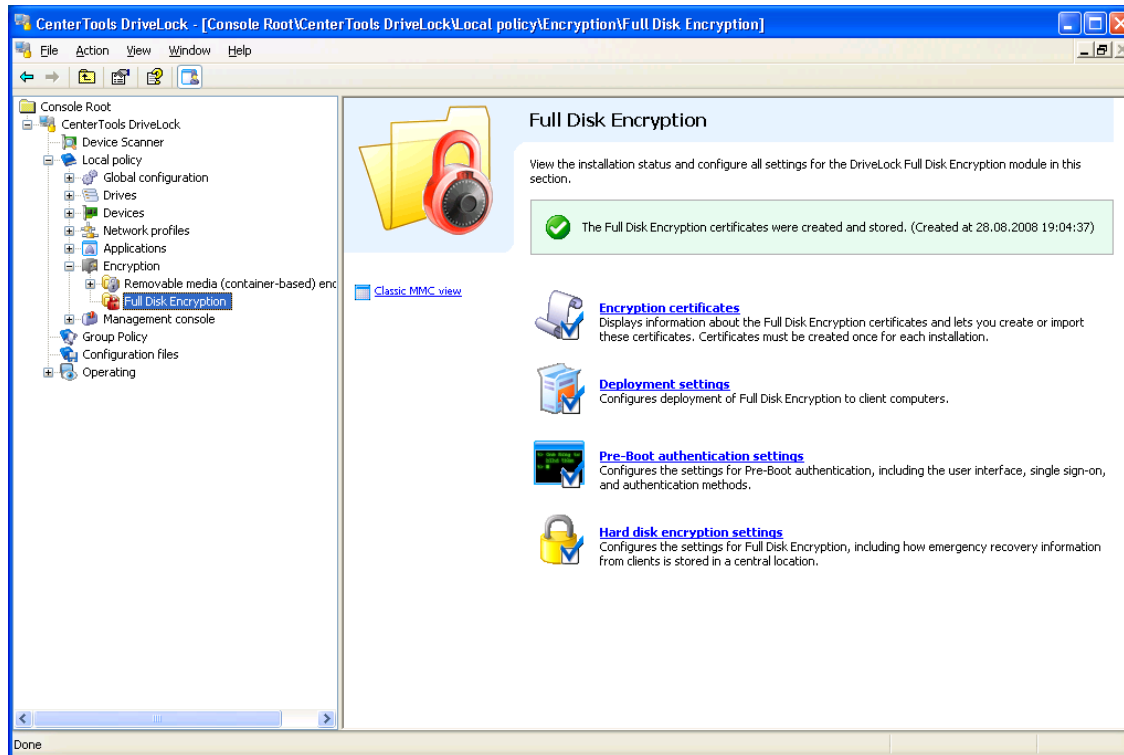
When the Agent receives the new configuration settings, it performs the following steps:

1. Decrypting all encrypted hard disks
2. Removing pre-boot authentication from the computer

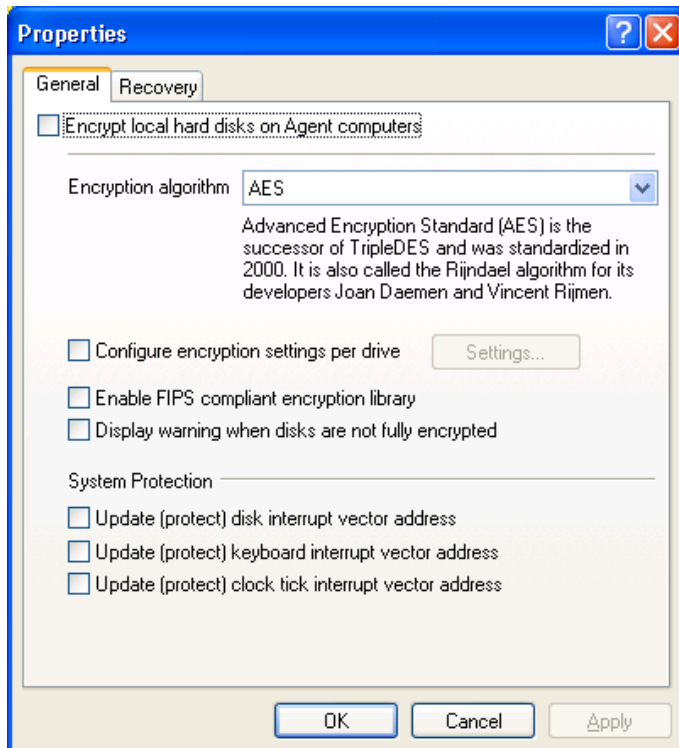
When you disable pre-boot authentication, DriveLock FDE is not uninstalled from the client computer and you can re-enable pre-boot authentication later.

6.3 Decrypting Hard Disks

You can configure DriveLock FDE to decrypt encrypted disk drives.



To disable encryption on client computers, click **Hard disk encryption settings**.



Clear the "Encrypt local hard disk on Agent computers" checkbox and then click **OK**.

When the Agent receives the new configuration settings, it starts decrypting all encrypted hard disks.

When you decrypt hard drives, DriveLock FDE is not uninstalled from the client computer and pre-boot authentication remains active. You can re-encrypt drives later.

7 User Logon and Appearance



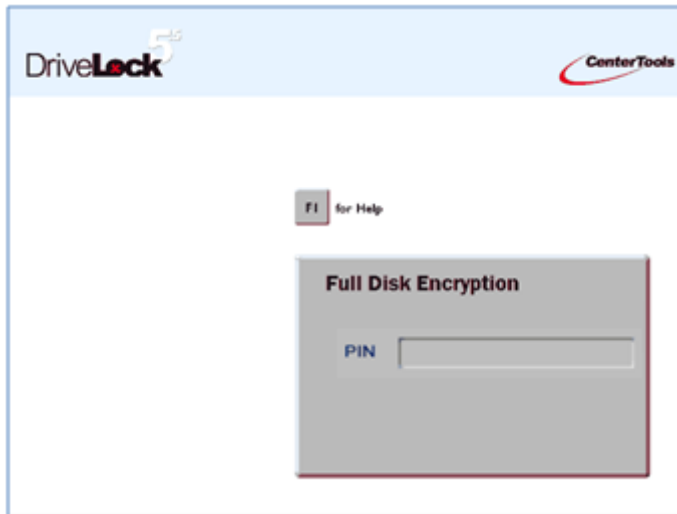
If you disabled pre-boot authentication in the System Policy settings, this section does not apply. Without pre-boot authentication users only see the standard Windows authentication dialog box and normal Windows logon procedures apply.

7.1 Authenticating With Smartcard or Token and PIN

7.1.1 Pre-boot authentication

If you selected the DriveLock FDE *Domain user access (token)* or *Shared Key Access* authentication check boxes, the pre-boot authentication screen shown below is displayed when the computer starts. If the *Local user access* or *Domain user access (password)* authentication options are also enabled, pressing **[F2]** toggles between the Username/Password/Domain Name logon screen and the Token/PIN password screen.

To authenticate from this screen a user must insert a smart card or token and type the corresponding PIN. To prevent PIN guessing, you can define a lockout policy to lock the computer after a configurable number of consecutive failed authentication attempts. To view details of failed logon attempts and other events use the *Windows Event Viewer*.



If a user doesn't remember the correct PIN and therefore cannot log on to the system, the user can press **SHIFT-F9** to start the *emergency logon for token user procedure*. For details about this procedure, refer to the section "Emergency logon recovery procedures".

7.1.2 Windows authentication



Every time a user successfully logs on to Windows or changes the password in Windows, the user's current Windows password is synchronized with the pre-boot user database.

7.1.2.1 Automatic - Single sign-on mode is on

If DriveLock FDE Single sign-on mode is enabled, users are automatically authenticated by Windows.

7.1.2.2 Manual - Single sign-on mode is off

If you didn't configure Single sign-on, the following standard Windows domain authentication dialog box appears.



If you insert a smartcard or token into a reader, the following standard Windows certificate authentication dialog box is displayed. At this point, the user must type the PIN to continue.

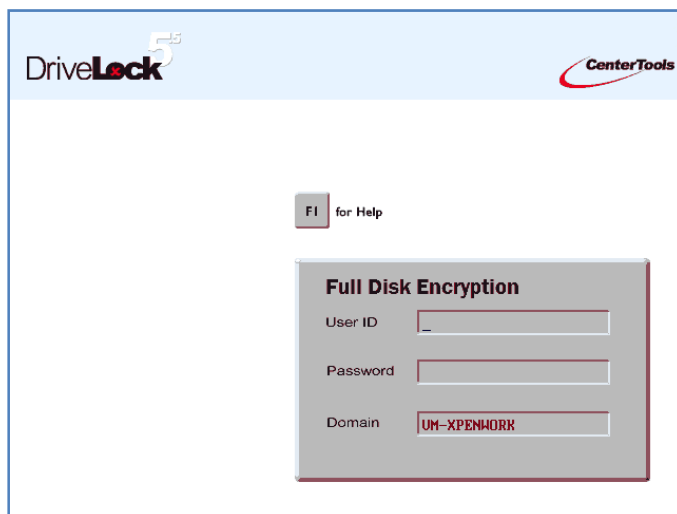


If the *Local user access* or the *Domain user access (password)* checkboxes are selected, the user can press **Ctrl-Alt-Del** at this point to display the standard Windows logon dialog box.

7.2 Authenticating With User Name, Password, and Domain Name

7.2.1 Pre-boot authentication

If the *Local user access* or the *Domain user access (password)* options are selected, the DriveLock FDE pre-boot authentication screen displayed below appears after the computer is turned on.



The domain field lists all available domains if *Domain user access (password)* is allowed, The *Local Computer Name* is also be listed in the Domain field of the pre-boot authentication screen. Use the [Up-

Arrow] and [Down-Arrow] keys to scroll through the list of available domains. To prevent password guessing, you can define a lockout policy to lock the computer after a configurable number of consecutive failed authentication attempts. To view details of failed logon attempts and other events use the Windows *Event Viewer*.

7.2.2 Windows authentication



Every time a user successfully logs on to Windows or changes the password in Windows, the user's current Windows password is synchronized with the pre-boot user database.

7.2.2.1 Automatic – Single sign-on mode is on

If the DriveLock FDE Single sign-on mode is enabled, users are automatically authenticated by Windows.

7.2.2.2 Manual – Single sign-on mode is off

If you didn't configure Single sign-on, the following standard Windows domain authentication dialog box appears.



After you press `Ctrl-Alt-Del` the following logon dialog box appears. To log on to Windows, type your Windows credentials.

